Sur les Extensions Galoisiennes de Degré Infini

CHEN Tong & WERTHE Alexandre
Projet M1 Maths Approfondies
Tuteur : Jean-Robert Bélliard

Janvier-Juin 2017

Introduction

La théorie de Galois, née de l'étude d'Évariste Galois des équations algébriques, est l'étude des extensions de corps commutatifs par le biais des groupes de Galois. Les résultats les plus importants de cette étude sont le théorème fondamental de la théorie de Galois, qui établit une correspondance entre les sous-groupes du groupe de Galois et les extensions intermédiaires de corps, et le théorème de l'élément primitif. La théorie de Galois finie traite les cas des extensions galoisiennes finies. Cependant, cette étude ne suffit pas pour traiter le cas infini. Nous avons en effet besoin des notions de groupe topologique et de limite inverse. La théorie de Galois s'étend dans d'autres branches que l'algèbre, telles que la géométrie, la cryptographie ou encore la théorie de Galois différentielle.
Le but de notre projet est d'établir la théorie de Galois pour les extensions galoisiennes de degré infini. Dans une première partie, nous ferons des rappels concernant la théorie de Galois finie ainsi que la topologie générale. Nous rappellerons par exemple la définition d'une extension galoisienne ou abélienne, du groupe de Galois d'une extension, de la topologie produit, quotient ou induite. Ensuite, nous calculerons le groupe de Galois des extensions finies de corps fini $\mathbb{F}_{p^n}/\mathbb{F}_p$ et des extensions cyclotomiques $\mathbb{Q}(\xi_n)/\mathbb{Q}$, puis nous énoncerons le théorème fondamental de la théorie de Galois et le théorème de Tychonoff qui dit qu'un produit d'espaces topologiques compacts est compact au sens de la topologie produit. Dans une deuxième partie nous étudierons la théorie de Galois infinie. Nous commencerons par donner la définition d'un groupe topologique puis par étudier ses propriétés. Ensuite, nous définirons les notions de système inverse et de limite projective puis nous étudierons leurs propriétés en considérant dans un premier temps un ensemble I pré-ordonné, puis par la suite filtrant à droite. Ensuite, nous définirons la topologie de Krull, qui est une topologie sur le groupe de Galois compatible avec la structure de groupe topologique. Nous énoncerons puis démontrerons le théorème de Krull, qui nous donne une correspondance entre les sous-groupes fermés du groupe de Galois et les extensions intermédiaires de corps et enfin nous étudierons le groupe de Galois de l'extension L/L', où L est la clôture séparable d'un corps et L' la clôture abélienne de ce même corps. Dans une dernière partie, nous étudierons l'extension $\overline{\mathbb{F}}_p/\mathbb{F}_p$ puis l'extension cyclotomique maximale du corps des rationnels. Pour cela, nous introduirons l'anneau des entiers p-adiques $\mathbb{Z}_p$ et démontrerons un théorème très utile nous permettant de décrire de manière précise leur groupe de Galois. Pour le deuxième exemple, nous aurons également besoin du théorème de Kronecker-Weber qui dit que toute extension abélienne finie du corps des rationnels est un sous-corps d'une extension cyclotomique et d'étudier la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Table des matières

1 Quelques Rappels

Dans cette partie, on rappellera des notions et des propriétés vues dans les cours précédents qui seront utiles pour établir la théorie de Galois infinie.

1.1 Théorie de Galois de degré fini

On commencera par rappeler quelques notions importantes dans la théorie des corps et quelques résultats connus dans la théorie de Galois finie. Soit K/k une extension de corps.

Définition 1.1. (i) Un corps k est dit *algébriquement clos* si tout polynôme non-constant $f \in k[X]$ est scindé sur k ;
(ii) On appelle *clôture algébrique* d'un corps k toute extension L de k telle que L est algébrique sur k et L est algébriquement clos. On le note $\overline{k}$.

Remarque. (i) Tout corps admet une clôture algébrique (cf. théorème de Steinitz, *L'arithmétique des corps* par P. Ribenboim [4], page 19) ;
(ii) Deux clôtures algébriques de k sont k-isomorphes.

Définition 1.2. Soient $f \in k[X]$ et $\overline{k}$ une clôture algébrique de k. Le sous-corps de $\overline{k}$ engendré par les racines de f est appelé le *corps de décomposition de* f ou le *corps des racines de* f.

Remarque. Le corps de décomposition dépend du choix de la clôture algébrique $\overline{k}$ de k, deux corps de décomposition d'un même polynôme sont k-isomorphes.

Définition 1.3. L'extension K/k est dite *normale* si elle est algébrique et si tout polynôme irréductible de $k[X]$ ayant au moins une racine dans K est scindé sur K.

Proposition 1.4. *Soit K/k une extension algébrique avec $K \subseteq \overline{k}$. Alors K/k est normale si et seulement si $\sigma(K) = K$ pour tout k-homomorphisme $\sigma : K \longrightarrow \overline{k}$.*

Preuve. Rappelons la preuve vue en cours de corps. Notons que si $x \in K$ et si $\sigma : K \longrightarrow \overline{k}$ est un k-homomorphisme, alors $\sigma(x)$ est un k-conjugué de x. Supposons que K/k est normale. Alors tout k-conjugué de x appartient à K et ainsi, $\sigma(x) \in K$ pour tout k-homomorphisme $\sigma : K \longrightarrow \overline{k}$. Réciproquement, si y est un k-conjugué de x, définissons un k-isomorphisme $\tau : k(x) \longrightarrow k(y)$ par $\tau(x) = y$. Par le théorème de prolongement, il existe un k-homomorphisme $\sigma : K \longrightarrow \overline{k}$ tel que $\sigma|_{k(x)} = \tau$. On a donc $\sigma(K) = K$ par hypothèse, c'est-à-dire, $y = \tau(x) = \sigma(x) \in K$. D'où K/k est normale.

□

Exemple 1.1. (i) Si $\overline{k}$ est une clôture algébrique de k, alors l'extension $\overline{k}/k$ est normale ;
(ii) L'extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n'est pas normale. En effet, $\mathbb{Q}(\sqrt[3]{2})$ contient $\sqrt[3]{2}$ mais pas ses $\mathbb{Q}$-conjugués $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

Définition 1.5. Un polynôme non constant P de $k[X]$ est dit *séparable* si toutes les racines de P dans un corps de décomposition de P sont simples.

Exemple 1.2. (i) Le polynôme $X^n - 1 \in \mathbb{Q}[X]$ est séparable, car ses racines sont $e^{\frac{2k\pi i}{n}}$ avec $k = 0, 1, \cdots, n-1$;
(ii) Le polynôme $P(X) = X^p - t \in \mathbb{F}_p(t)[X]$ n'est pas séparable. En effet, comme $\mathbb{F}_p$ est un corps, on en déduit que $\mathbb{F}_p[t]$ est un anneau factoriel avec t irréductible (donc aussi premier). On a ainsi que P est irréductible dans $\mathbb{F}_p[t][X]$ en appliquant le critère d'Eisenstein en t. Par conséquent, P est irréductible dans $\mathbb{F}_p(t)[X]$. Fixons une clôture algébrique $\overline{k}$ de k. Si α est une racine de P dans $\overline{k}$ alors $\alpha^p = t$ et ainsi on peut factoriser P dans $\overline{k}[X]$ de la manière suivante : $P(X) = X^p - \alpha^p = (X - \alpha)^p$. D'où P n'est pas séparable.

Définition 1.6. Un corps k est dit *parfait* si tout polynôme irréductible de $k[X]$ est séparable.

Proposition 1.7. *Un corps k est parfait si et seulement si*

$$\Big[car(k) = 0\Big] \ \ ou \ \ \Big[car(k) = p \neq 0 \ \ et \ \ k = \{a^p | a \in k\}\Big].$$

Preuve. Cf. *Extension de corps* par J. Calais [2] (page 44, théorème 3.27, chapitre 3).

□

Corollaire 1.8. *Si k est un corps de caractéristique zéro ou si k est un corps fini, alors k est parfait.*

Définition 1.9. Un élément α de K qui est algébrique sur k est dit *séparable sur k* si son polynôme minimal $Irr_k(\alpha)$ est séparable.

Définition 1.10. L'extension K/k est dite *séparable* si elle est algébrique et si tout élément de K est séparable sur k.

Remarque. Toute extension algébrique d'un corps parfait est une extension séparable.

Exemple 1.3. (i) Toute extension algébrique de $\mathbb{Q}$ est séparable car $\mathbb{Q}$ est de caractéristique zéro ;
(ii) L'extension $\mathbb{F}_p(t^{\frac{1}{p}})/\mathbb{F}_p(t)$ n'est pas séparable. En effet, on a déjà vu dans le point (ii) de l'exemple 1.2 que $P(X) = X^p - t \in \mathbb{F}_p(t)[X]$ est un polynôme irréductible qui s'annule en $t^{\frac{1}{p}}$. On en déduit que P est le polynôme minimal de $t^{\frac{1}{p}}$, qui n'est pas séparable.

Définition 1.11. Une extension K/k est dite *galoisienne* si elle est normale et séparable.

Remarque. (i) Une extension finie K/k est galoisienne si et seulement si $|(Aut(K/k)| = [K : k]$;
(ii) Une extension finie K/k est galoisienne si et seulement si K est le corps de décomposition d'un polynôme séparable $P(X) \in k[X]$.

Exemple 1.4. (i) L'extension $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}$ est galoisienne. En effet, $\mathbb{Q}(j, \sqrt[3]{2})$ est le corps de décomposition du polynôme séparable $X^3 - 2 \in \mathbb{Q}[X]$. D'après la remarque (ii) de la définition 1.11, $\mathbb{Q}(j, \sqrt[3]{2})/\mathbb{Q}$ est galoisienne ;
(ii) Toute extension quadratique d'un corps de caractéristique zéro est galoisienne. En effet, toute extension algébrique K/k d'un corps de caractéristique zéro est séparable. Soit $d \in K - k$, alors $K = k(d)$ car $[K : k] = 2$. Soient $P(x) = x^2 + ax + b$ le polynôme minimal de d et d' le k-conjugé de d, alors $d + d' = -a$. On en déduit que $d' \in K$. Donc K/k est le corps de décomposition du polynôme P et ainsi, K/k est une extension galoisienne.

Définition 1.12. Si K/k est une extension galoisienne, le groupe $Aut(K/k)$ est noté $Gal(K/k)$ et appelé le *groupe de Galois de K/k*.

Définition 1.13. Une extension K/k est dite *abélienne* (resp. *cyclique*) si elle est galoisienne de groupe de Galois abélien (resp. cyclique).

Théorème 1.14. (Groupe de Galois d'extensions finies de corps fini). *Soient k un corps fini de caractéristique p à q éléments et K/k une extension de degré n. Alors l'extension K/k est galoisienne. Son groupe de Galois $Gal(K/k)$ est cyclique d'ordre n, engendré par $F : K \to K, x \mapsto x^q$ un élément de $Aut(K/k)$.*

Preuve. Rappelons la preuve vue en cours de corps. Notons $|k| = q$ et $|K| = q^n$. D'après le corollaire 1.8, k est un corps parfait. Donc l'extension K/k est séparable. De plus, K est un corps de décomposition du polynôme $X^{q^n} - X \in \mathbb{F}_p[X]$ donc l'extension $K/\mathbb{F}_p$ est normale, et il en résulte que l'extension relative K/k est normale. Donc K/k est galoisienne de goupe de Galois d'ordre $[K : k] = n$.
Posons $F : K \to K, x \mapsto x^q$. C'est un k-automorphisme de K. Montrons que $ord(F) = n$.
Pour tout $x \in K$, $x^{q^n} = x$ car $|K| = q^n$. On en déduit que $F^n = id_K$, d'où $\boxed{ord(F)|n}$.
Si $F^d = id_K$ avec $d|n$ et $d \neq n$, alors $x^{q^d} = x$ pour tout $x \in K$. On en déduit que $K \subseteq \mathbb{F}_{p^d}$ et ceci contredit le fait que $|K| = q^n > q^d$. Ainsi $\boxed{ord(F) = n}$.
Par conséquent, F engendre $Gal(K/k)$ et donc $Gal(K/k)$ est cyclique d'ordre n.

□

Théorème 1.15. (Groupe de Galois d'extensions cyclotomiques). *Soit ξ_n une racine primitive n-ème de l'unité avec $n \in \mathbb{N}^*$. Alors $\mathbb{Q}(\xi_n)/\mathbb{Q}$ est une extension galoisienne. Son groupe de Galois $Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$ est abélien et est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Preuve. Rappelons la preuve vue en cours de corps. Remarquons d'abord que si ξ_n est une racine primitive n-ème de l'unité fixé (par exemple, $\xi_n = e^{-\frac{2\pi i}{n}}$) et si $\sigma \in Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$, alors $\sigma(\xi_n)$ est aussi une racine primitive n-ème de l'unité. En effet, $(\sigma(\xi_n))^n = \sigma(\xi_n^n) = \sigma(1) = 1$, donc $\boxed{ord(\sigma(\xi_n))|n}$. De plus, comme σ est un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\xi_n)$, on en déduit que $(\sigma(\xi_n))^k \neq 1$ pour tout k verifiant $1 \leq k \leq n-1$. D'où $\boxed{ord(\sigma(\xi_n)) = n}$, c'est-à-dire, ξ_n est une racine primitive n-ème de l'unité. Il existe donc un unique $k_\sigma \in \mathbb{N}$ avec $1 \leq k_\sigma \leq n-1$ et $pgcd(k, n) = 1$ tel que $\sigma(\xi_n) = (\xi_n)^{k_\sigma}$. Posons maintenant

$$\begin{array}{rccc} \varphi : & Gal(\mathbb{Q}(\xi_n)/\mathbb{Q}) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ & \sigma & \longmapsto & k_\sigma, \end{array}$$

puis montrons que φ est un isomorphisme.
$\star$ φ est un homomorphisme. En effet, si $\sigma, \tau \in Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$, alors

$$(\sigma \circ \tau)(\xi_n) = \sigma((\xi_n)^{k_\tau}) = (\sigma(\xi_n))^{k_\tau} = ((\xi_n)^{k_\sigma})^{k_\tau} = (\xi_n)^{k_\sigma k_\tau}.$$

On en déduit que $k_{\sigma\circ\tau} = k_\sigma k_\tau$.
$\star$ φ est injective. En effet, si $k_\sigma = 1$, alors $\sigma(\xi_n) = \xi_n$. On en déduit que $\sigma = id_{\mathbb{Q}(\xi_n)}$.
$\star$ φ est surjective. En effet, pour $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, posons $\sigma(\xi_n) = \xi_n^k$. Alors σ est un $\mathbb{Q}$-automorphisme de $\mathbb{Q}(\xi_n)$ car ξ_n^k est une racine primitive n-ème de l'unité, c'est-à-dire, $\sigma \in Gal(\mathbb{Q}(\xi_n)/\mathbb{Q})$.
Conclusion : φ est un isomorphisme.

□

Définition 1.16. Soient K un corps et H un sous-groupe de $Aut(K)$. Alors

$$Inv_K(H) = \{x \in K | \forall \sigma \in H, \sigma(x) = x\}$$

est un sous-corps de K. On l'appelle le *sous-corps de K fixé par H*. Un élément x de K est dit *fixé par H* si $x \in Inv_K(H)$.

Exemple 1.5. (i) Le sous-corps de $\mathbb{C}$ fixé par le sous-groupe de $Aut(\mathbb{C})$ engendré par la conjugaison complexe est $\mathbb{R}$;
(ii) On a vu dans le théorème 1.14 que l'extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ est galoisienne, de groupe de Galois cyclique engendré par le homomorphisme de Frobenius $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}, x \mapsto x^p$. Pour tout d tel que $d|n$, on a :

$$Inv_{\mathbb{F}_{p^n}}(\langle f^d \rangle) = \{x \in \mathbb{F}_{p^n} | f^d(x) = x\} = \{x \in \mathbb{F}_{p^n} | x^{p^d} = x\} = \mathbb{F}_{p^d}.$$

Théorème 1.17. (Correspondances de Galois). *Soit K/k une extension galoisienne finie, de groupe de Galois $Gal(K/k)$.*
(i) (Premier théorème fondamental). *L'application*

$$\begin{array}{ccc} \{\textit{sous-corps de } K \textit{ contenant } k\} & \longrightarrow & \{\textit{sous-groupes de } Gal(K/k)\} \\ F & \longmapsto & Gal(K/F) \end{array}$$

est une bijection, de bijection réciproque

$$\begin{array}{ccc} \{\textit{sous-groupes de } Gal(K/k)\} & \longrightarrow & \{\textit{sous-corps de } K \textit{ contenant } k\} \\ H & \longmapsto & Inv_K(H) \end{array}.$$

C'est-à-dire,

$$Inv_K(Gal(K/F)) = F, \textit{ pour tout corps } F,\ k \subseteq F \subseteq K,$$
$$Gal(K/Inv_K(H)) = H, \textit{ pour tout sous-groupe } H \textit{ de } Gal(K/k);$$

De plus, on a $[K : F] = |Gal(K/F)|$ et $[K : Inv_K(H)] = |H|$. Enfin ces deux applications sont décroissantes pour l'inclusion :

$$F_1 \subseteq F_2 \implies Gal(K/F_2) \subseteq Gal(K/F_1),$$
$$H_1 \subseteq H_2 \implies Inv_K(H_2) \subseteq Inv_K(H_1);$$

(ii) (Second théorème fondamental). *Soient F/k une sous-extension de K/k et $Gal(K/F)$ le groupe de Galois de l'extension relative. Alors F/k est galoisienne si et seulement si $Gal(K/F)$ est distingué dans $Gal(K/k)$. Dans ce cas, les groupes $Gal(K/k)/Gal(K/F)$ et $Gal(F/k)$ sont isomorphes, l'isomorphisme étant induit par l'homomorphisme de restriction à F*

$$\begin{array}{rccc} \phi : & Gal(K/k) & \longrightarrow & Gal(F/k) \\ & \sigma & \longmapsto & \sigma|_F \end{array}$$

avec noyau $\ker\phi = Gal(K/F)$.

Preuve. Cf. *Extension de corps* par J. Calais [2] (page 124, théorème 7.32, chapitre 7).

□

Remarque. L'extension F/k n'est pas galoisienne en général. Néanmoins, K/F est galoisienne et par multiplicativité du degré, on a :

$$[F : k] = \frac{[K : k]}{[K : F]} = \frac{Gal(K/k)}{Gal(K/F)} = (Gal(K/k) : Gal(K/F)).$$

En résumé, si K/k est une extension galoisienne finie de groupe de Galois $Gal(K/k)$, alors on a une bijection décroissante $F \mapsto Gal(K/F)$, de réciproque $H \mapsto Inv_K(H)$, entre les sous-corps de K contenant k et les sous-groupes de $Gal(K/k)$.

1.2 Topologie générale

Dans ce paragraphe, on rappellera quelques notions importantes et quelques résultats connus de la topologie générale.

Définition 1.18. Soit E un ensemble. On appelle *topologie* sur E toute famille $\tau \in \mathscr{P}(E)$ de parties de E vérifiant les propriétés suivantes :
(i) $\emptyset \in \tau, E \in \tau$;
(ii) τ est stable par union quelconque, i.e., $\forall i \in I, U_i \in \tau \implies \bigcup_{i\in I} U_i \in \tau$;
(iii) τ est stable par intersection finie, i.e., $\forall U, V \in \tau \implies U \cap V \in \tau$.
Le couple (E, τ) est appelé un *espace topologique*, et les éléments de τ sont appelés les *ouverts* de (E, τ).

Exemple 1.6. (i) Sur tout ensemble E on peut définir deux topologies $\tau_1 = \{\emptyset, E\}$, appelée la *topologie grossière*, qui est la topologie la moins fine sur E ; et $\tau_2 = \mathscr{P}(E)$, appelée la *topologie discrète*, qui est la topologie la plus fine sur E ;
(ii) Soit (E, d) un espace métrique. Alors

$$\tau_d = \{U \in \mathscr{P}(E) | \forall x \in U, \exists r > 0, \text{ tel que } B(x, r) \subseteq U\}$$

définit une topologie sur E. On l'appelle la *topologie associée à la métrique d*.

Définition 1.19. Un espace topologique (E, τ) est dit *discret* si τ est la topologie discrète.

Définition 1.20. Soient (E, τ) un espace topologique, $x \in E$ et $V \subseteq E$. On dit que V est un *voisinage de x pour τ*, s'il existe un ouvert $U \in \tau$ tel que $x \in U$ et $U \subseteq V$.

Définition 1.21. (i) Soient $(E_1, \tau_1), (E_2, \tau_2)$ deux espaces topologiques et $f : E_1 \longrightarrow E_2$ une application. Soit $x \in E_1$. On dit que f est *continue en x* si pour tout voisinage V de $f(x)$, il existe un voisinage U de x, tel que $f(U) \subseteq V$;
(ii) Soient $(E_1, \tau_1), (E_2, \tau_2)$ deux espaces topologiques et $f : E_1 \longrightarrow E_2$ une application. On dit que f est *continue sur E_1* si f est continue en tout point x de E_1.

Remarque. f est continue sur E_1 si et seulement si pour tout ouvert U de E_2, l'image réciproque $f^{-1}(U)$ est un ouvert de E_1.

Proposition 1.22. *Soient $(E, \tau), (E', \tau')$ deux espaces topologiques et $f : E \longrightarrow E'$ une application. Alors f est continue si et seulement si $f(\overline{U}) \subseteq \overline{f(U)}$ pour tout $U \subseteq E$.*

Preuve. Notons d'abord que :
$\star$ $f^{-1}(f(U)) \supseteq U$ pour tout $U \subseteq E$. Si f est de plus injective, alors $f^{-1}(f(U)) = U$.
$\star$ $f(f^{-1}(U')) \subseteq U'$ pour tout $U' \subseteq E'$. Si f est de plus surjective, alors $f(f^{-1}(U')) = U'$.
"$\Longrightarrow$" : Pour tout $U \subseteq E$, on a $U \subseteq f^{-1}(f(U)) \subseteq f^{-1}(\overline{f(U)})$. Comme f est continue, $f^{-1}(\overline{f(U)})$ est fermé. On en déduit que $\overline{U} \subseteq \overline{f^{-1}(\overline{f(U)})} = f^{-1}(\overline{f(U)})$. Ainsi $f(\overline{U}) \subseteq f(f^{-1}(\overline{f(U)})) \subseteq \overline{f(U)}$. D'où $\boxed{f(\overline{U}) \subseteq \overline{f(U)}}$.
"$\Longleftarrow$" : Si $f(\overline{U}) \subseteq \overline{f(U)}$ pour tout $U \subseteq E$, montrons que $f^{-1}(F)$ est fermé pour tout fermé F de E. Comme $f(\overline{f^{-1}(F)}) \subseteq \overline{f(f^{-1}(F))} \subseteq \overline{F} = F$, on en déduit que $\overline{f^{-1}(F)} \subseteq f^{-1}(f(\overline{f^{-1}(F)})) \subseteq f^{-1}(F)$. D'où $\overline{f^{-1}(F)} \subseteq f^{-1}(F)$, ainsi $\boxed{\overline{f^{-1}(F)} = f^{-1}(F)}$.
D'où l'équivalence.

□

Définition 1.23. Soient (E, τ) un espace topologique et F un sous-ensemble de E. Alors

$$\tau_F = \{U \cap F | U \in \tau\}$$

définit une topologie sur F. On l'appelle la *topologie induite par τ sur F*, et on appelle (F, τ_F) un *sous-espace topologique* de (E, τ).

Remarque. Si $F_1 \subseteq F_2 \subseteq E$, alors $(\tau_{F_2})_{F_1} = \tau_{F_1}$.

Exemple 1.7. (i) Considérons $[0,1]$ comme un sous-espace topologique de $\mathbb{R}$ et $\mathbb{R}$ muni de la topologie usuelle. Par la définition 1.23, $[0, \frac{1}{2}[$ est un ouvert de $[0,1]$ mais pas un ouvert de $\mathbb{R}$;
(ii) Considérons $]0,1[$ comme un sous-espace topologique de $\mathbb{R}$ et $\mathbb{R}$ muni de la topologie usuelle. Par la définition 1.23, $]0, \frac{1}{2}]$ est un fermé de $]0,1[$ mais pas un fermé de $\mathbb{R}$.

Définition 1.24. Soient (E,τ) un espace topologique et $\sim$ une relation d'équivalence sur E. On dit que $[x] = \{y \in E | x \sim y\}$ est une *classe d'équivalence* de $x \in E$ et que x est un *représentant* de cette classe. On pose

$$E/\sim := \{[x] | x \in E\}$$

et

$$\sigma := \{U \subseteq E/\sim \, | \pi^{-1}(U) \in \tau\}$$

où $\pi : E \longrightarrow E/\sim$ est la surjection canonique. Alors σ est une topologie sur $E/\sim$, on l'appelle la *topologie quotient*. Et on appelle $(E/\sim, \sigma)$ *l'espace quotient*.

Définition 1.25. Un espace topologique (E,τ) est dit *séparé* ou T_2 ou *de Hausdorff* si pour tout couple (x,y) de points distincts, x et y admettent des voisinages disjoints.

Exemple 1.8. (i) Un espace topologique discret (E,τ) est toujours séparé. En effet, pour la topologie discrète, tout point $x \in E$ est naturellement un voisinage de lui-même. Donc si $x \neq y$, on a $\{x\} \in \tau, \{y\} \in \tau$ et $\{x\} \cap \{y\} = \emptyset$. D'où (E,τ) est séparé ;
(ii) Un espace métrique (E,d) est un espace séparé pour la topologie associée à la métrique τ_d. En effet, pour deux points distincts x et y dans E, $d(x,y) \neq 0$. Posons $r = \frac{d(x,y)}{3}$, alors $x \in B(x,r), y \in B(y,r)$ et $B(x,r) \cap B(y,r) = \emptyset$. D'où (E,τ_d) est séparé.

Définition 1.26. Soit (E,τ) un espace topologique. Une famille d'ouverts $(U_i)_{i\in I}$ de E est appelée un *recouvrement en ouverts de* E si $\bigcup_{i\in I} U_i = E$. Un espace topologique (E,τ) est dit *compact* s'il est séparé et si de tout recouvrement en ouverts de E on peut extraire un sous-recouvrement fini de E.

Exemple 1.9. Dans l'espace topologique $\mathbb{R}^n$ muni de la topologie usuelle, $K \subseteq \mathbb{R}^n$ est un compact si et seulement si K est un fermé borné de $\mathbb{R}^n$.

Proposition 1.27. *Un espace topologique (E,τ) est compact si et seulement si il est séparé et si pour toute famille de fermés $(F_i)_{i\in I}$ de E, on a :*

$$\Big[\bigcap_{i\in J} F_i \neq \emptyset \text{ pour toute partie finie } J \subseteq I\Big] \Longrightarrow \Big[\bigcap_{i\in I} F_i \neq \emptyset\Big] \qquad (*)$$

Preuve. "$\Longrightarrow$" : Si (E,τ) est compact, il est par définition séparé.
Supposons que $\bigcap_{i\in I} F_i = \emptyset$, alors $E = \bigcup_{i\in I} F_i^c$ et dont $(F_i^c)_{i\in I}$ est un recouvrement en ouverts de E. Comme E est compact, il existe un $n \in \mathbb{N}$ et $i_1, \cdots, i_n \in I$ tels que $E = \bigcup_{k=1}^{n} F_{i_k}^c$. On en déduit que $\bigcap_{k=1}^{n} F_{i_k} = \emptyset$. Ceci est une contradiction.
"$\Longleftarrow$" : L'hypothèse $(*)$ est équivalente à :

$$\Big[\bigcap_{i\in I} F_i = \emptyset\Big] \Longrightarrow \Big[\text{il existe une partie finie } J \subseteq I \text{ telle que } \bigcap_{i\in J} F_i = \emptyset\Big]$$

ce qui est équivalent à :

$$\Big[\bigcup_{i\in I} F_i^c = E\Big] \Longrightarrow \Big[\text{il existe une partie finie } J \subseteq I \text{ telle que } \bigcup_{i\in J} F_i^c = E\Big]$$

ce qui revient à la définition d'un compact.

□

Proposition 1.28. *Soient (E,τ) un espace topologique séparé et K un sous-ensemble compact de E. Alors K est fermé.*

Preuve. Dire que l'ensemble K est fermé équivaut à dire que l'ensemble K^c est ouvert. Soit $x \in K^c$. Pour tout $y \in K$, il existe un voisinage ouvert U_y de x et un voisinage ouvert V_y de y tels que $U_y \cap V_y = \emptyset$ car E est séparé. Alors $(V_y)_{y\in K}$ est un recouvrement en ouverts de K qui admet un sous-recouvrement fini $(V_{y_i})_{i=1}^n$ de K car K est compact.
Posons $U = \bigcap_{i=1}^{n} U_{y_i}$ et $V = \bigcap_{i=1}^{n} V_{y_i}$, alors U est un voisinage ouvert de x, V est un voisinage ouvert de K (un ouvert contenant K) et $U \cap V = \emptyset$. On en déduit que $x \in U \subseteq K^c$. D'où K est fermé.

□

Proposition 1.29. *Soient (E,τ) un espace topologique compact et F un sous-ensemble fermé de E. Alors (F,τ_F) est un espace topologique compact.*

Preuve. E est un espace topologique compact, donc séparé. Tout sous-espace d'un espace séparé est séparé. On en déduit que F est séparé.
Soit $(U_i)_{i\in I}$ un recouvrement en ouverts de F, c'est-à-dire, $F = \bigcup_{i\in I} U_i$. Montrons qu'il existe un sous-recouvrement fini de F.
Par la définition 1.23, il existe une famille d'ouverts $(V_i)_{i\in I}$ de E telle que $U_i = V_i \cap F$ pour tout $i \in I$. On en déduit que $F \subseteq \bigcup_{i\in I} V_i$ et ainsi, $\Big(\bigcup_{i\in I} V_i\Big)^c \subseteq F^c$. Alors :

$$\Big(\bigcup_{i\in I} V_i\Big) \cup F^c \subseteq E = \Big(\bigcup_{i\in I} V_i\Big) \cup \Big(\bigcup_{i\in I} V_i\Big)^c \subseteq \Big(\bigcup_{i\in I} V_i\Big) \cup F^c.$$

On en déduit que $E = \Big(\bigcup_{i\in I} V_i\Big) \cup F^c$. Notons que F est un fermé de E, donc F^c est un ouvert de E. Ainsi $\{F^c, V_i | i \in I\}$ forme un recouvrement en ouverts de E. Comme E est compact, il existe un sous-recouvrement fini $\{F^c, V_i | i = 1, 2, \cdots, m\}$ de E, c'est-à-dire, $E = \Big(\bigcup_{i=1}^{m} V_i\Big) \cup F^c$. Ainsi $F \subseteq \bigcup_{i=1}^{m} V_i$. D'où $F = \bigcup_{i=1}^{m} (V_i \cap F) = \bigcup_{i=1}^{m} U_i$.

□

Définition 1.30. Soient (E,τ) un espace topologique et x un élément de E. On pose

$$\mathscr{V}(x) = \{V \subseteq E | V \text{ est un voisinage de } x\}$$

l'ensemble des voisinages de x. Soit $\mathscr{U}(x) \subseteq \mathscr{V}(x)$, on dit que $\mathscr{U}(x)$ est une *base de voisinages de x* si pour tout $V \in \mathscr{V}(x)$, il existe un $U \in \mathscr{U}(x)$ tel que $U \subseteq V$.

Exemple 1.10. (i) Considérons $\mathbb{R}$ muni de la topologie usuelle. $\mathscr{U}(x) = \Big\{\big]-\frac{1}{n}, \frac{1}{n}\big[\Big| n \in \mathbb{N}^*\Big\}$ forme une base de voisinages de 0. En effet, pour tout voisinage ouvert U de 0, il existe un $r > 0$ tel que $]-r, r[\subseteq U$. Soit $n \in \mathbb{N}$ tel que $\frac{1}{n} < r$. Alors $]-\frac{1}{n}, \frac{1}{n}[\subseteq U$. D'où $\mathscr{U}(x)$ est

une base de voisinages de 0 ;
(ii) Plus généralement, si (E,d) est un espace métrique et si τ_d est la topologie associée à la métrique d, alors pour tout $x \in E$, $\mathscr{U}(x) = \left\{B(x,\frac{1}{n})\middle| n \in \mathbb{N}^*\right\}$ forme une base de voisinages de x ;
(iii) Pour un espace topologique discret E, tout singleton $\{x\}$ forme une base de voisinages de x.

Définition 1.31. Soient (E,τ) un espace topologique et $\mathscr{B}$ un sous-ensemble de τ. On pose

$$\overline{\mathscr{B}} = \{U \in \tau | U \text{ est la réunion d'éléments de } \mathscr{B}\}.$$

$\mathscr{B}$ est appelé une *base de* τ si $\tau = \overline{\mathscr{B}}$.

Remarque. Une base de τ est naturellement une base de voisinages de tout point x de E. Réciproquement, si un sous-ensemble $\mathscr{B}$ de τ contient une base de voisinages de x pour tout $x \in E$, alors $\mathscr{B}$ forme une base de τ. On a donc la proposition suivante :

Proposition 1.32. *Soient (E,τ) un espace topologique et $\mathscr{B}$ un sous-ensemble de τ. Alors $\mathscr{B}$ forme une base de τ si et seulement si*

$$\forall U \in \tau, \forall x \in U, \exists V_x \in \mathscr{B} \text{ tel que } x \in V_x \subseteq U.$$

Preuve. "$\Longrightarrow$" : Supposons que $\mathscr{B}$ est une base de τ et que U est un ouvert de E. Par la définition 1.31, $U = \bigcup_{i\in I} U_i$ avec $(U_i)_{i\in I} \subseteq \mathscr{B}$. On en déduit que pour tout $x \in U$, il existe un $U_j \in \mathscr{B}$ tel que $x \in U_j \subseteq U$.
"$\Longleftarrow$" : Supposons que $\mathscr{B}$ est un sous-ensemble de τ tel que pour tout ouvert U de E et pour tout élément x de E, il existe un $V_x \in \mathscr{B}$ tel que $x \in V_x \subseteq U$. Montrons que $\mathscr{B}$ forme une base de τ, c'est-à-dire, montrons que U est la réunion d'éléments de $\mathscr{B}$. Or, il est clair que $\boxed{\bigcup_{x\in U} V_x = U}$. D'où le résultat.

□

Exemple 1.11. (i) Considérons $\mathbb{R}$ muni de la topologie usuelle. Alors $\mathscr{B} = \{]a,b[| a,b \in \mathbb{R}\}$ forme une base de $\mathbb{R}$;
(ii) Plus généralement, soient (E,d) un espace métrique et τ_d la topologie associée à la métrique d. Alors $\mathscr{B} = \{B(x,r) | x \in E, r \in \mathbb{R}^+\}$ forme une base de (E,τ_d) ;
(iii) Pour un espace topologique discret (E,τ), tout ensemble de parties réduites à un seul point forme une base de τ.

Définition 1.33. Soient $((E_i,\tau_i))_{i\in I}$ une famille d'espaces topologiques et $E = \prod_{i\in I} E_i$ le produit cartésien des E_i. On pose

$$\mathscr{B} = \left\{ \prod_{i\in I} A_i \in E \middle| \forall i \in I, A_i \in \tau_i, \text{ et } A_i = E_i \text{ sauf pour un nombre fini de } i \right\}$$

et

$$\tau = \overline{\mathscr{B}}.$$

Alors τ définit une topologie sur E appelée la *topologie produit* sur E, et on appelle (E,τ) *l'espace produit* des E_i. Les éléments de $\mathscr{B}$ sont appelés les *ouverts élémentaires de* E.

Remarque. (i) Par définition, $\mathscr{B}$ forme une base de la topologie produit ;
(ii) La topologie produit définie ci-dessus est la topologie la moins fine sur E rendant les projections canoniques $p_j : E \to E_j$ continues. En effet, soit U_j un ouvert de E_j. Alors $p_j^{-1}(U_j) = U_j \times \prod_{i \neq j} E_i$, on en déduit que $p_j^{-1}(U_j)$ est ouvert. Donc tous les p_j sont continues. Supposons maintemnant que τ' est une topologie sur E rendant les p_j continues. Soit $\prod_{i \in I} A_i \in \tau$. Alors il existe un sous-ensemble fini F de I tel que $A_j \in \tau_j$ pour $j \in F$ et $A_i = E_i$ pour $i \in I - F$. Alors $p_j^{-1}(A_j) \in \tau'$ pour $j \in F$ car p_j est continue. On en déduit que $\prod_{i \in I} A_i = \prod_{j \in F} A_j \times \prod_{i \in I - F} E_i = \bigcap_{j \in F} (A_j \times \prod_{i \neq j} E_i) = \bigcap_{j \in F} p_j^{-1}(A_j) \in \tau'$. D'où $\tau \subseteq \tau'$.

Théorème 1.34. (Tychonoff). *Soit $((E_i, \tau_i))_{i \in I}$ une famille d'espaces topologiques compacts. Alors $\prod_{i \in I} E_i$ muni de la topologie produit est compact.*

Remarque. Ce théorème est équivalent à l'axiome du choix.

Preuve. Il y a plusieurs démonstrations de ce théorème. Par exemple, la démonstration utilisant les ultrafiltres due à Bourbaki [1] (page 63, théorème 3) ; la démonstration élémentaire due à Munkres [3] (page 234, théorème 37.3, chapitre 5).

□

Définition 1.35. Un espace topologique (E, τ) est dit *connexe* s'il n'est pas la réunion de deux ouverts non vides disjoints.

Remarque. On a les équivalences suivantes :
(i) E est connexe ;
(ii) Les sous-ensembles à la fois ouverts et fermés de E ne sont d'autres que $\emptyset$ et E.

Proposition 1.36. *Soient $(E_1, \tau_1), (E_2, \tau_2)$ deux espaces topologiques et $f : E_1 \longrightarrow E_2$ une application continue. Si U est une partie connexe de E_1, alors $f(U)$ est une partie connexe de E_2.*

Preuve. Soit O une partie à la fois ouverte et fermée de $f(U)$, alors $f^{-1}(O)$ est une partie à la fois ouverte et fermée de U car f est continue. Comme U est connexe, on en déduit que $f^{-1}(O) = \emptyset$ ou $f^{-1}(O) = U$. Ainsi $O = \emptyset$ ou $O = f(U)$. D'où $f(U)$ est connexe.

□

Définition 1.37. Soient (E, τ) un espace topologique et x un élément de E. Alors la réunion de toutes les parties connexes contenant x est connexe, c'est la plus grande partie connexe contenant x. On la note $C(x)$ et l'appelle la *composante connexe de x dans E.*

Proposition 1.38. *Soient (E, τ) un espace topologique et $x \in E$. Soient $C(x)$ la composante connexe de x et V un voisinage à la fois ouvert et fermé de x. Alors $C(x) \subseteq V$.*

Preuve. Comme V est un sous-ensemble à la fois ouvert et fermé de E, on en déduit que $C(x) \cap V$ est un sous-ensemble à la fois ouvert et fermé de $C(x)$. De plus, $C(x)$ est connexe. D'après la remarque de la définition 1.35, $C(x) \cap V = \emptyset$ ou $C(x) \cap V = C(x)$. Or, $x \in C(x) \cap V$ par hypothèse. On en déduit que $C(x) \cap V = C(x)$. D'où $\boxed{C(x) \subseteq V}$.

□

Remarque. Si V est une partie à la fois ouverte et fermée de E, alors soit $C(x) \cap V = \emptyset$, soit $C(x) \subseteq V$.

Définition 1.39. Un espace topologique (E, τ) est dit *totalement discontinu* si la composante connexe de chaque point x dans E est l'ensemble $\{x\}$ réduit à ce point.

Remarque. (i) D'après la proposition 1.38, on en déduit que la composante connexe d'un point est contenue dans l'intersection de ses voisinages à la fois ouverts et fermés. Donc, si pour tout $x \in E$ l'intersection ci-dessus est égale à $\{x\}$, alors E est totalement discontinu ; (ii) Un sous-espace topologique d'un espace topologique totalement discontinu est totalement discontinu. En effet, si $U \subseteq E$ et si E est totalement discontinu, alors, en notant $C_U(x)$ la composante connexe de x dans U et $C(x)$ la composante connexe de x dans E pour $x \in U$, on a $C_U(x) = C(x) \cap U = \{x\}$. Ainsi U est totalement discontinu.

Exemple 1.12. (i) Un espace topologique discret (E, τ) est toujours totalement discontinu. En effet, pour la topologie discrète, tout singleton $\{x\}$ est à la fois ouvert et fermé. (ii) L'ensemble des entiers $\mathbb{Z}$ est discret dans $\mathbb{R}$, donc totalement discontinu. En effet, soit $n \in \mathbb{Z}$. Alors $\{n\} = \{n\} \cap [n - \frac{1}{2}, n + \frac{1}{2}] = \{n\} \cap]n - \frac{1}{2}, n + \frac{1}{2}[$, on en déduit que $\{n\}$ est à la fois ouvert et fermé dans $\mathbb{Z}$. Les composantes connexes dans $\mathbb{Z}$ sont exactement les $\{n\}$ avec $n \in \mathbb{Z}$;

2 Théorie de Galois de Degré Infini

2.1 Groupe topologique

La clé pour approcher la théorie de Galois infinie est de munir le groupe de Galois $Gal(K/k)$ d'une topologie (à savoir : la topologie de *Krull*) qui est compatible avec sa structure de groupe. Dans ce cas, le groupe de Galois $Gal(K/k)$ deviendra un *groupe topologique*. Dans ce paragraphe, on donnera les notions importantes concernant le groupe topologique et on étudiera ses propriétés fondamendales.

Définition 2.1. On appelle *groupe topologique* tout groupe multiplicatif $(G, \cdot)$ muni d'une topologie pour laquelle les applications $(x, y) \mapsto x \cdot y$ et $x \mapsto x^{-1}$ sont continues. On écrit aussi xy comme le produit de x et y.

Remarque. Un sous-groupe F de G est aussi un groupe topologique muni de la topologie induite par G.

Exemple 2.1. Tout groupe discret (c'est-à-dire, muni de la topologie discrète) est un groupe topologique.

Lemme 2.2. *Soient G un groupe topologique. Alors l'application*

$$\begin{array}{rccc} f: & G \times G & \longrightarrow & G \times G \\ & (x, y) & \longmapsto & (x, y^{-1}) \end{array}$$

est continue.

Preuve. Soit V un voisinage du couple (x, y^{-1}). Montrons qu'il existe un voisinage U du couple (x, y) tel que $f(U) \subseteq V$. Par la topologie produit, il existe un voisinage V_1 de x et un voisinage V_2 de y^{-1} tels que $V_1 \times V_2 \subseteq V$. Posons $U_1 = V_1$ et $U_2 = g^{-1}(V_2)$, où $g(y) = y^{-1}$ qui est par définition continue. Ainsi, $U_1 \times U_2$ est un voisinage du couple (x, y) et on a :

$$\begin{aligned} f(U_1 \times U_2) &= \{f(x, y) | (x, y) \in U_1 \times U_2\} = \{(x, y^{-1}) | (x, y) \in U_1 \times U_2\} \\ &= \{(x, g(y)) | (x, y) \in U_1 \times U_2\} = U_1 \times g(U_2). \end{aligned}$$

Or, $U_1 \times g(U_2) = V_1 \times g(g^{-1}(V_2)) \subseteq V_1 \times V_2 \subseteq V$. D'où f est continue.

□

Théorème 2.3. *Un groupe $(G, \cdot)$ muni d'une topologie est un groupe topologique si et seulement si l'application $(x, y) \mapsto x \cdot y^{-1}$ est continue.*

Preuve. "$\Longrightarrow$" : D'après le lemme 2.2, on sait que l'application $(x, y) \mapsto (x, y^{-1})$ est continue. De plus, par définition, $(x, y^{-1}) \mapsto x \cdot y^{-1}$ est continue. Ainsi l'application $(x, y) \mapsto x \cdot y^{-1}$ est continue par composition d'applications continues.
"$\Longleftarrow$" : On sait que l'injection canonique $y \mapsto (1_G, y)$ est continue, et que l'application $(1_G, y) \mapsto 1_G \cdot y^{-1} = y^{-1}$ est continue par hypothèse. Ainsi l'application $y \mapsto y^{-1}$ est continue par composition d'applications continues.
D'après le lemme 2.2, l'application $(x, y) \mapsto (x, y^{-1})$ est continue. De plus, l'application $(x, y^{-1}) \mapsto x \cdot (y^{-1})^{-1} = x \cdot y$ est continue par hypothèse. Donc $(x, y) \mapsto x \cdot y$ est continue par composition d'applications continues.
Ainsi G est un groupe topologique.

□

Proposition 2.4. *Soit G un groupe topologique. Alors, les translations $x \mapsto a \cdot x$ et $x \mapsto x \cdot a$ sont des homéomorphismes.*

Preuve. On sait que l'injection canonique $x \mapsto (a, x)$ est continue. Comme $(G, \cdot)$ est un groupe topologique, l'application $(a, x) \mapsto a \cdot x$ est continue pour tout a fixé. On en déduit que l'application $x \mapsto a \cdot x$ est continue pour tout a fixé par composition d'applications continues. Par un raisonnement similaire, on en déduit que les applications $x \mapsto x \cdot a$, $x \mapsto a^{-1} \cdot x$ et $x \mapsto x \cdot a^{-1}$ sont continues pour tout a fixé. Or, $x \mapsto a^{-1} \cdot x$ est l'application réciproque de $x \mapsto a \cdot x$ et $x \mapsto x \cdot a^{-1}$ est l'application réciproque de $x \mapsto x \cdot a$. D'où les homéomorphismes.

□

Proposition 2.5. *Soient G un groupe topologique et U un voisinage ouvert de l'élément unité 1_G. Alors aU et Ua sont des voisinages ouverts de a pour tout $a \in G$.*

Preuve. Comme $1_G \in U$, $a \in aU$. D'après la proposition 2.4, l'application $x \mapsto a \cdot x$ est un homéomorphisme. Ainsi aU est un ouvert. De même, Ua est aussi un ouvert.

□

Remarque. Soient U et H des sous-groupes de G. Si U est ouvert, alors UH et HU sont des ouverts de G. En effet, $UH = \bigcup_{h \in H} Uh$ et $HU = \bigcup_{h \in H} hU$, donc UH et HU sont ouverts comme union d'ouverts.

On sait que pour trouver une base d'un espace topologique (E, τ), il suffit de trouver une base de voisinages de tout point $x \in E$. D'après la proposition 2.5, si E est un groupe topologique, il suffit de trouver une base de voisinages de l'élément unité 1_E.

Proposition 2.6. *Soient G un groupe topologique et H un sous-groupe de G. Alors $\overline{H}$ est un sous-groupe de G. Si H est de plus distingué dans G, alors $\overline{H}$ est aussi distingué dans G.*

Preuve. Posons

$$\begin{array}{rccc} f: & G \times G & \longrightarrow & G \\ & (x, y) & \longmapsto & x \cdot y^{-1}, \end{array}$$

qui est continue par le théorème 2.3. Il suffit de montrer que $f(\overline{H} \times \overline{H}) \subseteq \overline{H}$.
Comme H est un sous-groupe de G, on a $f(H \times H) \subseteq H$. De plus, $f(\overline{H \times H}) \subseteq \overline{f(H \times H)}$ par la proposition 1.22. On en déduit que

$$f(\overline{H} \times \overline{H}) \subseteq f(\overline{H \times H}) \subseteq \overline{f(H \times H)} \subseteq \overline{H}.$$

D'où $f(\overline{H} \times \overline{H}) \subseteq \overline{H}$, ainsi $\overline{H}$ est un sous-groupe de G.
Supposons maintenant que H est normal et posons

$$\begin{array}{rccc} g_a: & G & \longrightarrow & G \\ & x & \longmapsto & a \cdot x \cdot a^{-1}, \end{array}$$

alors $g_a(H) \subseteq H$ pour tout $a \in G$ car H est un sous-groupe normal. Par la proposition 2.4, g_a est un homéomorphisme de G dans G. Ainsi, d'après la proposition 1.22, on a $g_a(\overline{H}) \subseteq \overline{g_a(H)} \subseteq \overline{H}$ pour tout $a \in G$. D'où $\overline{H}$ est normal.

□

Proposition 2.7. *Si $(G_i)_{i \in I}$ est une famille de groupes topologiques, alors $G = \prod_{i \in I} G_i$ est un groupe topologique (muni de la topologie produit).*

Preuve. Posons

$$\begin{array}{rccc} f_i: & G_i \times G_i & \longrightarrow & G_i \\ & (x_i^1, x_i^2) & \longmapsto & x_i^1 \cdot x_i^2 \end{array}$$

pour $i \in I$ et

$$\begin{array}{rccc} f: & G \times G & \longrightarrow & G \\ & ((x_i^1)_{i\in I}, (x_i^2)_{i\in I}) & \longmapsto & (x_i^1 \cdot x_i^2)_{i\in I}. \end{array}$$

Posons p_i la projection canonique de G dans G_i et $p_i \times p_i$ la projection canonique de $G \times G$ dans $G_i \times G_i$. Remarquons que l'on a $p_i \circ f = f_i \circ (p_i \times p_i)$ pour tout $i \in I$. Autrement dit, le diagramme suivant

$$\begin{array}{ccc} G \times G & \xrightarrow{f} & G \\ {\scriptstyle p_i \times p_i}\downarrow & & \downarrow{\scriptstyle p_i} \\ G_i \times G_i & \xrightarrow[f_i]{} & G_i \end{array}$$

est commutatif pour tout $i \in I$. En effet, si $((g_i^1)_{i\in I}, (g_i^2)_{i\in I}) \in G \times G$ et si $j \in I$, alors

$$\begin{aligned} (p_j \circ f)((x_i^1)_{i\in I}, (x_i^2)_{i\in I}) &= p_j((x_i^1 \cdot x_i^2)_{i\in I}) = x_j^1 \cdot x_j^2, \\ (f_j \circ (p_j \times p_j))((x_i^1)_{i\in I}, (x_i^2)_{i\in I}) &= f_j(x_j^1, x_j^2) = x_j^1 \cdot x_j^2. \end{aligned}$$

D'où $p_i \circ f = f_i \circ (p_i \times p_i)$ pour tout $i \in I$. Comme G_i est un groupe topologique pour tout $i \in I$, f_i est continue pour tout $i \in I$. On en déduit que $p_i \circ f$ est continue pour tout $i \in I$.

Soit U un ouvert de G. On peut supposer sans perte de généralité que $U = \prod_{i\neq k} G_i \times \prod_{k=1}^{n} U_k$ avec U_k un ouvert de G_k, alors $U = \bigcap_{k=1}^{n} p_k^{-1}(U_k)$. Ainsi :

$$f^{-1}(U) = f^{-1}\left(\bigcap_{k=1}^{n} p_k^{-1}(U_k)\right) = \bigcap_{k=1}^{n} f^{-1}(p_k^{-1}(U_k)) = \bigcap_{k=1}^{n} (p_k \circ f)^{-1}(U_k).$$

Or, $(p_k \circ f)^{-1}(U_k)$ est ouvert car $p_k \circ f$ est continue. On en déduit que $f^{-1}(U)$ est un ouvert comme intersection finie d'ouverts. D'où f est continue.

Posons maintenant

$$\begin{array}{rccc} g_i: & G_i & \longrightarrow & G_i \\ & x_i & \longmapsto & x_i^{-1} \end{array}$$

pour $i \in I$ et

$$\begin{array}{rccc} g: & G & \longrightarrow & G \\ & (x_i)_{i\in I} & \longmapsto & (x_i^{-1})_{i\in I}. \end{array}$$

Avec la même raisonnement, on peut montrer que g est continue. D'où G est un groupe topologique.

□

Lemme 2.8. *Soient G un groupe topologique et H un sous-groupe distingué de G. Alors la surjection canonique $\pi : G \longrightarrow G/H$ est une application ouverte, c'est-à-dire, $\pi(U)$ est ouvert pour tout ouvert U de G.*

Preuve. Soit U un ouvert dans G. Il suffit de montrer que $\pi^{-1}(\pi(U))$ est ouvert dans G. On a :

$$\begin{aligned} \pi^{-1}(\pi(U)) &= \{x \in G | \pi(x) \in \pi(U)\} = \{x \in G | xH \in \pi(U)\} \\ &= \{x \in G | \exists y \in U, xH = yH\} = \{x \in G | \exists y \in U, x \in yH\} \\ &= \{x \in G | x \in \bigcup_{y\in U} yH\} = \bigcup_{y\in U} yH = UH. \end{aligned}$$

D'où $\pi^{-1}(\pi(U))$ est ouvert par la proposition 2.5.

□

Corollaire 2.9. *Soit $(G_i)_{i\in I}$ une famille de groupes topologiques et $(H_i)_{i\in I}$ une famille de sous-groupes distingués de G_i. Alors la surjection canonique*

$$\pi = \prod_{i\in I}\pi_i : \prod_{i\in I} G_i \longrightarrow \prod_{i\in I}(G_i/H_i)$$

est une application ouverte, c'est-à-dire, $\pi(U)$ est ouvert pour tout ouvert U de $\prod_{i\in I} G_i$.

Preuve. Notons que $f\Big(\bigcup_{i\in I} U_i\Big) = \bigcup_{i\in I} f(U_i)$, donc il suffit de montrer que $\pi(U)$ est ouvert pour tout ouvert élémentaire U de $\prod_{i\in I} G_i$. Posons $U = \prod_{i\neq k} G_i \times \prod_{k=1}^{n} U_k$, alors :

$$\pi(U) = \prod_{i\neq k}\pi_i(G_i) \times \prod_{k=1}^{n}\pi_k(U_k) = \prod_{i\neq k}(G_i/H_i) \times \prod_{k=1}^{n}\pi_k(U_k).$$

D'après le lemme 2.8, π est ouverte.

□

Proposition 2.10. *Soient G un groupe topologique et H un sous-groupe distingué de G. Alors G/H est un groupe topologique.*

Preuve. Posons

$$\begin{array}{rccc} f: & G\times G & \longrightarrow & G \\ & (x,y) & \longmapsto & x\cdot y \end{array}$$

et

$$\begin{array}{rccc} \overline{f}: & G/H\times G/H & \longrightarrow & G/H \\ & (\overline{x},\overline{y}) & \longmapsto & \overline{x}\cdot\overline{y}. \end{array}$$

Posons π la surjection canonique de G dans G/H et $\pi\times\pi$ la surjection canonique de $G\times G$ dans $G/H\times G/H$. Remarquons que pour tout $i\in I$, on a $\pi\circ f = \overline{f}\circ(\pi\times\pi)$. Autrement dit, le diagramme suivant

$$\begin{array}{ccc} G\times G & \xrightarrow{\ f\ } & G \\ {\scriptstyle \pi\times\pi}\downarrow & & \downarrow{\scriptstyle \pi} \\ G/H\times G/H & \xrightarrow[\ \overline{f}\ ]{} & G/H \end{array}$$

est commutatif. En effet, si $(x,y)\in G\times G$ alors

$$(\pi\circ f)(x,y) = \pi(x\cdot y) = \overline{x\cdot y} = \overline{x}\cdot\overline{y} = \overline{f}(\overline{x},\overline{y}) = (\overline{f}\circ(\pi\times\pi))(x,y).$$

D'où $\pi\circ f = \overline{f}\circ(\pi\times\pi)$. Soit U un ouvert de G/H. Alors :

$$(\pi\times\pi)^{-1}\Big(\overline{f}^{-1}(U)\Big) = (\overline{f}\circ(\pi\times\pi))^{-1}(U) = (\pi\circ f)^{-1}(U).$$

Comme G est un groupe topologique, f est continue, et donc $\pi\circ f$ est continue. On en déduit que $(\pi\times\pi)^{-1}\Big(\overline{f}^{-1}(U)\Big)$ est ouvert. Comme $\pi\times\pi$ est surjective et ouverte (corollaire 2.9), on en déduit que $\overline{f}^{-1}(U) = (\pi\times\pi)\Big((\pi\times\pi)^{-1}\Big(\overline{f}^{-1}(U)\Big)\Big)$ est ouvert. D'où $\overline{f}$ est continue. Posons maintenant

$$\begin{array}{rccc} g: & G & \longrightarrow & G \\ & x & \longmapsto & x^{-1} \end{array}$$

et

$$\begin{array}{rccc} \overline{g}: & G/H & \longrightarrow & G/H \\ & \overline{x} & \longmapsto & \overline{x}^{-1}. \end{array}$$

Avec la même raisonnement, on peut montrer que g est continue. D'où G/H est un groupe topologique.

□

En résumé, l'adhérence (resp. produit, quotient) d'un groupe topologique est aussi un groupe topologique.

Définition 2.11. Soient G, G' deux groupes topologiques.
(i) Un *homomorphisme de groupes topologiques* est un homomorphisme de groupes $f : G \longrightarrow G'$ qui est continu ;
(ii) Un *isomorphisme de groupes topologiques* est un isomorphisme de groupes $f : G \longrightarrow G'$ ainsi qu'un homéomorphisme.

Proposition 2.12. *Soient G, G' des groupes topologiques et $f : G \longrightarrow G'$ un homomorphisme de groupes topologiques. Si f est une application ouverte, alors $G/\ker f \cong f(G)$ en tant que groupes topologiques.*

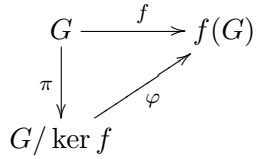
Preuve. On sait que l'isomorphisme de groupes $G/\ker f \cong f(G)$ est donné par

$$\begin{array}{rccc} \varphi: & G/\ker f & \longrightarrow & f(G) \\ & \overline{x} & \longmapsto & f(x), \end{array}$$

d'application réciproque

$$\begin{array}{rccc} \psi: & f(G) & \longrightarrow & G/\ker(f) \\ & f(x) & \longmapsto & \overline{x}. \end{array}$$

Il suffit de montrer que φ et ψ sont continues.
Posons $\pi : G \longrightarrow G/\ker f$ la surjection canonique, alors $f = \varphi \circ \pi$ par le théorème de factorisation. Autrement dit, le diagramme suivant



est commutatif. Soit U un ouvert de $f(G)$, alors

$$\pi^{-1}(\varphi^{-1}(U)) = (\varphi \circ \pi)^{-1}(U) = f^{-1}(U).$$

Donc $\pi^{-1}(\varphi^{-1}(U))$ est ouvert car f est continue, d'où $\varphi^{-1}(U)$ est ouvert par la définition de la topologie quotient. On en déduit que φ est continue.
De plus, soit V un ouvert de $G/\ker f$, alors $\pi^{-1}(V)$ est ouvert par définition. On a

$$\psi^{-1}(V) = \varphi(V) = \varphi(\pi(\pi^{-1}(V))) = f(\pi^{-1}(V))$$

car π est surjective. Ainsi $\psi^{-1}(V)$ est ouvert car $\pi^{-1}(V)$ est ouvert et f est une application ouverte. D'où ψ est continue. Conclusion : φ est un homéomorphisme.

□

2.2 Système inverse et limite projective

L'autre outil essentiel pour établir la correspondance de Galois est la *limite projective*.

Définition 2.13. Soient I un ensemble d'indices, muni d'une relation $\leq$ de pré-ordre (c'est-à-dire, réflexive et transitive) et $(S_i)_{i\in I}$ une famille d'ensembles (resp. espaces topologiques, groupes, groupes topologiques). Pour tout couple $(i,j) \in I \times I$ tel que $i \leq j$, soit $(\pi_{ji} : S_j \to S_i)_{i\leq j}$ une famille d'applications (resp. applications continues, homomorphismes, homomorphismes continus) vérifiant les conditions suivantes :
(i) $\pi_{ii} = id_{S_i}$ pour tout $i \in I$;
(ii) $\pi_{ki} = \pi_{ji} \circ \pi_{kj}$ pour tout $k, j, i \in I$ tels que $i \leq j \leq k$.
C'est-à-dire, le diagramme suivant

$$\begin{array}{ccc} S_k & \xrightarrow{\pi_{kj}} & S_j \\ & \searrow^{\pi_{ki}} & \downarrow{\scriptstyle \pi_{ji}} \\ & & S_i \end{array}$$

est commutatif. On dit que le système $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ est un *système inverse* d'ensembles (resp. espaces topologiques, groupes, groupes topologiques) et d'applications (resp. applications continues, homomorphismes, homomorphismes continus).

Proposition 2.14. *Soit $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ un système inverse d'ensembles (resp. espaces topologiques, groupes, groupes topologiques) et d'applications (resp. applications continues, homomorphismes, homomorphismes continus). Alors il existe un ensemble (resp. espace topologique, groupe, groupe topologique) S et une famille d'applications $(\pi_i : S \to S_i)_{i\in I}$ (resp. applications continues, homomorphismes, homomorphismes continus) tels que :*
(i) $\pi_i = \pi_{ji} \circ \pi_j$ lorsque $i \leq j$ (compatiblité) ;
(ii) Si S' est un ensemble (resp. espace topologique, groupe, groupe topologique) et si pour tout $i \in I$, $\pi'_i : S' \to S_i$ est une application (resp. application continue, homomorphismes, homomorphisme continu) vérifiant (i), alors il existe une unique application (resp. application continue, homomorphisme, homomorphisme continu) $\theta : S' \to S$ telle que pour tout $i \in I$, $\pi_i \circ \theta = \pi'_i$ (propriété universelle).

Preuve. (i) Posons

$$S = \left\{ (s_i)_{i\in I} \in \prod_{i\in I} S_i \,\middle|\, \pi_{ji}(s_j) = s_i, \forall i \leq j \right\}$$

et $\pi_i = p_i|_S$ où p_i est la restriction de la $i^{\text{ème}}$ projection canonique de $\prod_{i\in I} S_i$. Par définition de π_i, $\pi_i(s) = s_i$ pour tout $i \in I$. On en déduit que :

$$\forall i \in I, \boxed{\pi_{ji} \circ \pi_j(s) = \pi_{ji}(s_j) = s_i = \pi_i(s)}.$$

$\star$ Supposons que $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ est un système inverse d'ensembles et d'applications, alors π_i est bien une application pour tout $i \in I$.
$\star$ Supposons que $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ est un système inverse d'espaces topologiques et d'applications continues. Montrons que $(\pi_i)_{i\in I}$ est une famille d'applications continues. Pour cela, il suffit de montrer que pour tout ouvert $U \subseteq S_i$, $\pi_i^{-1}(U)$ est un ouvert.
Remarquons que si f est une application de E dans F et si U est un sous-ensemble de F, alors $(f|_A)^{-1}(U) = f^{-1}(U) \cap A$. Ainsi :

$$\forall U \subseteq S_i \text{ ouvert}, \pi_i^{-1}(U) = (p_i|_S)^{-1}(U) = p_i^{-1}(U) \cap S = \Big(\prod_{j\in I} A_j\Big) \cap S,$$

où $A_j = S_j$ pour tout $j \neq i$ et $A_i = U$. Or, S est inclus dans $\prod_{i\in I} S_i$ et $\prod_{j\in I} A_j$ est un ouvert de $\prod_{i\in I} S_i$ puisqu'il y a un nombre fini de A_i tels que $A_i \neq S_i$. Ainsi, $\left(\prod_{j\in I} A_j\right) \cap S$ est un ouvert de S, et donc π_i est continue.
⋆ Supposons que $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ est un système inverse de groupes et de homomorphismes. Montrons que $(\pi_i)_{i\in I}$ est une famille de homomorphismes. Soient $s = (s_i)_{i\in I}$ et $t = (t_i)_{i\in I}$ deux éléments dans S. Alors

$$s \cdot t = (s_i \cdot t_i)_{i\in I} \text{ et } p_i(s \cdot t) = s_i \cdot t_i = p_i(s) \cdot p_i(t).$$

Ainsi π_i est un homomorphisme pour tout $i \in I$.
⋆ Supposons que $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ est un système inverse de groupes topologiques et de homomorphismes continus. Alors π_i est un homomorphisme de groupes topologiques pour tout $i \in I$ grâce à ce qui précède.
(ii) Supposons que S' est un ensemble (resp. espace topologique, groupe, groupe topologique) et que pour tout $i \in I$, $\pi'_i : S' \to S_i$ est une application (resp. application continue, homomorphisme, homomorphisme continu) telle que $\pi'_i = \pi_{ji} \circ \pi'_j$ lorsque $i \leq j$. Posons

$$\begin{array}{rccc} \theta : & S' & \longrightarrow & \prod_{i\in I} S_i \\ & s' & \longmapsto & (\pi'_i(s'))_{i\in I}. \end{array}$$

Alors :
⋆ θ est une application (resp. application continue, homomorphisme, homomorphisme continu) de S' dans S. En effet :

$$\forall s' \in S',\, \theta(s') = (\pi'_i(s'))_{i\in I} \in S \iff \forall s' \in S',\, \forall i \leq j,\, \pi_{ji} \circ \pi'_j(s') = \pi'_i(s')\,;$$

ce qui est vrai par hypothèse.
⋆ $\pi_i \circ \theta = \pi'_i$ pour tout $i \in I$. En effet, $\pi_i \circ \theta(s') = \pi_i \circ (\pi'_j(s'))_{j\in I} = \pi'_i(s')$ pour tout $i \in I$.
Montrons maintenant l'unicité de l'application (resp. application continue, homomorphisme, homomorphisme continu) θ. Soit $\theta' : S' \to S$ une application (resp. application continue, homomorphisme, homomorphisme continu) telle que pour tout $i \in I$, $\pi_i \circ \theta' = \pi'_i$. Notons que $\pi_i = p_i|_S$ où $p_i : \prod_{i\in I} S_i \to S_i$ est la projection canonique et que $t = (p_i(t))_{i\in I}$ pour tout $t \in \prod_{i\in I} S_i$. Ainsi, comme $\theta'(s') \in S \subseteq \prod_{i\in I} S_i$ pour tout $s' \in S$ et comme $\pi_i = p_i$ sur S, on en déduit que pour tout $s' \in S'$,

$$\theta'(s') = (p_i(\theta'(s')))_{i\in I} = (\pi_i(\theta'(s')))_{i\in I} = (\pi'_i(s'))_{i\in I} = \theta(s').$$

D'où $\boxed{\theta = \theta'}$.

□

Définition 2.15. Soit $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ un système inverse d'ensembles (resp. espaces topologiques, groupes, groupes topologiques) et d'applications (resp. applications continues, homomorphismes, homomorphismes continus), et soit $(S, (\pi_i)_{i\in I})$ un couple avec S un ensemble (resp. espace topologique, groupe, groupe topologique) et π_i une application (resp. application continue, homomorphisme, homomorphisme continu) vérifiant les propriétés dans la proposition 2.14. On dit que le couple $(S, (\pi_i)_{i\in I})$ est la *limite inverse* ou *limite projective* de la famille $(S_i)_{i\in I}$ par rapport aux $(\pi_{ji})_{i\leq j}$, et on note $S = \varprojlim_I S_i$ ou simplement $S = \varprojlim S_i$ s'il n'y a pas d'ambiguïté.

Remarque. (i) π_i n'est pas nécessairement la restriction de la $i^{\text{ème}}$ projection canonique ;
(ii) D'après la démonstration de la proposition 2.14, la limite inverse S est éventuellement l'ensemble vide. On montrera plus tard (2.22) que si l'ensemble I est filtrant à droite (2.21) et si $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ est un système inverse d'espaces topologiques compacts non vides et d'applications continues, alors la limite inverse $S = \varprojlim S_i$ est un compact non vide. En particulier, si chaque S_i est un ensemble fini muni de la topologie discrète et si chaque π_{ji} est continue, alors la limite inverse $S = \varprojlim S_i$ est non vide.

La proposition 2.14 montre l'existence de la limite inverse. En fait, la limite inverse est unique dans le sens suivant :

Proposition 2.16. *Soient $(S, (\pi_i)_{i\in I})$ et $(S', (\pi'_i)_{i\in I})$ deux limites inverses de la famille $(S_i)_{i\in I}$ par rapport aux $(\pi_{ji})_{i\leq j}$. Alors il existe une unique bijection (resp. homéomorphisme, isomorphisme, isomorphisme de groupes topologiques) $\sigma : S \to S'$ telle que*

$$\pi'_i \circ \sigma = \pi_i, \forall i \in I. \qquad (*)$$

Preuve. Comme les deux systémes inverses d'ensembles (resp. espaces topologiques, groupes, groupes topologiques) et d'applications (resp. applications continues, homomorphismes, homomorphismes continus) $(S, (\pi_i)_{i\in I})$ et $(S', (\pi'_i)_{i\in I})$ satisfont les deux propriétés de la proposition 2.14, on en déduit que :
(i) Si $i \leq j$, alors

$$\pi_i = \pi_{ji} \circ \pi_j \text{ et } \pi'_i = \pi_{ji} \circ \pi'_j. \qquad (1)$$

(ii) Comme S' est un ensemble (resp. espace topologique, groupe, groupe topologique) et comme pour tout $i \in I$, $\pi'_i : S' \to S_i$ est une application (resp. application continue, homomorphisme, homomorphisme continu) vérifiant (1), il existe une unique application (resp. application continue, homomorphisme, homomorphisme continu) $\theta : S' \to S$ telle que

$$\pi_i \circ \theta = \pi'_i, \forall i \in I.$$

De même, il existe une unique application (resp. application continue, homomorphisme, homomorphisme continu) $\theta' : S \to S'$ telle que

$$\pi'_i \circ \theta' = \pi_i, \forall i \in I.$$

On remarque que :

$$\forall i \in I,\ \pi_i = \pi'_i \circ \theta' = (\pi_i \circ \theta) \circ \theta' = \pi_i \circ (\theta \circ \theta'),$$
$$\forall i \in I,\ \pi'_i = \pi_i \circ \theta = (\pi'_i \circ \theta') \circ \theta = \pi'_i \circ (\theta' \circ \theta).$$

Ainsi on peut en déduire que $\theta \circ \theta' = id_S$ et $\theta' \circ \theta = id_{S'}$ par la propriété de la limite inverse. Donc l'application (resp. application continue, homomorphisme, homomorphisme continu) θ' est une bijection (resp. homéomorphisme, isomorphisme, isomorphisme de groupes topologiques) de S dans S' vérifiant $(*)$ pour tout $i \in I$ et est unique. C'est la σ recherchée.

□

Comme la limite inverse est "unique" d'après la proposition 2.16, on va toujours considérer la limite inverse S comme un sous-ensemble (resp. sous-espace, sous-groupe, sous-groupe topologique) de $\prod_{i\in I} S_i$ et les π_i comme les restrictions de la projection canonique dans la suite de ce paragraphe.

Proposition 2.17. *Soit $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ et $((S'_i)_{i\in I}, (\pi'_{ji})_{i\leq j})$ deux systèmes inverses d'ensembles (resp. espaces topologiques, groupes, groupes topologiques) et d'applications (resp. applications continues, homomorphismes, homomorphismes continus). Pour tout $i \in I$ soit $h_i : S_i \longrightarrow S'_i$ une application (resp. application continue, homomorphisme, homomorphisme continu) compatible avec les π_{ji}, c'est-à-dire,*

$$h_i \circ \pi_{ji} = \pi'_{ji} \circ h_j, \text{ lorsque } i \leq j. \tag{2}$$

Alors il existe une unique application (resp. application continue, homomorphisme, homomorphisme continu) $h : \varprojlim S_i \longrightarrow \varprojlim S'_i$ compatible avec les π_i, c'est-à-dire, $h_i \circ \pi_i = \pi'_i \circ h$ pour tout $i \in I$.

Preuve. Posons

$$\begin{array}{rccc} h: & S = \varprojlim S_i & \longrightarrow & \prod\limits_{i\in I} S'_i \\ & s & \longmapsto & ((h_i \circ \pi_i)(s))_{i\in I}, \end{array}$$

alors h est une application (resp. application continue, homomorphisme, homomorphisme continu).

$\star$ Montrons que $h(s) \in S' = \varprojlim S'_i$ pour tout $s \in S = \varprojlim S_i$. Pour tout $i \leq j$,

$$\pi'_{ji}((h_j \circ \pi_j)(s_j)) = ((\pi'_{ji} \circ h_j) \circ \pi_j)(s) \overset{2}{=} ((h_i \circ \pi_{ji}) \circ \pi_j)(s) = (h_i \circ \pi_i)(s).$$

D'où $h(s) \in S'$ pour tout $s \in S$.

$\star$ Montrons que $h_i \circ \pi_i = \pi'_i \circ h$ pour tout $i \in I$. Soit $s \in S$. Alors

$$(\pi'_i \circ h)(s) = \pi'_i(h(s)) = \pi'_i(((h_j \circ \pi_j)(s))_{j\in I}) = (h_i \circ \pi_i)(s).$$

D'où $h_i \circ \pi_i = \pi'_i \circ h$ pour tout $i \in I$.

Montrons maintenant l'unicité de h. Soit $h' : S \longrightarrow S'$ une application (resp. application continue, homomorphisme, homomorphisme continu) vérifiant $h_i \circ \pi_i = \pi'_i \circ h'$. Alors

$$\pi'_i \circ h' = h_i \circ \pi_i = \pi'_i \circ h.$$

On en déduit que $\pi'_i \circ h' = \pi'_i \circ h$, et donc $h' = h$ par la propriété universelle de la limite inverse.

□

Grâce à la proposition 2.17, on obtient une catégorie de limites inverses : les objets sont des systèmes inverses $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ qui induisent les limites inverses $(S, (\pi_i)_{i\in I})$; les homomorphismes entre deux systèmes inverses $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ et $((S_i)'_{i\in I}, (\pi'_{ji})_{i\leq j})$ sont des applications $h_i : S_i \longrightarrow S'_i$ rendant le diagramme

$$\begin{array}{ccc} S_j & \xrightarrow{h_j} & S'_j \\ {\scriptstyle \pi_{ji}}\downarrow & & \downarrow{\scriptstyle \pi'_{ji}} \\ S_i & \xrightarrow[h_i]{} & S'_i \end{array}$$

commutatif, qui induisent les applications $h : S \longrightarrow S'$ entre deux limites inverses rendant le diagramme

$$\begin{array}{ccc} \varprojlim S_i & \overset{h}{\dashrightarrow} & \varprojlim S'_i \\ {\scriptstyle \pi_i}\downarrow & & \downarrow{\scriptstyle \pi'_i} \\ S_i & \xrightarrow[h_i]{} & S'_i \end{array}$$

commutatif ; la composition de homomorphismes est donnée par la composition de diagrammes commutatifs :

$$\begin{array}{ccccc} S_j & \xrightarrow{h_j} & S'_j & \xrightarrow{h'_j} & S''_j \\ \downarrow{\scriptstyle \pi_{ji}} & & \downarrow{\scriptstyle \pi'_{ji}} & & \downarrow{\scriptstyle \pi''_{ji}} \\ S_i & \xrightarrow[h_i]{} & S'_i & \xrightarrow[h'_i]{} & S''_i. \end{array}$$

Enfin, on a bien une identité :

$$\begin{array}{ccc} S_j & \xrightarrow{id_{S_j}} & S_j \\ \downarrow{\scriptstyle \pi_{ji}} & & \downarrow{\scriptstyle \pi_{ji}} \\ S_i & \xrightarrow[id_{S_i}]{} & S_i \end{array}$$

et la composition est associative :

$$\begin{array}{ccccccc} S_j & \xrightarrow{h_j} & S'_j & \xrightarrow{h'_j} & S'_j & \xrightarrow{h''_j} & S'''_j \\ \downarrow{\scriptstyle \pi_{ji}} & & \downarrow{\scriptstyle \pi'_{ji}} & & \downarrow{\scriptstyle \pi''_{ji}} & & \downarrow{\scriptstyle \pi'''_{ji}} \\ S_i & \xrightarrow[h_i]{} & S'_i & \xrightarrow[h'_i]{} & S''_i & \xrightarrow[h''_i]{} & S'''_i. \end{array}$$

Proposition 2.18. *Soit $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ un système inverse d'espaces topologiques séparés et d'applications continues. Alors $S = \varprojlim S_i$ est un sous-espace fermé de $\prod_{i\in I} S_i$. En particulier, ceci est vrai lorsque chaque S_i est un ensemble fini (muni de la topologie discrète).*

Preuve. Dire que l'ensemble S est fermé équivaut à dire que l'ensemble S^c est ouvert, ce qui équivaut également à dire que pour tout élément s dans S^c, il existe un ouvert $U \in \mathscr{V}(s)$ tel que $U \cap S = \emptyset$. De même, on sait que S est l'ensemble des familles $s = (s_i)_{i\in I}$ telles que $\pi_{ji}(s_j) = s_i$ pour tout $i \leq j$. Ainsi, si $s \notin S$, alors il existe un j avec $i \leq j$ tel que $\pi_{ji}(s_j) \neq s_i$. De plus, $\pi_{ji}(s_j)$ et s_i appartiennent tous les deux à S_i, et comme S_i est séparé, on en déduit qu'il existe deux ouverts $U_1 \in \mathscr{V}(s_i)$ et $U_2 \in \mathscr{V}(\pi_{ji}(s_j))$ tels que $U_1 \cap U_2 = \emptyset$.
Posons $W = \prod_{i\in I} A_i$, où $A_i = U_1$, $A_j = \pi_{ji}^{-1}(U_2)$ et $A_k = S_k$ pour tout $k \notin \{i, j\}$. Alors W est un ouvert de $\prod_{i\in I} A_i$ car U_1, U_2 sont ouverts dans S_i et l'application π_{ji} est continue.
$\star$ Montrons que $s \in W$. Pour tout $k \notin \{i, j\}$, on sait que $s_k \in S_k$. De plus, comme $U_1 \in \mathscr{V}(s_i)$, on en déduit par définition que $s_i \in U_1 = A_i$. De même, comme $U_2 \in \mathscr{V}(\pi_{ji}(s_j))$, on en déduit par définition que $s_j \in \pi_{ji}^{-1}(U_1) = A_j$. Ainsi, $\boxed{s \in W}$.
$\star$ Montrons que $W \cap S = \emptyset$. On a la série d'équivalences suivante :

$$\begin{aligned} [t \in W] &\iff [\forall k \in I,\, t_k \in A_k] \iff [\forall k \neq i, j,\, t_k \in S_k,\, t_i \in V_2 \text{ et } t_j \in V_1] \\ &\iff [\forall k \neq i, j,\, t_k \in S_k,\, t_i \in U_2 \text{ et } \pi_{ji}(t_j) \in U_1] \overset{U_1\cap U_2=\emptyset}{\iff} [t_i \neq \pi_{ji}(t_j)] \iff [t \in S^c]. \end{aligned}$$

Ainsi, $\boxed{W \cap S = \emptyset}$.

□

Proposition 2.19. *Soit $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ un système inverse d'espaces topologiques compacts et d'applications continues. Alors, $S = \varprojlim S_i$ est un espace topologique compact.*

En particulier, ceci est vrai lorsque chaque S_i est un ensemble fini (muni de la topologie discrète).

Preuve. Quelque soit $i \in I$, si S_i est compact, alors par définition S_i est séparé. De plus, les π_{ji} sont continues. Donc d'après la proposition 2.18, $S = \varprojlim S_i$ est un sous-ensemble fermé de $\prod_{i\in I} S_i$ qui est compact car tous les S_i sont compacts (théorème de Tychonoff). Ainsi, d'après la proposition 1.29, S est compact.

□

Proposition 2.20. *Soit $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ un système inverse d'espaces topologiques totalement discontinus et d'applications continues. Alors $S = \varprojlim S_i$ est un espace topologique totalement discontinu. En particulier, ceci est vrai lorsque chaque S_i est un ensemble fini (muni de la topologie discrète).*

Preuve. Soient $s = (s_i)_{i\in I} \in \prod_{i\in I} S_i$ et $C(s)$ la composante connexe de s dans $\prod_{i\in I} S_i$. Comme les π_i sont continues, on en déduit que $\pi_i(C(s))$ est connexe pour tout $i \in I$. Or, comme S_i est totalement discontinu et $s_i = \pi_i(s) \in \pi_i(C(s))$, on en déduit que $\pi_i(C(s)) = s_i$ pour tout $i \in I$. D'où $\boxed{C(s) = \{s\}}$.

□

Définition 2.21. Soit I un ensemble d'indices pré-ordonné. On dit que I est *filtrant à droite* si pour tout $i, j \in I$ il existe un $k \in I$ tel que $i \leq k$ et $j \leq k$.

Exemple 2.2. L'ensemble $\mathbb{Z}$ muni de la relation d'ordre $\leq$ est filtrant à droite. En particulier, tout ensemble totalement ordonné est filtrant à droite.

Proposition 2.22. *Soit $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ un système inverse d'espaces topologiques compacts non vides et d'applications continues avec I filtrant à droite. Alors $S = \varprojlim S_i$ est un espace topologique compact non vide. En particulier, ceci est vrai lorsque chaque S_i est un ensemble fini et non vide (muni de la topologie discrète).*

Preuve. D'après la proposition 2.19, il suffit de montrer que $S = \varprojlim S_i$ est non vide.
Posons $M_{kj} = \{s \in \prod_{i\in I} S_i | \pi_{kj}(s_k) = s_j\}$ avec $k, j \in I$ et $k > j$, alors $S = \bigcap_{k>j} M_{kj}$.

⋆ Montrons que M_{kj} est fermé dans $\prod_{i\in I} S_i$ pour tout $k > j$. Posons $N_{kj} = \{(s_k, s_j) \in S_k \times S_j | \pi_{kj}(s_k) = s_j\}$, alors $(N_{kj}, \{\pi_k, \pi_j\})$ est la limite inverse du système inverse

$$(\{S_k, S_j\}, \{id_{S_k}, \pi_{kj}, id_{S_j}\}).$$

Comme S_k, S_j sont compacts et $id_{S_k}, \pi_{kj}, id_{S_j}$ sont continues, d'après la proposition 2.19, N_{kj} est un compact de $S_k \times S_j$. Or, comme $S_k \times S_j$ est compact et donc séparé, on en déduit que N_{kj} est fermé. Notons que $M_{kj} = (p_k \times p_j)^{-1}(N_{kj})$, où $p_k \times p_j : \prod_{i\in I} S_i \longrightarrow S_k \times S_j$ est la projection canonique qui est continue. On en déduit que M_{kj} est fermé.

⋆ Montrons que $\bigcap_{k>j} M_{kj} \neq \emptyset$. Comme S est compact, d'après la proposition 1.27, il suffit de montrer que pour tout $n \in \mathbb{N}$ et pour tout $j_1 \leq k_1, \cdots, j_n \leq k_n$, $\bigcap_{i=1}^{n} M_{k_i,j_i} \neq \emptyset$.

Comme I est filtrant à droite, il existe un $l \in I$ tel que $k_r \leq l, r = 1, \cdots, n$. Fixons un $s_l \in S_l$, et posons

$$s_i = \begin{cases} s_l & \text{si } i = l; \\ \pi_{l,j_r}(s_l) & \text{si } i = j_r, r = 1, \cdots, n; \\ \pi_{l,k_r}(s_l) & \text{si } i = k_r, r = 1, \cdots, n; \\ s_i \text{ quelconque} & \text{si } i \notin \{l, j_1, \cdots, j_n, k_1, \cdots, k_n\}. \end{cases}$$

Alors $\pi_{k_i,j_i}(s_{k_i}) = \pi_{k_i,j_i}(\pi_{l,k_i}(s_l)) = \pi_{l,j_i}(s_l) = s_{j_i}$ pour $i = 1, \cdots, n$. On en déduit que $s = (s_i)_{i\in I} \in \bigcap_{k>j} M_{kj}$. D'où $\bigcap_{k>j} M_{kj} \neq \emptyset$. Conclusion : $\boxed{S \neq \emptyset}$.

□

En résumé, d'après les propositions 2.19, 2.20 et 2.22, si l'ensemble I est filtrant à droite et si $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ est un système inverse d'espaces topologiques compacts (resp. compacts non vides, totalement discontinus) et d'applications continues. Alors $S = \varprojlim S_i$ est un espace topologique compact (resp. compact non vide, totalement discontinu). En particulier, ceci est vrai lorsque chaque S_i est un ensemble fini (muni de la topologie discrète). On sait que les ouverts élémentaires $\bigcap_{i\in J} p_i^{-1}(V_i)$, avec $J \subseteq I$ fini et V_i ouvert dans S_i, forment une base de la topologie produit de $\prod_{i\in I} S_i$. La proposition suivante montre que la structure de la topologie induite de la limite inverse $S = \varprojlim S_i$ est plus simple que la topologie produit, dont les éléments dans la base se réduisent à la forme $p_i^{-1}(V_i)$ avec $i \in I$ et V_i ouvert dans S_i.

Proposition 2.23. *Si I est filtrant à droite et si $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ est un système inverse d'espaces topologiques et d'applications continues, alors*

$$\mathscr{B} = \{\pi_i^{-1}(V_i) | i \in I, V_i \text{ un ouvert de } S_i\}$$

forme une base de $S = \varprojlim S_i$. En particulier, soit $s \in S$, alors

$$\mathscr{B}_s = \{\pi_i^{-1}(V_i) | i \in I, V_i \text{ un ouvert de } S_i \text{ contenant } s_i\}$$

forme une base de voisinages de s.

Preuve. Posons τ_S la topologie induite de S. D'après la proposition 1.32, il suffit de montrer que $\mathscr{B} \subseteq \tau_S$ et que pour tout ouvert $U \in \tau_S$ et tout $s \in U$ il existe un $\pi_i^{-1}(V_i) \in \mathscr{B}$ tel que $s \in \pi_i^{-1}(V_i) \subseteq U$.
⋆ Montrons que $\mathscr{B} \subseteq \tau_S$. Comme les π_i sont continues, on en déduit que pour tout ouvert $V_i \subseteq S_i$, $\pi_i^{-1}(V_i)$ est un ouvert de S. D'où $\boxed{\mathscr{B} \subseteq \tau_S}$.
⋆ Montrons que pour tout ouvert U de S et tout x dans U il existe un $\pi_i^{-1}(V_i) \in \mathscr{B}$ tel que $x \in \pi_i^{-1}(V_i) \subseteq U$.
Soit U un ouvert de S. Par la topologie induite, il existe un ouvert W de $\prod_{i\in I} S_i$ tel que $U = W \cap S$. Ainsi, par la topologie produit, il existe un ouvert élémentaire O de $\prod_{i\in I} S_i$ tel que $s \in O \subseteq W$. Par conséquent, $s \in O \cap S \subseteq U$.
Supposons que $O = \prod_{k=1}^{m} V_{i_k} \times \prod_{j\neq i_k} S_j$ avec V_{i_k} ouverts de S_{i_k} pour $1 \leq k \leq m$. On a alors : $O = \bigcap_{k=1}^{m} (V_{i_k} \times \prod_{j\neq i_k} S_j) = \bigcap_{k=1}^{m} p_{i_k}^{-1}(V_{i_k})$. On en déduit que :

$$\bigcap_{k=1}^{m} \pi_{i_k}^{-1}(V_{i_k}) = \bigcap_{k=1}^{m} (p_{i_k}^{-1}(V_{i_k}) \cap S) = \left(\bigcap_{k=1}^{m} p_{i_k}^{-1}(V_{i_k}) \right) \cap S = O \cap S \subseteq U.$$

Comme I est filtrant à droite, il existe un indice $j \in I$ tel que $i_k \leq j$ pour $1 \leq k \leq m$. Posons maintenant $V_j = \bigcap_{k=1}^{m} \pi_{j,i_k}^{-1}(V_{i_k})$. Comme les applications π_{j,i_k} sont continues et

comme les V_{i_k} sont des ouverts de S_{i_k}, les $\pi_{j,i_k}^{-1}(V_{i_k})$ sont des ouverts de S_j. Ainsi, comme V_j est une intersection finie d'ouverts de S_j, c'est un ouvert de S_j.
De plus $\pi_j^{-1}(V_j) = \pi_j^{-1}\left(\bigcap_{k=1}^{m} \pi_{j,i_k}^{-1}(V_{i_k})\right) \subseteq \bigcap_{k=1}^{m} \pi_j^{-1}(\pi_{j,i_k}^{-1}(V_{i_k}))$. Or, comme $\pi_j^{-1} \circ \pi_{j,i_k}^{-1} = (\pi_{j,i_k} \circ \pi_j)^{-1}$ et $\pi_{j,i_k} \circ \pi_j = \pi_i$, on en déduit que : $\bigcap_{k=1}^{m} \pi_j^{-1}(\pi_{j,i_k}^{-1}(V_{i_k})) = \bigcap_{k=1}^{m} \pi_{i_k}^{-1}(V_{i_k}) \subseteq U$.
D'où $\pi_j^{-1}(V_j) \subseteq U$.
Enfin, comme $s \in O = \prod_{k=1}^{m} V_{i_k} \times \prod_{j \neq i_k} S_j$, $s_{i_k} \in V_{i_k}$ pour $1 \leq k \leq m$, et donc $\pi_{j,i_k}(s_j) = s_{i_k} \in V_{i_k}$. On en déduit que $s_j \in \bigcap_{k=1}^{m} \pi_{j,i_k}^{-1}(V_{i_k}) = V_j$. D'où $\boxed{s \in \pi_j^{-1}(V_j) \subseteq U}$.

□

Si (E_1, τ_1) et (E_2, τ_2) sont deux espaces topologiques et si $\mathscr{B}_1$ (resp. $\mathscr{B}_2$) est une base de τ_1 (resp. τ_2), alors $\mathscr{B}_1 \times \mathscr{B}_2 := \{B_1 \times B_2 | B_1 \in \tau_1, B_2 \in \tau_2\}$ forme une base de l'espace produit $E_1 \times E_2$. Ceci montre le corollaire suivant :

Corollaire 2.24. *Si I est filtrant à droite et si $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ est un système inverse d'espaces topologiques et d'applications continues, alors*

$$\mathscr{B} = \{\pi_i^{-1}(V_i) \times \pi_i^{-1}(U_i) | i \in I, V_i, U_i \text{ sont des ouverts de } S_i\}$$

forme une base de l'espace produit $S \times S$.

Proposition 2.25. *Soient I un ensemble filtrant à droite et $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ un système inverse d'espaces topologiques et d'applications continues. Soit U un sous-ensemble de $S = \varprojlim S_i$. Alors*

$$s = (s_i)_{i\in I} \in \overline{U} \iff s_i \in \overline{\pi_i(U)} \text{ pour tout } i \in I. \qquad (*)$$

Preuve. La propriété $(*)$ est équivalente à :

$$\overline{U} = \bigcap_{i\in I} \pi_i^{-1}(\overline{\pi_i(U)}). \qquad (**)$$

"$\subseteq$" : Comme $U \subseteq \pi_i^{-1}(\pi_i(U)) \subseteq \pi_i^{-1}(\overline{\pi_i(U)})$ pour tout $i \in I$, on en déduit que $U \subseteq \bigcap_{i\in I} \pi_i^{-1}(\overline{\pi_i(U)})$. Or, π_i est continue pour tout $i \in I$, et donc $\pi_i^{-1}(\overline{\pi_i(U)})$ est fermé pour tout $i \in I$. Ainsi $\bigcap_{i\in I} \pi_i^{-1}(\overline{\pi_i(U)})$ est fermé. D'où $\boxed{\overline{U} \subseteq \bigcap_{i\in I} \pi_i^{-1}(\overline{\pi_i(U)})}$.
"$\supseteq$" : Si $s \in \bigcap_{i\in I} \pi_i^{-1}(\overline{\pi_i(U)})$, alors $\pi_i(s) \in \overline{\pi_i(U)}$ pour tout $i \in I$. Montrons que $s \in \overline{U}$. Soit V un voisinage de s. D'après la proposition 2.23, on peut, sans perte de généralité, supposer que V est de la forme $\pi_i^{-1}(V_i)$ avec $i \in I$ et V_i un ouvert de S_i. Il suffit de montrer que $\pi_i^{-1}(V_i) \cap U \neq \emptyset$.
Comme $\pi_i^{-1}(V_i)$ est un voisinage de s, V_i est un voisinage de $\pi_i(s)$. Donc $V_i \cap \pi_i(U) \neq \emptyset$ car $\pi_i(s) \in \overline{\pi_i(U)}$. Ainsi :

$$\pi_i^{-1}(V_i) \cap U \subseteq \pi_i^{-1}(V_i) \cap \pi_i^{-1}(\pi_i(U)) = \pi_i^{-1}(V_i \cap \pi_i(U)) \neq \emptyset.$$

D'où $\boxed{\overline{U} \supseteq \bigcap_{i\in I} \pi_i^{-1}(\overline{\pi_i(U)})}$.

□

Remarque. L'implication "$\Longrightarrow$" est toujours vraie, mais la réciproque est fausse dans le cas général. Par exemple, considérons le sous-ensemble $U = \{(0,1),(1,0)\}$ dans l'espace produit $\mathbb{R}^2$. On a $(1,1) \in \overline{p_i(U)}$ pour $i = 1,2$, mais $(1,1) \notin U$.

2.3 Groupe de Galois en dimension infini

La normalité d'une extension s'étendant au cas infini, on dira qu'une extension est galoisienne si elle est normale et séparable. Soit K/k une extension galoisienne. Posons :

$$\mathscr{G} := \{F | F \text{ un sous-corps de } K \text{ tel que } F/k \text{ est une extension galoisienne finie}\}.$$

On munit une relation d'ordre $\leq$ sur l'ensemble $\mathscr{G}$ de la manière suivante :

$$F_1 \leq F_2 \Longleftrightarrow F_1 \subseteq F_2.$$

Alors :
(i) $F \leq F$ pour tout $F \in \mathscr{G}$ (réflexivité) ;
(ii) si $F_1 \leq F_2, F_2 \leq F_3$, alors $F_1 \leq F_3$ (transitivité) ;
(iii) si $F_1 \leq F_2, F_2 \leq F_1$, alors $F_1 = F_2$ (antisymétrie).
Ainsi $\mathscr{G}$ est un ensemble ordonné.

Proposition 2.26. *L'ensemble $\mathscr{G}$ défini ci-dessus est filtrant à droite. De plus, on a $K = \bigcup_{F \in \mathscr{G}} F$.*

Preuve. Soient F_1 et F_2 deux extensions galoisiennes finies de k. Alors F_1F_2 est une extension galoisienne finie de k. En effet, soient $P_1 \in k[x]$ et $P_2 \in k[x]$ tels que F_1 est le corps de décomposition de P_1 sur k et F_2 est le corps de décomposition de P_2 sur k. Alors F_1F_2 est le corps de décomposition de P_1P_2 sur k, et on en déduit que F_1F_2/k est normale. De plus, F_1F_2/k est séparable car K/k l'est. Enfin, F_1F_2/k est finie car $[F_1F_2 : k] = [F_1F_2 : F_1][F_1 : k] \leq [F_2 : k][F_1 : k] < \infty$. D'où F_1F_2/k est galoisienne finie.
Montrons que $K = \bigcup_{F \in \mathscr{G}} F$. Il est clair que $K \supseteq \bigcup_{F \in \mathscr{G}} F$. Réciproquement, soit $x \in K$. Alors x est algébrique sur k car K/k est une extension algébrique, il admet donc un polynôme minimal $Irr_k(x) \in k[x]$. Ainsi le corps de décomposition de $Irr_k(x)$ est une extension galoisienne finie de k.

□

Pour tout $F_1, F_2 \in \mathscr{G}$ avec $F_1 \leq F_2$, posons :

$$\begin{array}{rccc} \rho_{F_2F_1} : & Gal(F_2/k) & \longrightarrow & Gal(F_1/k) \\ & \sigma & \longmapsto & \sigma|_{F_1} \end{array}$$

l'homomorphisme de restriction. De même, pour tout $F \in \mathscr{G}$, posons :

$$\begin{array}{rccc} \rho_{KF} : & Gal(K/k) & \longrightarrow & Gal(F/k) \\ & \sigma & \longmapsto & \sigma|_{F} \end{array}$$

l'homomorphisme de restriction. Pour chaque $F \in \mathscr{G}$, on munit le groupe de Galois $Gal(F/k)$ de la topologie discrète, ainsi les homomorphismes $\rho_{F_2F_1}$ sont continus.

Proposition 2.27. *Le système $((Gal(F/k))_{F \in \mathscr{G}}, (\rho_{F_2F_1})_{F_1 \leq F_2})$ est un système inverse de groupes topologiques et de homomorphismes continus.*

Preuve. Par définition, il suffit de montrer que :
(i) Pour tout $F \in \mathscr{G}$, $\rho_{FF} = id_{Gal(F/k)}$. On a :

$$\rho_{FF}(\sigma) = \sigma|_F = \sigma$$

pour tout $\sigma \in Gal(F/k)$. D'où $\boxed{\rho_{FF} = id_{Gal(F/k)}}$.
(ii) Pour tout $F_1, F_2, F_3 \in \mathscr{G}$ avec $F_1 \subseteq F_2 \subseteq F_3$, $\rho_{F_2F_1} \circ \rho_{F_3F_2} = \rho_{F_3F_1}$. On a :

$$(\rho_{F_2F_1} \circ \rho_{F_3F_2})(\sigma) = \rho_{F_2F_1}(\rho_{F_3F_2}(\sigma)) = \rho_{F_2F_1}(\sigma|_{F_2}) = (\sigma|_{F_2})|_{F_1} = \sigma|_{F_1} = \rho_{F_3F_1}(\sigma)$$

pour tout $\sigma \in Gal(F_3/k)$. D'où $\boxed{\rho_{F_2F_1} \circ \rho_{F_3F_2} = \rho_{F_3F_1}}$.

□

D'après la proposition 2.14, il existe une limite inverse $(\varprojlim Gal(F/k), (\rho_F)_{F\in\mathscr{G}})$ de la famille $(Gal(F/k))_{F\in\mathscr{G}}$, par rapport aux homomorphismes continus $(\rho_{F_2F_1})_{F_1\leq F_2}$, où $\varprojlim Gal(F/k)$ est un groupe topologique et $\rho_F : Gal(K/k) \longrightarrow Gal(F/k)$ est un homomorphisme continu pour tout $F \in \mathscr{G}$.
On verra tout de suite que le groupe de Galois $Gal(K/k)$ est isomorphe (en tant que groupes) à la limite inverse $\varprojlim Gal(F/k)$, on peut ainsi le munir d'une topologie (la topologie de Krull) et l'identifie comme un sous-espace topologique de l'espace produit $\prod_{F\in\mathscr{G}} Gal(F/k)$.

Théorème 2.28. $(Gal(K/k), (\rho_{KF})_{F\in\mathscr{G}}) \cong (\varprojlim Gal(F/k), (\rho_F)_{F\in\mathscr{G}})$ *(en tant que groupes).*

Preuve. D'après la proposition 2.14, il suffit de montrer que :
(i) Pour tout $F_1, F_2 \in \mathscr{G}$ avec $F_1 \subseteq F_2$, $\rho_{KF_1} = \rho_{F_2F_1} \circ \rho_{KF_2}$. On a :

$$(\rho_{F_2F_1} \circ \rho_{KF_2})(\sigma) = \rho_{F_2F_1}(\rho_{KF_2}(\sigma)) = \rho_{F_2F_1}(\sigma|_{F_2}) = (\sigma|_{F_2})|_{F_1} = \sigma|_{F_1} = \rho_{KF_1}(\sigma)$$

pour tout $\sigma \in Gal(K/k)$. D'où $\boxed{\rho_{KF_1} = \rho_{F_2F_1} \circ \rho_{KF_2}}$.
(ii) Si G'_K est un groupe et si pour tout $F \in \mathscr{G}$, $\rho'_{KF} : G'_K \longrightarrow Gal(F/k)$ est un homomorphisme tel que $\rho'_{KF_1} = \rho_{F_2F_1} \circ \rho'_{KF_2}$ lorsque $F_1 \subseteq F_2$, alors il existe un unique homomorphisme $\rho : G'_K \longrightarrow Gal(K/k)$ tel que pour tout $F \in \mathscr{G}$, $\rho_{KF} \circ \rho = \rho'_{KF}$.
Posons :

$$\begin{array}{rccc} \rho : & G'_K & \longrightarrow & Gal(K/k) \\ & \sigma & \longmapsto & \rho(\sigma), \end{array}$$

où $\rho(\sigma)(x) = \rho'_{KF}(\sigma)(x)$ si $x \in F$ avec $F \in \mathscr{G}$. $\rho(\sigma)$ est bien défini. En effet, si $x \in F_1$ et $x \in F_2$ avec $F_1, F_2 \in \mathscr{G}$, alors il existe un $F_3 \in \mathscr{G}$ tel que $F_1 \subseteq F_3$ et $F_2 \subseteq F_3$ (notons que $\mathscr{G}$ est filtrant à droite). Alors :

$$\rho'_{KF_1}(\sigma)(x) \overset{F_1\subseteq F_3}{=} (\rho_{F_3F_1} \circ \rho'_{KF_3})(\sigma)(x) = (\rho'_{KF_3}(\sigma)|_{F_1})(x) \overset{x\in F_1}{=} \rho'_{KF_3}(\sigma)(x),$$

et

$$\rho'_{KF_2}(\sigma)(x) \overset{F_2\subseteq F_3}{=} (\rho_{F_3F_2} \circ \rho'_{KF_3})(\sigma)(x) = (\rho'_{KF_3}(\sigma)|_{F_2})(x) \overset{x\in F_2}{=} \rho'_{KF_3}(\sigma)(x).$$

On en déduit que $\rho'_{KF_1}(\sigma)(x) = \rho'_{KF_2}(\sigma)(x)$, ainsi $\rho(\sigma)$ est bien défini. De plus, $\rho(\sigma)$ est un k-automorphisme de K car $\rho'_{KF}(\sigma)$ est un k-automorphisme de F pour tout $F \in \mathscr{G}$. Enfin, ρ est un homomorphisme de groupes car ρ'_{KF} est un homomorphisme de groupes pour tout $F \in \mathscr{G}$.
Montrons maintenant que $\rho_{KF} \circ \rho = \rho'_{KF}$ pour tout $F \in \mathscr{G}$, i.e., $(\rho_{KF} \circ \rho)(\sigma) = \rho'_{KF}(\sigma)$ pour tout $\sigma \in G'_K$ et $F \in \mathscr{G}$. Soit $x \in F$. Alors :

$$(\rho_{KF} \circ \rho)(\sigma)(x) = \rho_{KF}(\rho(\sigma))(x) \overset{x\in F}{=} (\rho(\sigma)|_F)(x) = \rho(\sigma)(x) \overset{x\in F}{=} \rho'_{KF}(\sigma)(x).$$

On en déduit que $(\rho_{KF} \circ \rho)(\sigma) = \rho'_{KF}(\sigma)$. D'où $\boxed{\rho_{KF} \circ \rho = \rho'_{KF}}$.
Il reste à montrer que l'homomorphisme ρ est unique. Soit $\rho' : G'_K \longrightarrow Gal(K/k)$ un homomorphisme tel que pour tout $F \in \mathscr{G}$, $\rho_{KF} \circ \rho' = \rho'_{KF}$. Alors pour tout $\sigma \in G'_K$, si $x \in F$, on a :

$$\rho(\sigma)(x) \overset{x\in F}{=} \rho'_{KF}(\sigma)(x) = (\rho_{KF} \circ \rho')(\sigma)(x) = (\rho'(\sigma)|_F)(x) \overset{x\in F}{=} \rho'(\sigma)(x).$$

D'où $\boxed{\rho = \rho'}$.

□

Grâce à ce qui précède, on peut maintenant identifier les éléments de $Gal(K/k)$ dans l'espace produit $\prod_{F\in\mathscr{G}} Gal(F/k)$:

$$\sigma \in Gal(K/k) \longmapsto (\sigma|_F)_{F\in\mathscr{G}} \in \prod_{F\in\mathscr{G}} Gal(F/k).$$

Réciproquement, si $(\sigma_F)_{F\in\mathscr{G}} \in \prod_{F\in\mathscr{G}} Gal(F/k)$, alors $\sigma : x \mapsto \sigma_F(x)$ si $x \in F$ est un élément de $Gal(K/k)$ (c'est bien défini d'après le théorème 2.28).
Comme chaque $Gal(F/k)$ est muni de la topologie discrète, tout singleton est ouvert. D'après la proposition 2.23,

$$\{\rho_{KF}^{-1}(\tau)|F \in \mathscr{G}, \tau \in Gal(F/k)\} \tag{3}$$

forme une base de $Gal(K/k)$. En particulier, si $\sigma \in Gal(K/k)$, alors

$$\{\rho_{KF}^{-1}(\sigma|_F)|F \in \mathscr{G}\}$$

forme une base de voisinages de σ. Si on prend $\sigma = e$ (l'élément unité), on en déduit que

$$\{\rho_{KF}^{-1}(e|_F)|F \in \mathscr{G}\} = \{Gal(K/F)|F \in \mathscr{G}\} \tag{4}$$

forme une base de voisinages de l'élément unité. La topologie sur $Gal(K/k)$ définie ci-dessus est appelée la *topologie de Krull*. Ainsi $Gal(K/k)$ est un groupe topologique muni de la topologie de Krull, et ρ_{KF} est un homomorphisme continu pour tout $F \in \mathscr{G}$. On peut alors compléter le théorème 2.28 :

Théorème 2.29. $(Gal(K/k), (\rho_{KF})_{F\in\mathscr{G}}) \cong (\varprojlim Gal(F/k), (\rho_F)_{F\in\mathscr{G}})$ *(en tant que groupes topologiques).*

Preuve. D'après le théorème 2.28, il suffit de montrer que si G'_K est un groupe topologique et si pour tout $F \in \mathscr{G}$, $\rho'_{KF} : G'_K \longrightarrow Gal(F/k)$ est un homomorphisme continu tel que $\rho'_{KF_1} = \rho_{F_2F_1} \circ \rho'_{KF_2}$ lorsque $F_1 \subseteq F_2$, alors l'homomorphisme de groupe $\rho : G'_K \longrightarrow Gal(K/k)$ vérifiant $\rho_{KF} \circ \rho = \rho'_{KF}$ pour tout $F \in \mathscr{G}$ (il est déjà défini dans le théorème 2.28) est continu.
D'après (4), pour montrer que ρ est continu, il suffit de montrer que pour tout voisinage ouvert $Gal(K/F)$ de l'élément unité e (de $Gal(K/k)$), l'image réciproque $\rho^{-1}(Gal(K/F))$ est ouvert. Or,

$$\rho^{-1}(Gal(K/F)) \overset{(4)}{=} \rho^{-1}(\rho_{KF}^{-1}(e|_F)) = (\rho_{KF} \circ \rho)^{-1}(e|_F) = (\rho'_{KF})^{-1}(e|_F).$$

Comme $\{e|_F\}$ est ouvert dans $Gal(F/k)$ et ρ'_{KF} est continu, on en déduit que $\rho^{-1}(Gal(K/F))$ est ouvert dans G'_K. D'où ρ est continu.

□

Notons que chaque $Gal(F/k)$ est discret et non vide. D'après les propositions 2.19, 2.20 et 2.22, on a :

Corollaire 2.30. *Le groupe de Galois $Gal(K/k)$ est compact, non vide, et totalement discontinu.*

Maintenant, on va établir la théorie de Galois pour les extensions galoisiennes de degré infini.

Théorème 2.31. (Krull). *Soient K/k une extension galoisienne de groupe de Galois $Gal(K/k)$ muni de la topologie de Krull.*
(i) L'application

$$\begin{array}{ccc} \{\text{sous-corps de } K \text{ contenant } k\} & \longrightarrow & \{\text{sous-groupes fermés de } Gal(K/k)\} \\ F & \longmapsto & Gal(K/F) \end{array}$$

est une bijection, de bijection réciproque

$$\begin{array}{ccc} \{\text{sous-groupes fermés de } Gal(K/k)\} & \longrightarrow & \{\text{sous-corps de } K \text{ contenant } k\} \\ H & \longmapsto & Inv_K(H) \end{array}.$$

C'est-à-dire,

$$Inv_K(Gal(K/F)) = F, \text{ pour tout corps } F,\ k \subseteq F \subseteq K,$$
$$Gal(K/Inv_K(H)) = H, \text{ pour tout sous-groupe fermé } H \text{ de } Gal(K/k);$$

De plus, les deux applications sont décroissantes pour l'inclusion :

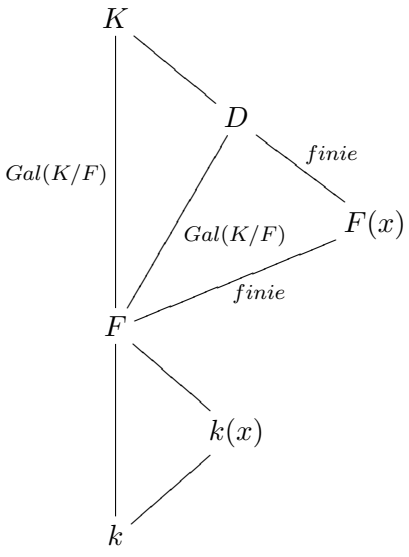
$$F_1 \subseteq F_2 \implies Gal(K/F_2) \subseteq Gal(K/F_1),$$
$$H_1 \subseteq H_2 \implies Inv_K(H_2) \subseteq Inv_K(H_1);$$

(ii) Soit F/k une sous-extension de K/k, et $Gal(K/F)$ le groupe de Galois de l'extension relative. Alors F/k est galoisienne si et seulement si $Gal(K/F)$ est distingué dans $Gal(K/k)$. Dans ce cas, l'homomorphisme naturel $Gal(K/k)/Gal(K/F) \longrightarrow Gal(F/k)$ est un isomorphisme en tant que groupes topologiques, l'isomorphisme étant induit par l'homomorphisme de groupes topologiques

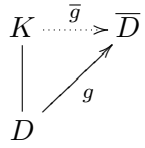
$$\begin{array}{rccc} \phi: & Gal(K/k) & \longrightarrow & Gal(F/k) \\ & \sigma & \longmapsto & \sigma|_F \end{array}$$

avec noyau $\ker\phi = Gal(K/F)$.

Preuve. (i) $\star$ Commençons par montrer que $Inv_K(Gal(K/F)) = F$ pour tout sous-corps F de K contenant k.
Soit $x \in F \subseteq K$. Alors, pour tout $\sigma \in Gal(K/F)$, $\sigma(x) = x$ par définition. Ainsi, $x \in Inv_K(Gal(K/F))$ et $\boxed{F \subseteq Inv_K(Gal(K/F))}$. Supposons que l'inclusion est stricte, c'est-à-dire, il existe un $x \in Inv_K(Gal(K/F))$ tel que $x \notin F$. Posons D la clôture galoisienne de $F(x)/F$. On a le dessin suivant :



Alors, il existe un F-automorphisme g de D tel que $g(x) \neq x$. L'application g s'injecte de D dans $\overline{D}$. Ainsi, par prolongement, il existe un homomorphisme $\overline{g} : K \longrightarrow \overline{D}$ tel que $\overline{g}|_D = g$. On a alors le dessin suivant :



Comme K est galoisienne, $\overline{g}$ est un homomorphisme de K dans K. Ainsi, $\overline{g} \in Gal(K/F)$ et $\overline{g}|_D = g$. Ceci contredit le fait que $x \in Inv_K(Gal(K/F))$ et donc $\boxed{Inv_K(Gal(K/F)) = F}$.
$\star$ Montrons maintenant que $Gal(K/Inv_K(H)) = H$ pour tout sous-groupe fermé H de $Gal(K/k)$. Pour cela, montrons d'abord que tout sous-groupe H de $Gal(K/k)$ est dense dans $Gal(K/Inv_K(H))$.
Soit H un sous-groupe de $Gal(K/k)$. Notons $L = Inv_K(H)$. Soit $\sigma \in Gal(K/L)$. Pour montrer que H est dense dans $Gal(K/L)$, il suffit de montrer que pour tout voisinage U de σ, $U \cap H \neq \emptyset$. Or, les $V_{F'}(\sigma) := \rho^{-1}_{KF'}(\sigma|_{F'})$ avec $F' \in \mathscr{G}$ forment une base de voisinages de σ (par (3)) et $V_{F'L}(\sigma) \subseteq V_{F'}(\sigma)$. Donc il suffit de montrer que pour tout $F' \in \mathscr{G}$, $V_{F'L}(\sigma) \cap H \neq \emptyset$.
Remarquons que $F'L/L$ est une extension galoisienne finie. En effet, comme l'extension K/k est galoisienne, on peut en déduire que K est séparable sur k et donc sur L. Or, $L \subseteq F'L \subseteq K$. Ainsi, $F'L$ est séparable sur L. Soit maintenant un polynôme $P \in k[X]$ tel que F' soit le corps de ses racines sur k. Alors $P \in L[X]$ et $F'L$ est le corps de ses racines sur L. On peut ainsi en déduire que l'extension $F'L/L$ est normale et donc galoisienne. De plus, comme $F' \in \mathscr{G}$, l'extension F'/k est finie. Par conséquent, $F' = k(\alpha_1, ..., \alpha_n)$, où $\alpha_i \in F'$ et est algébrique sur k pour tout $i \in \{1, ..., n\}$. Il en résulte alors que $F'L = k(F' \cup L) = L(\alpha'_1, ..., \alpha'_n)$, où $\alpha'_i \in F'L$ et est algébrique sur L pour tout $i \in \{1, ..., n\}$ et donc que l'extension $F'L/L$ est finie.
Notons $H' = \{\alpha|_{F'L} : \alpha \in H\}$. Alors H' est un sous-groupe de $Gal(F'L/L)$. En effet :
- H' est non vide : $(id_K)|_{F'L} \in H'$.
- Si $\alpha|_{F'L} \in H'$ avec $\alpha \in H$, alors $\alpha|_L = id_L$ par définition de L, ce qui implique que $\alpha \in Gal(K/L)$. Ainsi, $\alpha|_{F'L} \in Gal(F'L/L)$ car $F'L/L$ est galoisienne et par conséquent, $H' \subseteq Gal(F'L/L)$.
- Soient $\alpha_1|_{F'L}$ et $\alpha_2|_{F'L}$ deux éléments de H' avec α_1 et α_2 dans H. Comme H est un groupe, il en découle que $\alpha_1 \circ (\alpha_2)^{-1} \in H$. Montrons les égalités suivantes :

$$(\alpha_2|_{F'L})^{-1} = \alpha_2^{-1}|_{F'L} \text{ et } (\alpha_1|_{F'L}) \circ (\alpha_2^{-1}|_{F'L}) = (\alpha_1 \circ \alpha_2^{-1})|_{F'L}.$$

Pour cela, il suffit de montrer que pour tout α et β dans H, $(\alpha|_{F'L}) \circ (\beta|_{F'L}) = (\alpha \circ \beta)|_{F'L}$. Soient $\alpha, \beta \in H$. Alors pour tout $x \in F'L$,

$$\begin{aligned}((\alpha|_{F'L}) \circ (\beta|_{F'L}))(x) = (\alpha|_{F'L})((\beta|_{F'L})(x)) &\overset{x \in F'L}{=} (\alpha|_{F'L})(\beta(x)) \overset{\beta(x) \in F'L}{=} \alpha(\beta(x)) \\ &= \alpha \circ \beta(x) \overset{x \in F'L}{=} ((\alpha \circ \beta)|_{F'L})(x).\end{aligned}$$

D'où l'égalité. Ainsi, $\alpha_1|_{F'L} \circ (\alpha_2|_{F'L})^{-1} = \alpha_1|_{F'L} \circ \alpha_2^{-1}|_{F'L} = (\alpha_1 \circ \alpha_2^{-1})|_{F'L} \in H'$.
Remarquons maintenant que $Inv_{F'L}(H') = L$. En effet :
"$\supseteq$" : Si $x \in L$ et $\alpha \in H$, alors $(\alpha|_{F'L})(x) \overset{x \in L \subseteq F'L}{=} \alpha(x) = x$. D'où $\boxed{L \subseteq Inv_{F'L}(H')}$.
"$\subseteq$" : Supposons que $x \in Inv_{F'L}(H')$ et que $x \notin L$. Alors il existe un élément ϕ de H vérifiant $\phi(x) \neq x$. Or, $x \in F'L$. On en déduit ainsi que $(\phi|_{F'L})(x) \neq x$, ce qui contredit l'hypothèse $x \in Inv_{F'L}(H')$. D'où $\boxed{Inv_{F'L}(H') \subseteq L}$.
Comme $Inv_{F'L}(H') = L$ et comme H' est un sous-groupe de $Gal(F'L/L)$ qui est une extension galoisienne finie, on en déduit que $\boxed{Gal(F'L/L) = H'}$.

Posons maintenant $\theta' = \sigma|_{F'L}$. Comme σ appartient à $Gal(K/L)$ qui est un sous-groupe de $Gal(K/k)$, on en déduit que $\theta' \in Gal(F'L/L) = H'$. Ainsi il existe un élément θ de H tel que $\theta|_{F'L} = \theta' = \sigma|_{F'L}$; ce qui implique que

$$\theta \in V_{F'L}(\sigma) = \{\eta \in Gal(K/k) | \eta|_{F'L} = \sigma|_{F'L}\}.$$

On vient ainsi de montrer que $\theta \in V_{F'L}(\sigma) \cap H$. D'où $\boxed{V_{F'L}(\sigma) \cap H \neq \emptyset}$.
Supposons maintenant que H est un sous-groupe fermé de $Gal(K/k)$. Ainsi, $\overline{H} = H$ et comme H est dense dans $Gal(K/Inv_K(H))$, il en résulte que $\boxed{H = \overline{H} = Gal(K/Inv_K(H))}$. D'où l'égalité.
$\star$ Soient F_1 et F_2 deux sous-corps de K contenant k tels que $F_1 \subseteq F_2$. Soit σ un F_2-automorphisme de K. Alors par définition, σ est un automorphisme de K et $\sigma(x) = x$ pour tout $x \in F_2$. De plus, comme $F_1 \subseteq F_2$, il en découle que $\sigma(x) = x$ pour tout $x \in F_1$. On peut ainsi en déduire que σ est un F_1-automorphisme de K et que $\boxed{Gal(K/F_2) \subseteq Gal(K/F_1)}$.
$\star$ Soient H_1 et H_2 deux sous-groupes de $Gal(K/k)$ tels que $H_1 \subseteq H_2$. Soit x un élément de $Inv_K(H_2)$. Alors par définition, $\sigma(x) = x$ pour tout $\sigma \in H_2$. De plus, comme $H_1 \subseteq H_2$, il en découle que $\sigma(x) = x$ pour tout $\sigma \in H_1$. On a ainsi montré que x est un élément de $Inv_K(H_1)$ et que $\boxed{Inv_K(H_2) \subseteq Inv_K(H_1)}$.
(ii) L'extension F/k est séparable car K/k l'est, donc F/k est galoisienne si et seulement si F/k est normale.
Si F/k est une extension normale, alors ϕ est bien définie. Elle est de plus surjective. En effet, soit $\tau \in Gal(F/k)$, par le théorème de prolongement, il existe un homomorphisme $\sigma : K \longrightarrow \overline{k}$ tel que $\sigma|_F = \tau$. Comme K/k est une extension galoisienne, on en déduit que $\sigma \in Gal(K/k)$. Notons que

$$\ker \phi = \{\sigma \in Gal(K/k) | \phi(\sigma) = id_F\} = \{\sigma \in Gal(K/k) | \sigma|_F = id_F\} = Gal(K/F).$$

Donc $Gal(K/F)$ est distingué dans $Gal(K/k)$, et on a l'isomorphisme

$$Gal(K/k)/Gal(K/F) \cong Gal(F/k)$$

en tant que groupes topologiques par la proposition 2.12.
Réciproquement, si $Gal(K/F)$ est distingué dans $Gal(K/k)$, montrons que F/k est une extension normale. Il suffit de montrer que $\tau(F) = F$ pour tout k-homomorphisme $\tau : F \longrightarrow \overline{k}$ par proposition 1.4. Notons d'abord que $\sigma(F) = F$ pour tout $\sigma \in Gal(K/k)$.
En effet, si $\rho \in Gal(K/F)$ et si $x \in F$, alors $\rho(\sigma(x)) = \sigma(\sigma^{-1}\rho\sigma)(x) = \sigma(x)$ car $Gal(K/F)$ est distingué dans $Gal(K/k)$. On en déduit que $\rho \in Gal(K/\sigma(F))$, d'où $Gal(K/F) \subseteq Gal(K/\sigma(F))$. Par le théorème de Galois (1.17), on a

$$\sigma(F) = Inv_K(Gal(K/\sigma(F))) \subseteq Inv_K(Gal(K/F)) = F.$$

De plus, $[K : \sigma(F)] = [\sigma(K) : \sigma(F)] = [K : F]$ car σ est un k-automorphisme de K. On en déduit que $F = \sigma(F)$ pour tout $\sigma \in Gal(K/k)$.
Pour τ un k-homomorphisme de F dans $\overline{k}$, il existe σ un k-homomorphisme de K dans $\overline{k}$ tel que $\sigma|_F = \tau$ par le théorème de prolongement. Or, K/k est galoisienne, ainsi $\sigma \in Gal(K/k)$. On a donc $\tau(F) = \sigma(F) = F$. D'où F est normale.

□

En résumé, si K/k une extension galoisienne de groupe de Galois $Gal(K/k)$, alors on a une bijection décroissante $F \mapsto Gal(K/F)$, d'application réciproque $H \mapsto Inv_K(H)$, entre les sous-corps de K contenant k et les sous-groupes fermés de $Gal(K/k)$.
Dans la suite de ce paragraphe, on étudiera le groupe de Galois de l'extension L/L', où L est la clôture séparable de k et L' est la clôture abélienne de k. Commençons par rappeler quelques notions et propriétés de la clôture séparable et la clôture abélienne.

Proposition 2.32. *Soit $\overline{k}$ une clôture algébrique de k. Alors l'ensemble d'éléments séparables sur k dans $\overline{k}$ est un corps.*

Preuve. Il suffit de montrer que si x et y sont deux éléments séparables, alors $x+y, x-y, xy$ et xy^{-1} sont aussi séparables. Remarquons que si $k(x)/k$ est une extension algébrique, alors $k(x)/k$ est une extension séparable si et seulement si x est séparable sur k. Remarquons également que si $k(x)/k$ est une extension séparable, alors $k(x,y)/k(y)$ est aussi une extension séparable. On en déduit que si x et y sont séparables sur k, alors $k(x,y)/k$ est une extension séparable. D'où $x+y, x-y, xy$ et xy^{-1} sont séparables sur k.

□

Définition 2.33. Soit $\overline{k}$ une clôture algébrique de k. La *clôture séparable* de k est l'ensemble des éléments séparables sur k dans $\overline{k}$.

Remarque. (i) La clôture séparable dépend du choix de la clôture algébrique et deux clôture séparables de k sont k-isomorphes ;
(ii) La clôture séparable de k, noté K, est une extension galoisienne sur k. En effet, si $x \in K$, alors x est séparable sur k par définition. Donc son polynôme minimal $Irr_k(x)$ n'a que des racines simples. Si y est un k-conjugué de x, alors $Irr_k(y) = Irr_k(x)$ qui est séparable sur k. On en déduit que K/k est une extension normale et donc galoisienne.

Lemme 2.34. *Soient $\overline{k}$ une clôture algébrique de k et $(N_i/k)_{i\in I}$ une famille d'extensions abéliennes de k contenues dans $\overline{k}$. Alors $k\Big(\bigcup\limits_{i\in I} N_i\Big)/k$ est une extension abélienne.*

Preuve. Il suffit de montrer que $k\Big(\bigcup\limits_{i\in I} N_i\Big)/k$ est une extension normale, séparable, et de groupe de Galois abélien. Posons $N = \bigcup\limits_{i\in I} N_i$.
⋆ Montrons que si $(N_i/k)_{i\in I}$ est une famille d'extensions normales, alors $k(N)/k$ est une extension normale.
Remarquons d'abord que $k(N) = \bigcup\limits_{\substack{F \text{ finie} \\ F \subseteq N}} k(F)$. Si $x \in k(N)$, alors $x \in k(n_1, \cdots, n_r)$ avec $n_i \in N_{k_i}$ pour $k_i \in I$ et $1 \leq i \leq r$. On note P_i les polynômes minimaux de n_i et on pose $P = P_1 \cdots P_r$. Comme les extensions N_{k_i}/k sont normales, le corps de décomposition de P, noté K, est une extension normale sur k qui est incluse dans $k\Big(\bigcup\limits_{i=1}^{n} N_{k_i}\Big) \subseteq k(N)$. On en déduit que tous les conjugués de x sont dans K, donc dans $k(N)$. D'où $k(N)/k$ est normale.
⋆ Montrons que si $(N_i/k)_{i\in I}$ est une famille d'extensions séparables, alors $k(N)/k$ est une extension séparable.
Si $x \in k(N)$, alors $x \in k(n_1, \cdots, n_r)$ avec $n_i \in N_{k_i}$ pour $k_i \in I$ et $1 \leq i \leq r$. Comme les extensions N_{k_i}/k sont séparables, les n_i sont séparables sur k. On en déduit que $k(n_1, \cdots, n_r)/k$ est une extension séparable. D'où x est séparable sur k.
⋆ Montrons que si $(N_i/k)_{i\in I}$ est une famille d'extensions abéliennes, alors $k(N)/k$ est une extension abélienne.
Grâce à ce qui précède, il suffit de montrer que le groupe de Galois $Gal(k(N)/k)$ est abélien. Posons

$$\begin{array}{rccc} \phi: & Gal(k(N)/k) & \longrightarrow & \prod\limits_{i\in I} Gal(N_i/k) \\ & \sigma & \longmapsto & (\sigma|_{N_i})_{i\in I}, \end{array}$$

alors ϕ est injective. En effet, si $\sigma|_{N_i} = id_{N_i}$ pour tout $i \in I$, on a $\sigma = id_{k(N)}$ car $N = \bigcup\limits_{i\in I} N_i$ et $\sigma|_k = id_k$. On peut donc identifier $Gal(k(N)/k)$ comme un sous-groupe du groupe pro-

duit $\prod_{i\in I} Gal(N_i/k)$. Or, $\prod_{i\in I} Gal(N_i/k)$ est un groupe abélien car tous les $Gal(N_i/k)$ le sont.
On en déduit que $Gal(k(N)/k)$ est bien un groupe abélien.

□

Définition 2.35. Soient $\overline{k}$ une clôture algébrique de k et $(N_i/k)_{i\in I}$ la famille de toutes les extensions abéliennes de k contenues dans $\overline{k}$. Le corps $k\Big(\bigcup_{i\in I} N_i\Big) = \prod_{i\in I} N_i$ est appelé la *clôture abélienne* de k.

Remarque. (i) La clôture abélienne dépend du choix de la clôture algébrique et deux clôture abéliennes de k sont k-isomorphes ;
(ii) La clôture abélienne de k est un sous-corps de la clôture séparable de k.

Définition 2.36. Soient G un groupe et x, y deux éléments de G. Le *commutateur* du couple (x, y) est un élément de G défini par $[x, y] = xyx^{-1}y^{-1}$.

Lemme 2.37. *Soit G un groupe et G' le sous-groupe engendré par les commutateurs d'éléments de G. Alors G' est normal et G/G' est abélien. Réciproquement, si H est un sous-groupe normal de G et si G/H est abélien, alors $G' \subseteq H$.*

Preuve. Montrons d'abord que G' est normal et que G/G' est abélien.
Soient $x, y, z \in G$. Alors

$$z[x, y]z^{-1} = zxyx^{-1}y^{-1}z^{-1} = zxyx^{-1}z^{-1}y^{-1}yzy^{-1}z^{-1} = [zx, y][y, z] \in G'.$$

D'où G' est normal. De plus, on a :

$$(xG')(yG') = xyG' = yxx^{-1}y^{-1}xyG' = yx[x^{-1}, y^{-1}]G' = yxG' = (yG')(xG').$$

D'où G/G' est abélien.
Réciproquement, si H est un sous-groupe normal de G et si G/H est abélien, soit $x, y \in G$. Alors on a :

$$[x, y]H = xy(x^{-1}y^{-1}H) \overset{G/H \text{ abélien}}{=} xy(y^{-1}x^{-1}H) = H.$$

On en déduit que $[x, y] \in H$ pour tout $x, y \in G$. D'où $G' \subseteq H$.

□

Proposition 2.38. *Soient L la clôture séparable de k et L' la clôture abélienne de k. Alors le groupe de Galois $Gal(L/L')$ est l'adhérence de G' dans $Gal(L/k)$, où G' est le sous-groupe de $Gal(L/k)$ engendré par les commutateurs d'éléments de $Gal(L/k)$.*

Preuve. On a l'isomorphisme suivant : $Gal(L/k)/Gal(L/L') \cong Gal(L'/k)$. En effet, comme L est une clôture séparable de k, l'extension L/k est galoisienne et par conséquent, l'extension L/L' est également galoisienne. De plus, comme L' est une clôture abélienne de k, il en découle que l'extension L'/k est abélienne et donc galoisienne. Ainsi, par le theórème 2.31, on peut en déduire l'isomorphisme $\boxed{Gal(L/k)/Gal(L/L') \cong Gal(L'/k)}$.
Comme L' est la clôture abélienne de k, on peut en déduire que $Gal(L'/k)$ est abélien. Donc d'après le lemme 2.37, $G' \subseteq Gal(L/L')$. Montrons que $Gal(L/L') = \overline{G'}$.
"$\supseteq$" : On sait déjà que $G' \subseteq Gal(L/L')$. Ainsi, $\overline{G'} \subseteq \overline{Gal(L/L')}$. Comme L' est un sous-corps de L, on en déduit par le théorème 2.31 que $Gal(L/L')$ est un sous-groupe fermé de $Gal(L/k)$. D'où $\overline{Gal(L/L')} = Gal(L/L')$ et $\boxed{\overline{G'} \subseteq Gal(L/L')}$.
"$\subseteq$" : Notons $S = Inv_L(G')$. Étant donné que G' est le sous-groupe normal engendré par les commutateurs d'éléments de $Gal(L/k)$, on peut en déduire par le lemme 2.37 que G'

est normal. Ainsi, d'après la proposition 2.6, $\overline{G'}$ est normal. Comme $\overline{G'}$ est un sous-groupe fermé de $Gal(L/k)$, on peut en déduire par le théorème 2.31 que S est un sous-corps de L. De plus, par le théorème 2.31, $Gal(L/S) = Gal(L/Inv_L(\overline{G'})) = \overline{G'}$. Donc S est de groupe de Galois $\overline{G'}$. Comme $\overline{G'}$ est normal, on en déduit par le théorème 2.31 que S/k est une extension galoisienne et on a l'isomorphisme suivant :

$$Gal(S/k) \cong Gal(L/k)/Gal(L/S)$$

Comme $G' \subseteq \overline{G'} = Gal(L/S)$, on en déduit par le lemme 2.37 que $Gal(S/k)$ est abélien, c'est-à-dire, S/k est une extension abélienne. Ainsi, comme L' est la clôture abélienne de k, S est un sous-corps de L' et par conséquent, comme l'opération $Gal(L/\cdot)$ inverse l'inclusion, $\boxed{Gal(L/L') \subseteq Gal(L/S) = \overline{G'}}$.

D'où $\boxed{Gal(L/L') = \overline{G'}}$.

□

3 Quelques Exemples

Dans cette partie, on appliquera le théorème de Krull pour décrire explicitement certaines extensions galoisiennes de degré infini.

3.1 Clôture algébrique des corps finis

Le but de ce paragraphe est de décrire le groupe de Galois de l'extension $\overline{\mathbb{F}}_p/\mathbb{F}_p$.

Proposition 3.1. *Soit p un nombre premier. Posons pour $m \leq n$*

$$\begin{array}{rccc} \rho_{nm}: & \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & \mathbb{Z}/p^m\mathbb{Z} \\ & \bar{x}^{[n]} & \longmapsto & \bar{x}^{[m]} \end{array}$$

les homomorphismes de groupes, où $\bar{x}^{[n]}$ désigne la classe de x modulo p^n et $\bar{x}^{[m]}$ désigne la classe de x modulo p^m. Alors $((\mathbb{Z}/p^n\mathbb{Z})_{n\geq 1}, (\rho_{nm})_{m\leq n})$ est un système inverse de groupes et de homomorphismes.

Preuve. Il est clair que $\rho_{nn} = id_{\mathbb{Z}/p^n\mathbb{Z}}$ pour tout $n \geq 1$. Si $m \leq n \leq l$, et si $\bar{x}^{[l]} \in \mathbb{Z}/p^l\mathbb{Z}$, alors

$$(\rho_{nm} \circ \rho_{ln})(\bar{x}^{[l]}) = \rho_{nm}(\bar{x}^{[n]}) = \bar{x}^{[m]} = \rho_{lm}(\bar{x}^{[l]}).$$

D'où $\rho_{nm} \circ \rho_{ln} = \rho_{lm}$.

□

Définition 3.2. Soient p un nombre premier et ρ_{nm} les homomorphismes définis comme ci-dessus. On note $\mathbb{Z}_p$ la limite inverse de la famille $(\mathbb{Z}/p^n\mathbb{Z})_{n\geq 1}$ par rapport aux homomorphismes $(\rho_{nm})_{m\leq n}$, et on l'appelle *l'anneau des entiers p-adiques.*

Lemme 3.3. *Soit F_1/k et F_2/k des extensions galoisiennes. Alors $F_1F_2/F_1 \cap F_2$ est une extension galoisienne et*

$$Gal(F_1F_2/F_1 \cap F_2) \cong Gal(F_1/F_1 \cap F_2) \times Gal(F_2/F_1 \cap F_2). \qquad (*)$$

En particulier, si $F_1 \cap F_2 = k$ alors on a $Gal(F_1F_2/k) \cong Gal(F_1/k) \times Gal(F_2/k)$.

Preuve. D'après le lemme 2.34, F_1F_2/k est une extension galoisienne, donc $F_1F_2/F_1 \cap F_2$ est galoisienne. Il reste à montrer $(*)$. Posons

$$\begin{array}{rccc} \phi: & Gal(F_1F_2/F_1 \cap F_2) & \longrightarrow & Gal(F_1/F_1 \cap F_2) \times Gal(F_2/F_1 \cap F_2) \\ & \sigma & \longmapsto & (\sigma|_{F_1}, \sigma|_{F_2}). \end{array}$$

Alors :
$\star$ L'application ϕ est bien définie car $F_1/F_1 \cap F_2$ et $F_2/F_1 \cap F_2$ sont des extensions galoisiennes.
$\star$ ϕ est un homomorphisme. En effet, si $\sigma, \tau \in Gal(F_1F_2/F_1 \cap F_2)$, alors

$$\phi(\sigma \circ \tau) = ((\sigma \circ \tau)|_{F_1}, (\sigma \circ \tau)|_{F_2}) = (\sigma|_{F_1} \circ \tau|_{F_1}, \sigma|_{F_2} \circ \tau|_{F_2}) = (\sigma|_{F_1}, \sigma|_{F_2}) \circ (\tau|_{F_1}, \tau|_{F_2}).$$

$\star$ ϕ est injective. En effet, si $\sigma|_{F_1} = id_{F_1}$ et si $\sigma|_{F_2} = id_{F_2}$, alors $\sigma = id_{F_1F_2}$ car $F_1F_2 = k(F_1 \cup F_2)$ et $\sigma|_k = id_k$.
$\star$ ϕ est surjective. En effet, soit $(\sigma_1, \sigma_2) \in Gal(F_1/F_1 \cap F_2) \times Gal(F_2/F_1 \cap F_2)$. Pour $x \in F_1 \cup F_2$, on définit

$$\sigma(x) = \begin{cases} \sigma_1(x) & \text{si } x \in F_1; \\ \sigma_2(x) & \text{si } x \in F_2, \end{cases}$$

puis on la prolonge linéairement sur F_1F_2. L'application σ est un $F_1 \cup F_2$-automorphisme de F_1F_2 car $F_1F_2/F_1 \cap F_2$ est galoisienne et σ_1, σ_2 sont $F_1 \cap F_2$-stables. Ainsi $\sigma \in Gal(F_1F_2/F_1 \cap F_2)$ et $\phi(\sigma) = (\sigma_1, \sigma_2)$.
Conclusion : ϕ est un isomorphisme.

□

Lemme 3.4. *Soient K/k une extension galoisienne finie et $F_1/k, F_2/k$ des sous-extensions de K. Alors $Gal(K/F_1\cap F_2) = \langle Gal(K/F_1), Gal(K/F_2)\rangle$. En particulier, si $F_1/k, F_2/k$ sont galoisiennes et si $K = F_1F_2$, alors $Gal(K/F_1 \cap F_2) \cong Gal(K/F_1) \times Gal(K/F_2)$.*

Preuve. Comme $F_1 \cap F_2 \subseteq F_1$ et $F_1 \cap F_2 \subseteq F_2$, on a $Gal(K/F_1) \subseteq Gal(K/F_1 \cap F_2)$ et $Gal(K/F_2) \subseteq Gal(K/F_1 \cap F_2)$. D'où $\langle Gal(K/F_1), Gal(K/F_2)\rangle \subseteq Gal(K/F_1 \cap F_2)$.
Réciproquement, d'après le théorème de Galois (1.17), il suffit de montrer que

$$Inv_K(\langle Gal(K/F_1), Gal(K/F_2)\rangle) \subseteq Inv_K(Gal(K/F_1 \cap F_2)) = F_1 \cap F_2.$$

Si $x \in Inv_K(\langle Gal(K/F_1), Gal(K/F_2)\rangle)$, alors $\sigma(x) = x$ pour tout $\sigma \in \langle Gal(K/F_1), Gal(K/F_2)\rangle$. En particulier, $\sigma(x) = x$ pour tout $\sigma \in Gal(K/F_1)$ et pour tout $\sigma \in Gal(K/F_2)$. C'est-à-dire, $x \in Inv_K(Gal(K/F_1)) \cap Inv_K(Gal(K/F_2)) = F_1 \cap F_2$.
Conclusion : $\boxed{Gal(K/F_1 \cap F_2) = \langle Gal(K/F_1), Gal(K/F_2)\rangle}$.
Si F_1/k et F_2/k sont en plus galoisiennes, alors $Gal(K/F_1)$ et $Gal(K/F_2)$ sont distingués par le théorème de Galois (1.17). De plus, $Gal(K/F_1)\cap Gal(K/F_2) = \{id_K\}$ car $K = F_1F_2$.
On en déduit que $\boxed{\langle Gal(K/F_1), Gal(K/F_2)\rangle \cong Gal(K/F_1) \times Gal(K/F_2)}$. D'où le résultat.

□

D'après le lemme 3.3 et 3.4, on a le corollaire suivant :

Corollaire 3.5. *Soient F_1/k et F_2/k des extensions galoisiennes finies. Alors $F_1F_2/F_1\cap F_2$ est une extension galoisienne et*

$$Gal(F_1F_2/F_1\cap F_2) \cong Gal(F_1/F_1\cap F_2)\times Gal(F_2/F_1\cap F_2) \cong Gal(F_1F_2/F_1)\times Gal(F_1F_2/F_2).$$

Proposition 3.6. $Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/n\mathbb{Z}$.

Preuve. Soit F un corps inclus dans $\overline{\mathbb{F}}_p$ tel que l'extension $F/\mathbb{F}_p$ est galoisienne finie et soit n le degré de l'extension $F/\mathbb{F}_p$. Alors $F = \mathbb{F}_{p^n}$ et par le théorème 2.29, $Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \varprojlim Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Or, $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$ par le théorème 1.14.
D'où l'isomorphisme $\boxed{Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \varprojlim \mathbb{Z}/n\mathbb{Z}}$.

□

On va maintenant donner une description plus précise du groupe de Galois de l'extension $\overline{\mathbb{F}}_p/\mathbb{F}_p$. Pour cela, on va avoir besoin du théorème suivant :

Théorème 3.7. *Soit $(L_n)_{n\geq 1}$ une famille d'extensions galoisiennes de k telle que :*
(i) $K = k\left(\bigcup_{n\geq 1} L_n\right)$;
(ii) $\forall m \geq 1$, $k\left(\bigcup_{n\neq m} L_n\right) \cap L_m = k$.
Alors, $Gal(K/k) \cong \prod_{n\geq 1} Gal(L_n/k)$.

Preuve. Posons

$$\begin{array}{rccc} \theta : & Gal(K/k) & \longrightarrow & \prod_{n\geq 1} Gal(L_n/k) \\ & \sigma & \longmapsto & (\sigma|_{L_n})_{n\geq 1}. \end{array}$$

⋆ L'application θ est bien définie. En effet, si $\sigma \in Gal(K/k)$, alors comme L_n/k est une extension galoisienne, $\sigma|_{L_n} \in Gal(L_n/k)$ pour tout $n \geq 1$.
⋆ L'application θ est un homomorphisme de groupes. En effet, pour tout $\sigma_1, \sigma_2 \in Gal(K/k)$:

$$\theta(\sigma_1 \circ \sigma_2) \overset{\text{déf}}{=} ((\sigma_1 \circ \sigma_2)|_{L_n})_{n\geq 1} = (\sigma_1|_{L_n} \circ \sigma_2|_{L_n})_{n\geq 1}$$
$$= (\sigma_1|_{L_n})_{n\geq 1} \circ (\sigma_2|_{L_n})_{n\geq 1} \overset{\text{déf}}{=} \theta(\sigma_1) \circ \theta(\sigma_2).$$

De plus, $\theta(id_K) = ((id_K)|_{L_n})_{n\geq 1} = (id_{L_n})_{n\geq 1}$.
$\star$ Montrons que l'application θ est injective. Soit σ un k-automorphisme de K. Supposons que $\theta(\sigma) = (id_{L_n})_{n\geq 1}$. Alors $\sigma|_{L_n} = id_{L_n}$ pour tout $n \geq 1$, c'est-à-dire, $\sigma(x) = x$ pour tout $x \in L_n$ avec $n \geq 1$. De plus, par hypothèse, $K = k\left(\bigcup_{n\geq 1} L_n\right)$ et $\sigma(x) = x$ pour tout $x \in k$. On peut alors en déduire que $\sigma(x) = x$ pour tout $x \in K$ et donc que $\boxed{Ker(\theta) = id_K}$. D'où l'injectivité de l'application θ.
$\star$ Montrons que l'application θ est surjective. Soit $\sigma^{(n)} \in Gal(L_n/k)$ pour tout $n \geq 1$. Pour tout $n \geq 1$, notons K_n le plus petit sous-corps de K qui contient k et $\bigcup_{i=1}^{n} L_i$, c'est-à-dire $K_n = k\left(\bigcup_{i=1}^{n} L_i\right)$. Alors K_n/k est une extension galoisienne par le lemme 2.34. Par conséquent, on a $K = k\left(\bigcup_{n\geq 1} L_n\right) = \bigcup_{n\geq 0} K_n$ et $K_n \subseteq K_{n+1}$ pour tout $n \geq 0$ en posant $K_0 = k$. Construisons maintenant par récurrence sur $n \geq 0$ un k-automorphisme σ_n de K_n vérifiant les propriétés suivantes :
(1) $\sigma_{n-1} = \sigma_n|_{K_{n-1}}$ pour tout $n \geq 1$;
(2) $\sigma^{(i)} = \sigma_n|_{L_i}$ pour tout i tel que $1 \leq i \leq n$.
Prenons tout d'abord $\sigma_0 = id_k$ et $\sigma_1 = \sigma^{(1)} \in Gal(L_1/k)$. L'application σ_1 vérifie bien les hypothèses (1) et (2). En effet, $K_1 = L_1$ par définition. Il en résulte que $\sigma_1 \in Gal(K_1/k)$. De plus, on a :

$$\sigma_1|_{L_1} = \sigma^{(1)}|_{L_1} = \sigma^{(1)},$$

et

$$\sigma_1|_{K_0} = \sigma^{(1)}|_k = id_k = \sigma_0.$$

Supposons maintenant que les applications $\sigma_0, \cdots, \sigma_{n-1}$ sont déjà construites. Comme

$$K_n = k\left(\bigcup_{i=1}^{n} L_i\right) = k(K_{n-1} \cup L_n) = K_{n-1}L_n \text{ et } k = K_{n-1} \cap L_n$$

pour tout $n \geq 1$, on peut en déduire par le lemme 3.3 que

$$Gal(K_n/k) \cong Gal(K_{n-1}/k) \times Gal(L_n/k).$$

Ainsi, il existe un k-automorphisme σ_n de K_n tel que $\sigma_n|_{K_{n-1}} = \sigma_{n-1}$ et $\sigma_n|_{L_n} = \sigma^{(n)}$. De plus, pour tout $i \in \{1, ..., n-1\}$, on a :

$$\sigma_n|_{L_i} \overset{L_i \subseteq K_{n-1}}{=} (\sigma_n|_{K_{n-1}})|_{L_i} = \sigma_{n-1}|_{L_i} \overset{hyp.}{=} \sigma^{(i)}.$$

D'où la récurrence.
Soit σ un k-automorphisme de K défini par $\sigma(x) = \sigma_n(x)$ si $x \in K_n$. L'application σ est bien définie. En effet, si $x \in K_n$ et si $x \in K_m$ avec $n \leq m$, alors

$$\sigma_m(x) \overset{x \in K_n \subseteq K_m}{=} ((\sigma_m)|_{K_n})(x) = \sigma_n(x).$$

De plus,

$$\theta(\sigma) = (\sigma_n|_{L_n})_{n\geq 1} = (\sigma^{(n)})_{n\geq 1}.$$

D'où la surjectivité de l'application θ.
$\star$ Il reste à montrer que l'application θ est continue. Pour cela, il suffit de montrer que pour tout ouvert $U \subseteq \mathscr{V}((id_{L_n})_{n\geq 1})$, $\theta^{-1}(U)$ est ouvert. Comme les $Gal(L_i/F_j)$ forment une base de voisinages de $id_{L_i} \in Gal(L_i/k)$ pour tout $i \in I$ avec F_j/k une extension galoisienne, il suffit de prendre $U = \prod_{n\neq m_i} Gal(L_n/k) \times \prod_{i=1}^{l} V_{m_i}$, où $V_{m_i} = Gal(L_{m_i}/F_{m_i})$ avec F_{m_i}/k une extension galoisienne pour tout $i \in \{1, \cdots, l\}$. On a :

$$\theta^{-1}(U) = \theta^{-1}\left(\bigcap_{i=1}^{l}\left(\prod_{n\neq m_i} Gal(L_n/k) \times V_{m_i}\right)\right) = \bigcap_{i=1}^{l} \theta^{-1}\left(\prod_{n\neq m_i} Gal(L_n/k) \times V_{m_i}\right).$$

Or :

$$\begin{aligned}\theta^{-1}\left(\prod_{n\neq m_i} Gal(L_n/k) \times V_{m_i}\right) &= \left\{\sigma \in Gal(K/k) \;\middle|\; \theta(\sigma) \in \prod_{n\neq m_i} Gal(L_n/k) \times V_{m_i}\right\} \\ &\overset{df}{=} \left\{\sigma \in Gal(K/k) \;\middle|\; (\sigma|_{L_n})_{n\geq 1} \in \prod_{n\neq m_i} Gal(L_n/k) \times V_{m_i}\right\} \\ &= \{\sigma \in Gal(K/k) \mid \sigma|_{L_n} \in Gal(L_n/k)\ \forall n \neq m_i \text{ et } \sigma|_{L_{m_i}} \in V_{m_i} = Gal(L_{m_i}/F_{m_i})\}.\end{aligned}$$

De plus :

$$\begin{aligned}\sigma|_{L_{m_i}} \in Gal(L_{m_i}/F_{m_i}) &\iff (\sigma|_{L_{m_i}})|_{F_{m_i}} = id_{F_{m_i}} \\ &\overset{F_{m_i}\subseteq L_{m_i}}{\iff} \sigma|_{F_{m_i}} = id_{F_{m_i}} \iff \sigma \in Gal(K/F_{m_i}).\end{aligned}$$

Ainsi, $\theta^{-1}\left(\prod_{n\neq m_i} Gal(L_n/k) \times V_{m_i}\right) = Gal(K/F_{m_i})$ et donc :

$$\boxed{\theta^{-1}(U) = \bigcap_{i=1}^{l} \theta^{-1}\left(\prod_{n\neq m_i} Gal(L_n/k) \times V_{m_i}\right) = \bigcap_{i=1}^{l} Gal(K/F_{m_i})}.$$

Comme $Gal(K/F_{m_i})$ est un ouvert de $Gal(K/k)$ pour tout $i \in \{1, ..., l\}$, on peut en déduire que $\theta^{-1}(U)$ est ouvert comme intersection finie d'ouverts. D'où la continuité de l'application θ.
Ainsi, on peut conclure que $\boxed{Gal(K/k) \cong \prod_{n\geq 1} Gal(L_n/k)}$.

□

Grâce au théorème 3.7, on peut maintenant énoncer le théorème suivant :

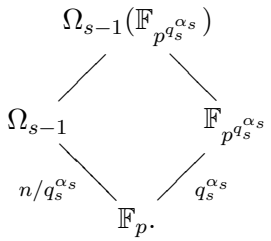
Théorème 3.8. *$Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \prod_{q\in\mathbb{P}} \mathbb{Z}_q$.*

Preuve. Posons $L_q = \bigcup_{n\geq 1} \mathbb{F}_{p^{q^n}}$ où q est un nombre premier. Remarquons que $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$ si et seulement si $d|n$. Alors :
$\star$ $L_q/\mathbb{F}_p$ est une extension galoisienne infinie car $\mathbb{F}_{p^{q^n}} \subseteq \mathbb{F}_{p^{q^{n+1}}}$ et $\mathbb{F}_{p^{q^n}}/\mathbb{F}_p$ est une extension galoisienne pour tout $n \geq 1$.
$\star$ $\overline{\mathbb{F}}_p = \mathbb{F}_p\left(\bigcup_{q\in\mathbb{P}} L_q\right)$. En effet, si $x \in \overline{\mathbb{F}}_p$, alors x est algébrique sur $\mathbb{F}_p$. Ainsi, $\mathbb{F}_p(x)/\mathbb{F}_p$ est une extension finie et donc $\mathbb{F}_p(x) = \mathbb{F}_{p^n}$ pour un $n \geq 1$. Posons $n = q_1^{\alpha_1}...q_s^{\alpha_s}$ avec $q_i \in \mathbb{P}$

deux à deux distincts et $\alpha_i \geq 1$ pour tout $i \in \{1, \cdots, s\}$.
Montrons que $\mathbb{F}_{p^n} = \mathbb{F}_p\left(\bigcup_{i=1}^{s} \mathbb{F}_{p^{q_i^{\alpha_i}}}\right)$. Posons $\Omega_s := \mathbb{F}_p\left(\bigcup_{i=1}^{s} \mathbb{F}_{p^{q_i^{\alpha_i}}}\right)$, comme $q_i^{\alpha_i} | n$, on a $\mathbb{F}_{p^{q_i^{\alpha_i}}} \subseteq \mathbb{F}_{p^n}$ pour tuot $i \in \{1, \cdots, s\}$. On en déduit que $\Omega_s \subseteq \mathbb{F}_{p^n}$. Il suffit donc de montrer que $[\Omega_s : \mathbb{F}_p] = n$. Procédons par réccurence sur $s \in \mathbb{N}^*$.
Pour le cas $s = 1$, on a bien $[\Omega_1 : \mathbb{F}_p] = [\mathbb{F}_{p^{q_1^{\alpha_1}}} : \mathbb{F}_p] = q_1^{\alpha_1}$. Supposons que $[\Omega_{s-1} : \mathbb{F}_p] = q_1^{\alpha_1} ... q_{s-1}^{\alpha_{s-1}}$ et montrons que $[\Omega_s : \mathbb{F}_p] = n$. On a :

$$[\Omega_s : \mathbb{F}_p] = [\Omega_s : \Omega_{s-1}][\Omega_{s-1} : \mathbb{F}_p] \overset{hyp.}{=} q_1^{\alpha_1} ... q_{s-1}^{\alpha_{s-1}} [\Omega_s : \Omega_{s-1}].$$

De plus, on a le dessin suivant :



Comme $n/q_s^{\alpha_s}$ et $q_s^{\alpha_s}$ sont premiers entre eux, on a :

$$q_s^{\alpha_s} \Big| [\Omega_{s-1}(\mathbb{F}_{p^{q_s^{\alpha_s}}}) : \Omega_{s-1}] \leq [\mathbb{F}_{p^{q_s^{\alpha_s}}} : \mathbb{F}_p] = q_s^{\alpha_s}.$$

D'où

$$[\Omega_s : \Omega_{s-1}] = [\Omega_{s-1}(\mathbb{F}_{p^{q_s^{\alpha_s}}}) : \Omega_{s-1}] = q_s^{\alpha_s}.$$

Ainsi, $[\Omega_s : \mathbb{F}_p] = q_1^{\alpha_1} ... q_{s-1}^{\alpha_{s-1}} q_s^{\alpha_s} = n$. D'où la réccurence.
On peut ainsi en déduire que

$$x \in \mathbb{F}_{p^n} = \mathbb{F}_p\left(\bigcup_{i=1}^{s} \mathbb{F}_{p^{q_i^{\alpha_i}}}\right) \subseteq \mathbb{F}_p\left(\bigcup_{i=1}^{s} L_{q_i}\right) \subseteq \mathbb{F}_p\left(\bigcup_{q \in \mathbb{P}} L_q\right).$$

Ainsi $\overline{\mathbb{F}}_p \subseteq \mathbb{F}_p\left(\bigcup_{q \in \mathbb{P}} L_q\right)$. D'où l'égalité $\boxed{\overline{\mathbb{F}}_p = \mathbb{F}_p\left(\bigcup_{q \in \mathbb{P}} L_q\right)}$ car l'inclusion inverse est immédiate.
$\star$ $\mathbb{F}_p\left(\bigcup_{q \neq q'} L_q\right) \cap L_{q'} = \mathbb{F}_p$ pour tout q' premier. En effet :
- Si $x \in L_{q'}$, alors il existe un $m \geq 1$ tel que $x \in \mathbb{F}_{p^{(q')^m}}$ et ainsi :

$$[\mathbb{F}_p(x) : \mathbb{F}_p] \mid [\mathbb{F}_{p^{(q')^m}} : \mathbb{F}_p] = (q')^m.$$

- Si $x \in \mathbb{F}_p\left(\bigcup_{q \neq q'} L_q\right)$, alors $x \in \mathbb{F}_p\left(\bigcup_{i=1}^{s} \mathbb{F}_{p^{q_i^{\alpha_i}}}\right) = \mathbb{F}_{p^n}$ avec $n = q_1^{\alpha_1} ... q_s^{\alpha_s}$, $q_i \neq q'$ et $\alpha_1 \geq 1$.
Ainsi, $[\mathbb{F}_p(x) : \mathbb{F}_p] \mid [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. Par conséquent, $[\mathbb{F}_p(x) : \mathbb{F}_p] \mid pgcd(n, (q')^m) = 1$ et donc $[\mathbb{F}_p(x) : \mathbb{F}_p] = 1$. On en déduit alors que $\mathbb{F}_p(x) = \mathbb{F}_p$ et que $x \in \mathbb{F}_p$.
Ainsi, $\mathbb{F}_p\left(\bigcup_{q \neq q'} L_q\right) \cap L_{q'} \subseteq \mathbb{F}_p$. L'inclusion inverse étant immédiate, on peut en déduire l'égalité $\boxed{\mathbb{F}_p\left(\bigcup_{q \neq q'} L_q\right) \cap L_{q'} = \mathbb{F}_p}$.

On peut alors appliquer le théorème 3.7 et en déduire que $\boxed{Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \prod_{q\in\mathbb{P}} Gal(L_q/\mathbb{F}_p)}$.

Le but maintenant est de déterminer $Gal(L_q/\mathbb{F}_p)$. Pour tout $q \in \mathbb{P}$, posons

$$\mathscr{G}_q := \{F \subseteq L_q \mid F/\mathbb{F}_p \text{ galoisienne finie}\}.$$

Alors $\mathscr{G}_q$ est un ensemble ordonné filtrant à droite. Ainsi :

$$Gal(L_q/\mathbb{F}_p) = \varprojlim_{\mathscr{G}_q} Gal(F/\mathbb{F}_p) = \varprojlim Gal(\mathbb{F}_{p^{q^n}}/\mathbb{F}_p) = \varprojlim \mathbb{Z}/q^n\mathbb{Z} = \mathbb{Z}_q.$$

D'où l'isomorphisme $\boxed{Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p) \cong \prod_{p\in\mathbb{P}} \mathbb{Z}_q}$.

□

3.2 Extension cyclotomique maximale du corps des rationnels

Dans ce paragraphe, on étudiera l'extension cyclotomique maximale du corps des rationnels $\mathbb{Q}$. Plus précisément, soit $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$, posons

$$\begin{aligned}\mathscr{F} &= \{F \mid \mathbb{Q} \subseteq F \subseteq \overline{\mathbb{Q}} \text{ et } F \text{ est une extension cyclotomique de } \mathbb{Q}\}\\ &= \{\mathbb{Q}(\xi) \mid \xi \text{ une racine primitive } n\text{-ième de l'unité avec } n \in \mathbb{N}^*\}\end{aligned}$$

et

$$K = \mathbb{Q}\Big(\bigcup_{F\in\mathscr{F}} F\Big).$$

Alors $\mathscr{F}$ est filtrant à droite par le lemme 3.9 et K/k est une extension galoisienne de degré infini. On appelle *K l'extension cyclotomique maximale du corps de rationnels.*

Lemme 3.9. *Soit ξ_r (resp. ξ_n) une racine primitive r-ième (resp. n-ième) de l'unité avec $r \in \mathbb{N}^*$ (resp. $n \in \mathbb{N}^*$). Alors :*
(i) $\mathbb{Q}(\xi_r, \xi_n) = \mathbb{Q}(\xi_m)$ avec $m = ppcm(r, n)$;
(ii) $\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_d)$ avec $d = pgcd(r, n)$.

Preuve. (i) Comme $ord(\xi_r) = r|m$ et $ord(\xi_n) = n|m$, on en déduit que $\xi_r, \xi_n \in \mathbb{Q}(\xi_m)$. D'où $\mathbb{Q}(\xi_r, \xi_n) \subseteq \mathbb{Q}(\xi_m)$. Réciproquement, on a $ord((\xi_m)^{\frac{m}{r}}) = r$ et $ord((\xi_m)^{\frac{m}{n}}) = n$. Or, $\frac{m}{r} = \frac{n}{d}$ et $\frac{m}{n} = \frac{r}{d}$, donc $\frac{m}{r}$ et $\frac{m}{n}$ sont premier entre eux, il existe donc $p, q \in \mathbb{Z}$ tels que $p\frac{m}{r} + q\frac{m}{n} = 1$. On en déduit que $\xi_m = (\xi_m)^{p\frac{m}{r}+q\frac{m}{n}} = ((\xi_m)^{\frac{m}{r}})^p((\xi_m)^{\frac{m}{n}})^q$, ainsi $\xi_m \in \mathbb{Q}(\xi_r, \xi_n)$. D'où $\mathbb{Q}(\xi_m) \subseteq \mathbb{Q}(\xi_r, \xi_n)$. Conclusion : $\boxed{\mathbb{Q}(\xi_m) = \mathbb{Q}(\xi_r, \xi_n)}$.
(ii) Comme $ord(\xi_d) = d$ et $d|r, d|n$, on en déduit que $\xi_d \in \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)$. D'où $\mathbb{Q}(\xi_d) \subseteq \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)$. Ainsi $[\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n) : \mathbb{Q}] \geq [\mathbb{Q}(\xi_d) : \mathbb{Q}] = \varphi(d)$.
D'après le lemme 3.3,

$$Gal(\mathbb{Q}(\xi_r, \xi_n)/\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)) \cong Gal(\mathbb{Q}(\xi_r)/\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)) \times Gal(\mathbb{Q}(\xi_n)/\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)).$$

D'après le théorème de Galois (1.17),

$$\begin{aligned}|Gal(\mathbb{Q}(\xi_r, \xi_n)/\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n))| &= [\mathbb{Q}(\xi_r, \xi_n) : \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)],\\ |Gal(\mathbb{Q}(\xi_r)/\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n))| &= [\mathbb{Q}(\xi_r) : \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)],\\ |Gal(\mathbb{Q}(\xi_n)/\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n))| &= [\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)].\end{aligned}$$

On en déduit que

$$[\mathbb{Q}(\xi_r, \xi_n) : \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)] = [\mathbb{Q}(\xi_r) : \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)] \cdot [\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)].$$

On a donc :

$$\begin{aligned}[\mathbb{Q}(\xi_r, \xi_n) : \mathbb{Q}] &= [\mathbb{Q}(\xi_r, \xi_n) : \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)] \cdot [\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n) : \mathbb{Q}]\\ &= [\mathbb{Q}(\xi_r) : \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)] \cdot [\mathbb{Q}(\xi_n) : \mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n)] \cdot [\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n) : \mathbb{Q}]\\ &= \frac{[\mathbb{Q}(\xi_r) : \mathbb{Q}] \cdot [\mathbb{Q}(\xi_n) : \mathbb{Q}]}{[\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n) : \mathbb{Q}]} = \frac{\varphi(r) \cdot \varphi(n)}{[\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n) : \mathbb{Q}]}.\end{aligned}$$

Ainsi $[\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n) : \mathbb{Q}] = \dfrac{\varphi(r) \cdot \varphi(n)}{[\mathbb{Q}(\xi_r, \xi_n) : \mathbb{Q}]}$.
Remarquons que $\varphi(r)\varphi(n) = \varphi(d)\varphi(m)$. En effet, posons $r = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ (resp. $n = p_1^{\beta_1} \cdots p_s^{\beta_s}$) avec $s \in \mathbb{N}, \alpha_i$ (resp. β_i) $\in \mathbb{N}$ et p_i des nombres premiers deux à deux distincts. Alors

$$\begin{aligned}\varphi(r) &= \varphi(p_1^{\alpha_1} \cdots p_s^{\alpha_s}) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_s^{\alpha_s}),\\ \varphi(n) &= \varphi(p_1^{\beta_1} \cdots p_s^{\beta_s}) = \varphi(p_1^{\beta_1}) \cdots \varphi(p_s^{\beta_s}).\end{aligned}$$

On en déduit que

$$\begin{aligned}\varphi(r)\varphi(n) &= \varphi(p_1^{\alpha_1})\cdots\varphi(p_s^{\alpha_s})\varphi(p_1^{\beta_1})\cdots\varphi(p_s^{\beta_s})\\ &= \varphi(p_1^{\mu_1})\cdots\varphi(p_s^{\mu_s})\varphi(p_1^{\nu_1})\cdots\varphi(p_s^{\nu_s}) = \varphi(d)\varphi(m),\end{aligned}$$

où $\mu_i = \min\{\alpha_i, \beta_i\}$ et $\nu_i = \max\{\alpha_i, \beta_i\}$ pour $1 \leq i \leq s$. On a donc

$$[\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n) : \mathbb{Q}] = \frac{\varphi(d)\cdot\varphi(m)}{[\mathbb{Q}(\xi_r, \xi_n) : \mathbb{Q}]}.$$

D'après (i), $[\mathbb{Q}(\xi_r, \xi_n) : \mathbb{Q}] = [\mathbb{Q}(\xi_m) : \mathbb{Q}] = \varphi(m)$, on en déduit que

$$[\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n) : \mathbb{Q}] = \varphi(d).$$

D'où $\boxed{\mathbb{Q}(\xi_r) \cap \mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_d)}$.

□

Définition 3.10. Soit I un ensemble d'indices pré-ordonné par rapport à $\leq$ qui est filtrant à droite. Un sous-ensemble J de I est dit *cofinal* si il est filtrant à droite et si pour tout $i \in I$, il existe un $j \in J$ tel que $i \leq j$.

D'après le théorème de *Kronecker-Weber* ([4], page 45, théorème 2), toute extension abélienne de $\mathbb{Q}$ est contenue dans une extension cyclotomique de $\mathbb{Q}$ et ainsi K est égal à la clôture abélienne de $\mathbb{Q}$. Posons maintenant

$$\mathscr{G} = \{F \mid \mathbb{Q} \subseteq F \subseteq K \text{ et } F/\mathbb{Q} \text{ est une extension galoisienne finie}\}.$$

Alors $\mathscr{F}$ est un sous-ensemble cofinal de $\mathscr{G}$ par le théorème de *Kronecker-Weber*.

Lemme 3.11. *Soient I un ensemble d'indices pré-ordonné par rapport à $\leq$ qui est filtrant à droite et J un sous-ensemble cofinal de I. Soit $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ un système inverse d'ensembles (resp. groupes, espaces topologiques, groupes topologiques) et d'applications (resp. homomorphismes, application continues, homomorphismes continus). Alors* $\varprojlim_I S_i = \varprojlim_J S_i$.

Preuve. Posons $S = \varprojlim_I S_i$ et $\pi_i : S \longrightarrow S_i$ pour tout $i \in I$.

$\star$ $\pi_{ji} \circ \pi_j = \pi_i$ pour tout $i, j \in J$ avec $i \leq j$. En effet, comme S est la limite inverse du système inverse $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$, on a $\pi_{ji} \circ \pi_j = \pi_i$ pour tout $i, j \in I$ avec $i \leq j$.

$\star$ Si S' est un ensemble (resp. groupe, espace topologique, groupe topologique) et si pour tout $i \in J$, $\pi'_i : S' \longrightarrow S_i$ est une application (resp. homomorphisme, application continue, homomorphisme continu) telle que $\pi_{ji} \circ \pi'_j = \pi'_i$ pour tout $i, j \in J$ avec $i \leq j$, définissons

$$\begin{array}{rccc}\theta : & S' & \longrightarrow & S\\ & s & \longmapsto & \theta(s)\end{array}$$

où $\theta(s) = (\pi_{j_i,i} \circ \pi'_{j_i}(s))_{i\in I}$ avec $j_i \in J$ et $i \leq j_i$ (ceci est possible car J est filtrant à droite).

Alors l'application θ est bien définie. En effet, si $j_i, j'_i \in J$ avec $i \leq j_i$ et $i \leq j'_i$, alors comme J est filtrant à droite, il existe un $k \in J$ tel que $j_i \leq k, j'_i \leq k$. De plus, si $s \in S'$, alors on a :

$$\begin{aligned}\pi_{j_i,i} \circ \pi'_{j_i}(s) &= \pi_{j_i,i} \circ (\pi_{k,j_i} \circ \pi'_k)(s) = (\pi_{j_i,i} \circ \pi_{k,j_i}) \circ \pi'_k(s) = \pi_{k,i} \circ \pi'_k(s),\\ \pi_{j'_i,i} \circ \pi'_{j'_i}(s) &= \pi_{j'_i,i} \circ (\pi_{k,j'_i} \circ \pi'_k)(s) = (\pi_{j'_i,i} \circ \pi_{k,j'_i}) \circ \pi'_k(s) = \pi_{k,i} \circ \pi'_k(s).\end{aligned}$$

D'où $\pi_{j_i,i} \circ \pi'_{j_i}(s) = \pi_{j'_i,i} \circ \pi'_{j'_i}(s)$. Ainsi θ est bien une application (resp. homomorphisme, application continue, homomorphisme continu).
De plus, $\pi_i \circ \theta = \pi'_i$ pour tout $i \in J$. En effet, si $s \in S'$, alors

$$(\pi_i \circ \theta)(s) = \pi_{j_i,i} \circ \pi'_{j_i}(s) = \pi'_i(s).$$

Il reste à montrer l'unicité de θ. Soit $\theta' : S' \longrightarrow S$ une application (resp. homomorphisme, application continue, homomorphisme continu) vérifiant $\pi_i \circ \theta' = \pi'_i$ pour tout $i \in I$. Alors

$$\theta(s) = (\pi_i \circ \theta(s))_{i\in I} = (\pi'_i(s))_{i\in I} = (\pi_i \circ \theta'(s))_{i\in I} = \theta'(s).$$

D'où $\theta = \theta'$. Ainsi $\varprojlim_I S_i$ vérifie la propriété universelle de la limite projective des S_i pour $i \in J$ et donc : $\boxed{\varprojlim_I S_i = \varprojlim_J S_i}$.

□

Proposition 3.12. *$Gal(K/\mathbb{Q}) \cong \varprojlim(\mathbb{Z}/n\mathbb{Z})^\times$.*

Preuve. D'après le théorème de *Krull*, le théorème 1.15 et le lemme 3.11,

$$Gal(K/\mathbb{Q}) \overset{2.31}{\cong} \varprojlim_{\mathscr{G}} Gal(F/\mathbb{Q}) \overset{3.11}{\cong} \varprojlim_{\mathscr{F}} Gal(F/\mathbb{Q}) \overset{1.15}{\cong} \varprojlim(\mathbb{Z}/n\mathbb{Z})^\times.$$

D'où le résultat.

□

Soit p un nombre premier. Posons

$$\mathscr{F}_p = \{\mathbb{Q}(\xi) \mid \xi \text{ une racine primitive } p^n\text{-ième de l'unité avec } n \in \mathbb{N}^*\}$$

et

$$T_p = \mathbb{Q}\Big(\bigcup_{F\in\mathscr{F}_p} F\Big).$$

Alors $T_p/\mathbb{Q}$ est une extension galoisienne de degré infini pour tout p premier.

Proposition 3.13. *Soit p un nombre premier. Soient T_p et K définis comme ci-dessus. Alors :*
(i) $K = \mathbb{Q}\Big(\bigcup_{p\in\mathbb{P}} T_p\Big)$;
(ii) $\mathbb{Q}\Big(\bigcup_{p\neq q} T_p\Big) \cap T_q = \mathbb{Q}$ pour tout q premier ;
(iii) $Gal(K/\mathbb{Q}) \cong \prod_{p\in\mathbb{P}} Gal(T_p/\mathbb{Q})$.

Preuve. (i) Il suffit de montrer que $K \subseteq \mathbb{Q}\Big(\bigcup_{p\in\mathbb{P}} T_p\Big)$. Soit $x \in K$. Alors $\mathbb{Q}(x)/\mathbb{Q}$ est une extension abélienne car K l'est, et ainsi, par le théorème de *Kronecker-Weber*, il existe un $n \in \mathbb{N}^*$ et ξ_n une racine primitive n-ième de l'unité telle que $\mathbb{Q}(x) \subseteq \mathbb{Q}(\xi_n)$. Posons $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, d'après le premier point du lemme 3.9, on a

$$\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_{p_1^{\alpha_1}}, \cdots, \xi_{p_s^{\alpha_s}}) \subseteq \mathbb{Q}(T_{p_1} \cup \cdots \cup T_{p_s}) \subseteq \mathbb{Q}\Big(\bigcup_{p\in\mathbb{P}} T_p\Big).$$

On en déduit que $x \in \mathbb{Q}(x) \subseteq \Big(\bigcup_{p\in\mathbb{P}} T_p\Big)$. D'où $\boxed{K \subseteq \mathbb{Q}\Big(\bigcup_{p\in\mathbb{P}} T_p\Big)}$.

(ii) Il suffit de montrer que $\mathbb{Q}\Big(\bigcup_{p\neq q} T_p\Big)\cap T_q \subseteq \mathbb{Q}$. Notons d'abord que $\mathbb{Q}(A) = \bigcup_{B\subseteq A \text{ fini}} \mathbb{Q}(B)$. Si $x \in \mathbb{Q}\Big(\bigcup_{p\neq q} T_p\Big)$, alors il existe

$$S_1 := \{p_i^{\alpha_{i,t_i}} | t_i \in \mathbb{N}^*, \alpha_{i,t_i} \in \mathbb{N}, i = 1, \cdots, s, s \in \mathbb{N}^*\}$$

tel que $x \in \mathbb{Q}(S_1)$. D'après le premier point du lemme 3.9, $\mathbb{Q}(S_1) = \mathbb{Q}(\xi_{p_1^{\alpha_1}}, \cdots, \xi_{p_s^{\alpha_s}}) = \mathbb{Q}(\xi_n)$ où $\alpha_i = \max_{1\leq j\leq t_i} \alpha_{i,j}$ pour $1 \leq i \leq s$ et $n = p_1^{\alpha_1}\cdots p_s^{\alpha_s}$. De même, si $x \in \mathbb{Q}(T_q)$, il existe

$$S_2 = \{q^{\beta_i} | \beta_i \in \mathbb{N}, i = 1, \cdots, t, t \in \mathbb{N}^*\}$$

tel que $x \in \mathbb{Q}(S_2)$. D'après le premier point du lemme 3.9, $\mathbb{Q}(S_2) = \mathbb{Q}(\xi_{q^\beta})$ où $\beta = \max_{1\leq i\leq t} \beta_i$. Comme n et q sont premiers entre eux, on en déduit que $\mathbb{Q}(\xi_n)\cap\mathbb{Q}(\xi_{q^\beta}) = \mathbb{Q}$ par le deuxième point du lemme 3.9, c'est-à-dire, $x \in \mathbb{Q}$. D'où $\boxed{\mathbb{Q}\Big(\bigcup_{p\neq q} T_p\Big) \cap T_q \subseteq \mathbb{Q}}$.

(iii) Il suffit d'appliquer le théorème 3.7.

□

Grâce à la proposition 3.13, étudier la structure de $Gal(K/\mathbb{Q})$ revient à étudier la structure de $Gal(T_p/\mathbb{Q})$. Posons

$$\mathscr{G}_p = \{F \mid \mathbb{Q} \subseteq F \subseteq T_p \text{ et } F/\mathbb{Q} \text{ est une extension galoisienne finie}\},$$

alors $\mathscr{F}_p$ est un sous-ensemble cofinal de $\mathscr{G}_p$ par le théorème de *Kronecker-Weber* et le lemme 3.9.

Lemme 3.14. *Soit I un ensemble d'indice totalement ordonné. Soient G un ensemble (resp. groupe, espace topologique, groupe topologique) et $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ un système inverse d'ensembles (resp. groupes, espaces topologiques, groupes topologiques) et d'applications (resp. homomorphismes, applications continues, homomorphismes continus). Soit*

$$\begin{array}{rccc} \widetilde{\pi}_{ji}: & G\times S_j & \longrightarrow & G\times S_i \\ & (g, s_j) & \longmapsto & (g, \pi_{ji}(s_j)) \end{array}$$

une application (resp. homomorphisme, application continue, homomorphisme continu) avec $i, j \in I$ tels que $i \leq j$. Alors $((G\times S_i)_{i\in I}, (\widetilde{\pi}_{ji})_{i\leq j})$ est un système inverse d'ensembles (resp. groupes, espaces topologiques, groupes topologiques) et d'applications (resp. homomorphismes, applications continues, homomorphismes continus) et $\varprojlim(G\times S_i) \cong G\times \varprojlim S_i$.

Preuve. Notons que $\widetilde{\pi}_{ii} = id_{G\times S_i}$ pour tout $i \in I$ et $\widetilde{\pi}_{ji}\circ\widetilde{\pi}_{kj} = \widetilde{\pi}_{ki}$ pour $i \leq j \leq k$. En effet, si $(g, s_i) \in G\times S_i$ et si $(g, s_k) \in G\times S_k$, alors

$$\widetilde{\pi}_{ii}(g, s_i) = (g, \pi_{ii}(s_i)) = (g, s_i) = id_{G\times S_i}(g, s_i)$$
$$(\widetilde{\pi}_{ji}\circ\widetilde{\pi}_{kj})(g, s_k) = \widetilde{\pi}_{ji}(g, \pi_{kj}(s_k)) = (g, (\pi_{ji}\circ\pi_{kj})(s_k)) = (g, \pi_{ki}(s_k)) = \widetilde{\pi}_{ki}(g, s_k).$$

On en déduit que $((G\times S_i)_{i\in I}, (\widetilde{\pi}_{ji})_{i\leq j})$ est un système inverse d'ensembles (resp. groupes, espaces topologiques, groupes topologiques) et d'applications (resp. homomorphismes, applications continues, homomorphismes continus). Il reste à montrer que $\varprojlim(G\times S_i) \cong G\times\varprojlim S_i$. Posons $(S, (\pi_i)_{i\in I})$ la limite projective du système inverse $((S_i)_{i\in I}, (\pi_{ji})_{i\leq j})$ et

$$\begin{array}{rccc} \widetilde{\pi}_i: & G\times S & \longrightarrow & G\times S_i \\ & (g, s) & \longmapsto & (g, \pi_i(s)) \end{array}$$

pour tout $i \in I$, alors $\widetilde{\pi}_{ji} \circ \widetilde{\pi}_j = \widetilde{\pi}_i$ pour tout $i \leq j$. En effet, si $(g, s) \in G \times S$, alors

$$(\widetilde{\pi}_{ji} \circ \widetilde{\pi}_j)(g, s) = \widetilde{\pi}_{ji}(g, \pi_j(s)) = (g, (\pi_{ji} \circ \pi_j)(s)) = (g, \pi_i(s)) = \widetilde{\pi}_i(g, s).$$

Soient H un ensemble (resp. groupe, espace topologique, groupe topologique) et $\rho_i : H \longrightarrow G \times S_i$ une application (resp. homomorphisme, application continue, homomorphisme continu) pour tout $i \in I$ telle que $\widetilde{\pi}_{ji} \circ \rho_j = \rho_i$ pour tout $i \leq j$. Posons $\rho_i = (\rho_i^{(1)}, \rho_i^{(2)})$ pour tout $i \in I$, où $\rho_i^{(1)} : H \longrightarrow G$ et $\rho_i^{(2)} : H \longrightarrow S_i$ sont des applications (resp. homomorphismes, applications continues, homomorphismes continus), alors :

$$\rho_i(h) = (\rho_i^{(1)}(h), \rho_i^{(2)}(h)),$$
$$(\widetilde{\pi}_{ji} \circ \rho_j)(h) = \widetilde{\pi}_{ji}(\rho_j^{(1)}(h), \rho_j^{(2)}(h)) = (\rho_j^{(1)}(h), (\pi_{ji} \circ \rho_j^{(2)})(h)),$$

pour tout $h \in H$ et $i \leq j$. On en déduit que

$$\rho_i^{(1)} = \rho_j^{(1)} \text{ et } \rho_i^{(2)} = \pi_{ji} \circ \rho_j^{(2)} \qquad (*)$$

pour tout $i \leq j$. Comme I est totalement ordonné, on a $\rho_i^{(1)} = \rho_j^{(1)}$ pour tout $i, j \in I$. Posons $\rho_0 = \rho_i^{(1)}$ et

$$\begin{array}{rccc} \rho : & H & \longrightarrow & G \times S \\ & h & \longmapsto & (\rho_0(h), (\rho_i^{(2)}(h))_{i \in I}), \end{array}$$

alors ρ est une application (resp. homomorphisme, application continue, homomorphisme continu) telle que $\widetilde{\pi}_i \circ \rho = \rho_i$ pour tout $i \in I$. En effet, si $h \in H$, alors

$$(\widetilde{\pi}_i \circ \rho)(h) = \widetilde{\pi}_i(\rho_0(h), (\rho_j^{(2)}(h))_{j \in I}) = (\rho_0(h), \rho_i^{(2)}(h)) = \rho_i(h).$$

Montrons maintenant l'unicité de ρ. Soit $\widetilde{\rho} : H \longrightarrow G \times S$ une application (resp. homomorphisme, application continue, homomorphisme continu) telle que $\widetilde{\pi}_i \circ \widetilde{\rho} = \rho_i$ pour tout $i \in I$. Posons $\widetilde{\rho} = (\widetilde{\rho}^{(1)}, \widetilde{\rho}^{(2)})$, alors :

$$\rho_i(h) = (\widetilde{\rho}_0(h), \widetilde{\rho}_i^{(2)}(h)),$$
$$(\widetilde{\pi}_i \circ \widetilde{\rho})(h) = \widetilde{\pi}_i(\widetilde{\rho}^{(1)}(h), \widetilde{\rho}^{(2)}(h)) = (\widetilde{\rho}^{(1)}(h), (\pi_i \circ \widetilde{\rho}^{(2)})(h)).$$

On en déduit que $\widetilde{\rho}^{(1)} = \widetilde{\rho}_0$ et $\pi_i \circ \widetilde{\rho}^{(2)} = \widetilde{\rho}_i^{(2)}$ pour tout $i \in I$ et ainsi, $\widetilde{\rho}^{(1)} = \widetilde{\rho}_0$ et $\widetilde{\rho}^{(2)} = (\widetilde{\rho}_i^{(2)})_{i \in I}$. D'où $\widetilde{\rho} = \rho$. Ainsi $G \times \varprojlim S_i$ vérifie la propriété universelle de la limite projective des $G \times S_i$ et donc : $\boxed{\varprojlim (G \times S_i) \cong G \times \varprojlim S_i}$.

□

Lemme 3.15. *Pour tout p premier, $Gal(T_p/\mathbb{Q}) \cong \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times$.*

Preuve. D'après le théorème de *Krull*, le théorème 1.15 et le lemme 3.11,

$$Gal(T_p/\mathbb{Q}) \overset{2.31}{\cong} \varprojlim_{\mathscr{G}_p} Gal(F/\mathbb{Q}) \overset{3.11}{\cong} \varprojlim_{\mathscr{F}_p} Gal(F/\mathbb{Q}) \overset{1.15}{\cong} \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times.$$

D'où le résultat.

□

Lemme 3.16. (La structure de $(\mathbb{Z}/n\mathbb{Z})^\times$). *Soit $n = 2^t p_1^{t_1} \cdots p_s^{t_s}$ avec $s \in \mathbb{N}, t_i \in \mathbb{N}^*$ et p_i des nombres premiers deux à deux distincts. Alors :*
(i) $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/2^t\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{t_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{t_s}\mathbb{Z})^\times$;
(ii) $(\mathbb{Z}/2\mathbb{Z})^\times = \{\bar{1}\}$, $(\mathbb{Z}/2^2\mathbb{Z})^\times = \{\bar{1}, \bar{3}\} \cong \mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/2^t\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{t-2}\mathbb{Z}$ *pour* $t \geq 3$;
(iii) $(\mathbb{Z}/p^t\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{t-1}\mathbb{Z}$ *pour p premier impair et* $t \geq 1$.

Preuve. (i) D'après le théorème des restes chinois

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/2^t\mathbb{Z} \times \mathbb{Z}/p_1^{t_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{t_s}\mathbb{Z}.$$

De plus,

$$\begin{aligned}
\overline{x}^{[n]} \in (\mathbb{Z}/n\mathbb{Z})^\times &\Leftrightarrow pgcd(x,n) = 1;\\
&\Leftrightarrow pgcd(x,2^t) = pgcd(x,p_i^{t_i}) = 1 \text{ avec } i = 1,\cdots,s;\\
&\Leftrightarrow \overline{x}^{[2^t]} \in (\mathbb{Z}/2^t\mathbb{Z})^\times, \overline{x}^{[p_i^{t_i}]} \in (\mathbb{Z}/p_i^{t_i}\mathbb{Z})^\times \text{ avec } i = 1,\cdots,s;\\
&\Leftrightarrow (\overline{x}^{[2^t]}, \overline{x}^{[p_1^{t_1}]}, \cdots, \overline{x}^{[p_s^{t_s}]}) \in (\mathbb{Z}/2^t\mathbb{Z})^\times \times (\mathbb{Z}/p_1^{t_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{t_s}\mathbb{Z})^\times.
\end{aligned}$$

D'où le résultat.
(ii) Les cas $t = 1$ et $t = 2$ sont clairs. Supposons que $t \geq 3$.
$\star$ Montrons que $\overline{5} \in (\mathbb{Z}/2^t\mathbb{Z})^\times$ est d'ordre 2^{t-2}. Pour cela, montrons d'abord par récurrence sur $l \in \mathbb{N}$ que $(1+2^2)^{2^l} = 1 + 2^{l+2}r$ avec r impair.
L'égalité est vérifiée pour $l = 0$ et $r = 1$. Supposons que $(1+2^2)^{2^l} = 1 + 2^{l+2}r$ avec r impair, alors

$$(1+2^2)^{2^{l+1}} = (1+2^{l+2}r)^2 = 1 + 2^{l+3}r + 2^{2l+4}r^2 = 1 + 2^{l+3}(r + 2^{l+1}r^2)$$

avec $r + 2^{l+1}r^2$ impair car r est impair. D'où la récurrence.
Par conséquent, $(1+2^2)^{2^{t-k}} = 1 + 2^{t-k+2}r_k$ avec $2 \leq k \leq t$ et r_k impairs. On en déduit que

$$\overline{5}^{2^{t-2}} = \overline{1 + 2^t r_2} = \overline{1} \text{ et } \overline{5}^{2^{t-k}} = \overline{1 + 2^{t-k+2}r_k} \neq \overline{1} \text{ pour } k = 3,\cdots,t.$$

D'où $\boxed{ord(\overline{5}) = 2^{t-2}}$.
$\star$ Montrons que $\overline{-1} \notin \langle\overline{5}\rangle$. Il est clair que $\overline{-1}$ est d'ordre 2. Notons que $ord(\overline{5}^{2^{t-3}}) = 2$ car $ord(\overline{5}) = 2^{t-2}$. Ainsi, si $\overline{-1} \in \langle\overline{5}\rangle$, alors $\overline{-1} = \overline{5}^{2^{t-3}} = \overline{1 + 2^{t-1}r_3}$. On en déduit que $2(1 + 2^{t-2}r_3) \in 2^t\mathbb{Z}$, donc $1 \in 2^{t-2}\mathbb{Z}$, contradiction. D'où $\boxed{\overline{-1} \notin \langle\overline{5}\rangle}$.
$\star$ Montrons que $(\mathbb{Z}/2^t\mathbb{Z})^\times = \langle\overline{-1}, \overline{5}\rangle \cong \langle\overline{-1}\rangle \times \langle\overline{5}\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{t-2}\mathbb{Z}$. Comme $(\mathbb{Z}/2^t\mathbb{Z})^\times$ est abélien, $\langle\overline{-1}\rangle$ et $\langle\overline{5}\rangle$ sont distingués dans $(\mathbb{Z}/2^t\mathbb{Z})^\times$. De plus, $ord(\overline{-1}) = 2$ et $ord(\overline{5}) = 2^{t-2}$. Ainsi, on en déduit que

$$\boxed{\langle\overline{-1}, \overline{5}\rangle \cong \langle\overline{-1}\rangle \times \langle\overline{5}\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{t-2}\mathbb{Z}}.$$

D'après le premier théorème d'isomorphisme de groupes,

$$\frac{\langle\overline{-1}, \overline{5}\rangle}{\langle\overline{-1}\rangle} \cong \frac{\langle\overline{5}\rangle}{\langle\overline{-1}\rangle \cap \langle\overline{5}\rangle}.$$

On en déduit que

$$|\langle\overline{-1}, \overline{5}\rangle| = \frac{|\langle\overline{-1}\rangle| \cdot |\langle\overline{5}\rangle|}{|\langle\overline{-1}\rangle \cap \langle\overline{5}\rangle|} = |\langle\overline{-1}\rangle| \cdot |\langle\overline{5}\rangle| = 2^{t-1} = \varphi(2^t) = |(\mathbb{Z}/2^t\mathbb{Z})^\times|.$$

D'où $\boxed{(\mathbb{Z}/2^t\mathbb{Z})^\times = \langle\overline{-1}, \overline{5}\rangle}$.
(iii) $\star$ Montrons qu'il existe un élément $\overline{q} \in (\mathbb{Z}/p^t\mathbb{Z})^\times$ d'ordre $p-1$. Posons

$$\pi : \mathbb{Z}/p^t\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

la surjection canonique. Choisissons $\overline{x}^{[p]} \in (\mathbb{Z}/p\mathbb{Z})^\times$ tel que $ord(\overline{x}^{[p]}) = p-1$, alors il existe un $\overline{y}^{[p^t]} \in (\mathbb{Z}/p^t\mathbb{Z})^\times$ tel que $\pi(\overline{y}^{[p^t]}) = \overline{x}^{[p]}$. Posons $u = ord(\overline{y}^{[p^t]})$, alors

$$\overline{1}^{[p]} = \pi((\overline{y}^{[p^t]})^u) = (\pi(\overline{y}^{[p^t]}))^u = (\overline{x}^{[p]})^u,$$

et on en déduit que $p-1|u$. Donc $\boxed{ord((\overline{y}^{[p^t]})^{\frac{u}{p-1}}) = p-1}$, c'est le $\overline{q}$ recherché.
$\star$ Montrons que $\overline{1+p} \in (\mathbb{Z}/p^t\mathbb{Z})^\times$ est d'ordre p^{t-1}. Pour cela, montrons d'abord par récurrence sur $l \in \mathbb{N}$ que $(1+p)^{p^l} = 1 + p^{l+1}r$ avec $pgcd(r,p) = 1$.
L'égalité est vérifiée pour $l = 0$ et $r = 1$. Supposons que $(1+p)^{p^l} = 1 + p^{l+1}r$ avec $pgcd(r,p) = 1$, alors

$$\begin{aligned}(1+p)^{p^{l+1}} &= (1+p^{l+1}r)^p = \sum_{i=0}^{p} C_p^i (p^{l+1}r)^i \\ &= 1 + p \cdot p^{l+1}r + \frac{p(p+1)}{2} p^{2l+2} r^2 + p^{l+3}A \\ &= 1 + p^{l+2}r + p^{l+3}B = 1 + p^{l+2}(r + pB),\end{aligned}$$

où $pgcd(r,p) = 1$, $A = \sum_{i=3}^{p} C_p^i p^{(i-1)l+(i-3)} r^i$ et $B = \frac{p+1}{2} p^l r^2 + A$. Comme $pgcd(r,p) = 1$, on a $pgcd(r+pB, p) = 1$, d'où la récurrence.
Par conséquent, $(1+p)^{p^{t-k}} = 1 + p^t r_k$ avec $1 \leq k \leq t$ et $pgcd(r_k, p) = 1$. On en déduit que

$$\overline{1+p}^{p^{t-1}} = \overline{1+p^t r} = \overline{1} \text{ et } \overline{1+p}^{p^{t-k}} = \overline{1+p^{t-k+1}r_k} \neq \overline{1} \text{ pour } k = 2, \cdots, t.$$

D'où $\boxed{ord(\overline{1+p}) = p^{t-1}}$.
$\star$ Montrons que $(\mathbb{Z}/p^t\mathbb{Z})^\times = \langle \overline{q}, \overline{1+p} \rangle \cong \langle \overline{q} \rangle \times \langle \overline{1+p} \rangle \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{t-1}\mathbb{Z}$. Comme $(\mathbb{Z}/p^t\mathbb{Z})^\times$ est abélien, $\langle \overline{q} \rangle$ et $\langle \overline{1+p} \rangle$ sont distingués dans $(\mathbb{Z}/p^t\mathbb{Z})^\times$. De plus, $ord(\overline{q}) = p-1$ et $ord(\overline{1+p}) = p^{t-1}$. Ainsi, on en déduit que

$$\boxed{\langle \overline{q}, \overline{1+p} \rangle \cong \langle \overline{1} \rangle \times \langle \overline{1+p} \rangle \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{t-1}\mathbb{Z}}.$$

D'après le premier théorème d'isomorphisme de groupes,

$$\frac{\langle \overline{q}, \overline{1+p} \rangle}{\langle \overline{q} \rangle} \cong \frac{\langle \overline{1+p} \rangle}{\langle \overline{q} \rangle \cap \langle \overline{1+p} \rangle}.$$

On en déduit que

$$|\langle \overline{q}, \overline{1+p} \rangle| = \frac{|\langle \overline{q} \rangle| \cdot |\langle \overline{1+p} \rangle|}{|\langle \overline{q} \rangle \cap \langle \overline{1+p} \rangle|} = |\langle \overline{q} \rangle| \cdot |\langle \overline{1+p} \rangle| = (p-1)p^{t-1} = \varphi(p^t) = |(\mathbb{Z}/p^t\mathbb{Z})^\times|.$$

D'où $\boxed{(\mathbb{Z}/p^t\mathbb{Z})^\times = \langle \overline{q}, \overline{1+p} \rangle}$.

□

Corollaire 3.17. *$Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2) \times \prod_{p \geq 3} (\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p)$.*

Preuve. D'après la proposition 3.13 et les lemmes 3.14, 3.15, 3.16,

$$\begin{aligned}Gal(K/\mathbb{Q}) &\cong \prod_{p \in \mathbb{P}} Gal(T_p/\mathbb{Q}) \cong \prod_{p \in \mathbb{P}} \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times = \varprojlim (\mathbb{Z}/2^n\mathbb{Z})^\times \times \prod_{p \geq 3} \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^\times \\ &\cong (\mathbb{Z}/2\mathbb{Z} \times \varprojlim \mathbb{Z}/2^n\mathbb{Z}) \times \prod_{p \geq 3} (\mathbb{Z}/(p-1)\mathbb{Z} \times \varprojlim \mathbb{Z}/p^n\mathbb{Z}) \\ &\cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2) \times \prod_{p \geq 3} (\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p).\end{aligned}$$

D'où le résultat.

□

Références

[1] N. Bourbaki. *Topologie Générale*. Hermann, Paris, 1971.

[2] J. Calais. *Extensions de corps*. Ellipses, Paris, 2006.

[3] J. R. Munkres. *Topology*. Prentice-Hall, New Jersey, 1975.

[4] P. Ribenboim. *L'Arithmétique des Corps*. Hermann, Paris, 1972.