Théorie de Galois en dimension infinie

Bulois Michaël

10 juillet 2003

Introduction

Étant donnée une extension de corps galoisienne finie K/k, un théorème fondamental de la théorie de Galois, pour les extensions galoisiennes finies, relie de façon bijective les sous-extensions de K/k avec les sous-groupes du groupe de Galois $\mathrm{Gal}(K/k)$, de l'extension K/k. Ceci n'est plus vrai lorsque K/k est une extension de degré infini. Néanmoins, on peut voir K/k comme union d'extensions galoisiennes finies F/k et les éléments de $\mathrm{Gal}(K/k)$ sont entièrement définis par leurs restrictions aux sous-corps F. Ceci se formalise en considérant $\mathrm{Gal}(K/k)$ comme *limite inverse* (ou *limite projective*) des groupes $\mathrm{Gal}(F/k)$. Cette identification permet de munir $\mathrm{Gal}(K/k)$ d'une topologie. Grâce à cette topologie, nous pourrons énoncer un théorème de correspondance bijective entre les sous-extensions de K/k et les sous-groupes fermés de $\mathrm{Gal}(K/k)$. À titre d'exemple nous détaillerons le cas de certaines extensions infinies dont le groupe de Galois est isomorphe au groupe additif de l'anneau des entiers p-adiques $\mathbb{Z}_p$.

1 Passage des extensions finies aux extensions infinies

1.1 Limite projective

Soit $(S_i)_{i\in I}$ une famille d'ensembles. On suppose I ordonné et filtrant à droite, *i.e.*, $\forall (i,j) \in I^2$, $\exists k \in I$ tel que $k \geqslant i$ et $k \geqslant j$. Pour tout couple $(i,j) \in I^2$ tel que $i \leqslant j$ on se donne une application $\pi_{ji} : S_j \to S_i$ vérifiant les conditions :

1. π_{ii} est l'application identique de S_i (pour tout $i \in I$) ;
2. si $i \leqslant j \leqslant k$, alors $\pi_{ki} = \pi_{ji} \circ \pi_{kj}$.

On dit que $((S_i)_{i\in I}, (\pi_{ji})_{i\leqslant j})$ est un *système inverse* (ou *système projectif*) d'ensembles et d'applications. On appelle les applications π_{ji} les applications de liaison. Dans ces conditions, on a :

Théorème 1.1. *Il existe un ensemble S (unique à isomorphisme près) et une famille d'applications $\pi_i : S \to S_i$ ayant les propriétés suivantes :*

1. si $i \leqslant j$ alors $\pi_i = \pi_{ji} \circ \pi_j$;

2. *si S' est un ensemble, si pour tout $i \in I, \pi'_i : S' \to S_i$ est une application vérifiant $\pi'_i = \pi_{ji} \circ \pi'_j$ lorsque $i \leqslant j$, alors il existe une et une seule application $\theta : S' \to S$ telle que $\pi_i \circ \theta = \pi'_i$ pour tout $i \in I$.*

$$
\begin{tikzcd}
S_j \arrow[d, "\pi_{ji}"'] & S \arrow[l, "\pi_j"'] \arrow[dl, "\pi_i"] \\
S_i &
\end{tikzcd}
$$

On dit que S est la *limite projective* de la famille $(S_i)_{i\in I}$ par rapport aux applications $(\pi_{ji})_{i\leqslant j}$. On note alors $S = \varprojlim S_i$.

Démonstration. Il suffit de prendre pour S le sous-ensemble de $\prod_{i\in I} S_i$ composé des éléments $(s_i)_{i\in I}$ tels que pour tout $i \leqslant j$, on ait $\pi_{ji}(s_j) = s_i$ et de prendre $\pi_i : S \to S_i$ définie pour $s = (s_i)_{i\in I} \in S$ par $\pi_i(s) = s_i$. □

S sera considéré dans la suite comme sous-ensemble de $\prod_{i\in I} S_i$.

Lemme 1.2. *si $((S_i)_{i\in I}, (\pi_{ji})_{i\leqslant j})$ est un système inverse d'espaces topologiques tel que pour chaque $i \leqslant j$, $\pi_{ji} : S_j \to S_i$ soit une application continue, et si $S = \varprojlim S_i$, alors on a les quelques propriétés suivantes concernant la topologie produit induite sur S :*

1. *si les ensembles S_i sont des espaces séparés, alors S est un sous-ensemble fermé de $\prod_{i\in I} S_i$ et les applications π_i sont continues ;*
2. *si les S_i sont des espaces séparés compacts non vides, alors S est un espace compact non vide ;*
3. *Une base d'ouverts de la topologie de S est donnée par les $\pi_i^{-1}(U_i)$ où les U_i sont les ouverts de S_i ;*
4. *si les S_i sont des espaces totalement discontinus, alors S est un espace totalement discontinu.*

Démonstration.
1. Soit $z = (z_i)_{i\in I} \in \prod_{i\in I} S_i$, $z \notin S$. Alors il existe $(j,k) \in I^2$ tels que $j < k$ et $\pi_{kj}(z_k) \neq z_j$. Soient alors U et V des voisinages disjoints de z_j et $\pi_{kj}(z_k)$. Il s'en suit que $U \times V \times \prod_{i\neq j,k} S_i$ est un voisinage de z qui n'intersecte pas S. Donc le complémentaire de S est ouvert et S est fermé. Pour tout ouvert U_i de S_i, on a $\pi_i^{-1}(U_i) = S \cap (U_i \times \prod_{j\neq i} S_j)$ est un ouvert de S. Donc π_i est continue.
2. Par le théorème de Tychonoff, $\prod_{i\in I} S_i$ est compact. D'autre part, c'est un espace séparé. Ainsi S est fermé dans $\prod_{i\in I} S_i$, donc compact.

Par ailleurs, $S = \bigcap_{k \geqslant j} R_{k,j}$ où $R_{k,j} = \{s \in \prod_{i \in I} S_i \mid \pi_{kj}(s_k) = s_j\}$. Or $T = \{(s_k, s_j) \in S_k \times S_j \mid \pi_{kj}(s_k) = s_j\}$ est fermé, donc $R_{k,j} = (\pi_k \times \pi_j)^{-1}(T)$ est fermé dans S donc compact. Montrons maintenant que toute intersection finie $\bigcap_{i=1}^{n} R_{k(i),j(i)}$ est non vide ce qui suffit à montrer que S est non vide. Considérons pour cela $j(1) \leqslant k(1), \ldots, j(n) \leqslant k(n)$, n paires de I ; soit $m \in I$ tel que $m \geqslant k(i)$ pour $i = 1, \ldots, n$ et soit $s_m \in S_m$. On définit alors $s_{j(i)} = \pi_{m,j(i)}(s_m)$ et $s_{k(i)} = \pi_{m,k(i)}(s_m)$ pour $i = 1, \ldots, n$ et $s_r \in S_r$ quelconque si r n'est pas de la forme $j(i)$ ou $k(i)$. L'élément $s = (s_i)_{i \in I}$ appartient bien à $\bigcap_{i=1}^{n} R_{k(i),j(i)}$.

3. Remarquons tout d'abord que $\bigcap_{i=1}^{n} \pi_{j(i)}^{-1}(U_{j(i)})$ forme une base pour la topologie produit de S. Il faut maintenant voir que chacun de ces éléments contient un $\pi_k^{-1}(U_k)$. Il suffit pour cela de montrer que $\pi_i^{-1}(U_i) \cap \pi_j^{-1}(U_j) = \pi_k^{-1}(U_k)$. Cela se fait en prenant $k \geqslant i, j$ et $U_k = \pi_{kj}^{-1}(U_j) \cap \pi_{ki}^{-1}(U_i)$.
4. À partir du résultat précédent on trouve une base de voisinages ouverts et fermés autour de chaque élément $a \in S$ dont l'intersection vaut $\{a\}$.

$\square$

Corollaire 1.3. *Une limite projective de groupes finis (où les groupes sont munis de la topologie discrète et où les π_{ji} sont des morphismes de groupes) est un groupe topologique séparé compact totalement discontinu.*

On appelle un tel groupe un *groupe profini.*

Proposition 1.4. *Soit $(S_i)_{i \in I}$ un système inverse d'espaces topologiques séparés compacts (ce sera notamment le cas si les S_i sont des groupes finis). Soit $J \subseteq I$ un sous-ensemble vérifiant $\forall i \in I, \exists j \in J$, tel que $j \geqslant i$. Alors J est filtrant à droite et $S := \varprojlim_{i \in I} S_i$ est isomorphe en tant qu'espace topologique à $S' := \varprojlim_{j \in J} S_j$.*

Démonstration.

$$\text{Soit } \varphi : \begin{array}{rcl} S & \longrightarrow & S', \\ s = (s_i)_{i \in I} & \longmapsto & (s_j)_{j \in J}. \end{array}$$

Montrons que φ est bijective. Soit $(s, t) \in S^2$, $s = (s_i)_{i \in I}$, $t = (t_i)_{i \in I}$ tels que $\varphi(s) = \varphi(t)$, ce qui équivaut à $\forall j \in J$, $s_j = t_j$. Alors $\forall i \in I$, $\exists j \in J$, $j \geqslant i$ et $s_i = \pi_{ji}(s_j) = \pi_{ji}(t_j) = t_i$. On en conclut que $t = s$ et que φ est injective.

$$\text{Soit } \psi : \begin{array}{rcl} S' & \longrightarrow & S, \\ (s_j)_{j \in J} & \longmapsto & (s_i)_{i \in I} \text{ avec } s_i = \begin{cases} s_i \text{ si } i \in J, \\ \pi_{ji}(s_j) \text{ pour } j \in J,\ j \geqslant i \text{ sinon.} \end{cases} \end{array}$$

L'application ψ est bien définie. En effet, si $k \geqslant i$ et $j \geqslant i$, où $(k, j) \in J^2$, alors $\exists\, m \in J$ avec $m \geqslant j$ et $m \geqslant k$. On a alors $\pi_{ji}(s_j) = \pi_{ji} \circ \pi_{mj}(s_m) = \pi_{mi}(s_\ell) = \pi_{ki} \circ \pi_{mk}(s_m) = \pi_{ki}(s_k)$.

Reste à montrer que ψ est à valeur dans S. Ceci s'obtient en considérant $(i, i') \in I^2$, $i \leqslant i'$, alors $\exists j \in J$, $j \geqslant i'$ et $\pi_{i'i}(s_{i'}) = \pi_{i'i} \circ \pi_{ji'}(s_j) = \pi_{ji}(s_j) = s_i$. Donc ψ est bien définie et $\varphi \circ \psi = \mathrm{Id}_{S'}$, ce qui montre la surjectivité (donc la bijectivité) de φ. Par conséquent, on obtient aussi la bijectivité de ψ.

Le dernier point à vérifier concerne la continuité de φ et de $\psi = \varphi^{-1}$. Pour cela, considérons la base d'ouverts $\pi_j^{-1}(O_j)$ de S' avec $j \in J$ et O_j ouvert de S_j. Alors $\varphi^{-1}(\pi_j^{-1}(O_j)) = \{s \in S \mid s_j \in O_j\} = \pi_j^{-1}(O_j)$, donc φ est continue. Il s'en suit que φ est une application continue d'un compact vers un espace compact séparé, c'est donc une application ouverte. D'où la continuité de ψ. □

1.2 Application aux groupes de Galois

Soit K/k une extension galoisienne (*i.e.*, normale et séparable) de corps que l'on supposera de degré infini. Soit $\mathcal{F}$ l'ensemble des sous-corps F de K ($k \subseteq F \subseteq K$), extensions galoisiennes finies de k. Alors $\mathcal{F}$ est ordonné par inclusion et est filtrant à droite.

En effet, si F_1/k et F_2/k sont des extensions galoisiennes de degré fini, alors

$$[F_1F_2 : k] \leqslant [F_1 : k][F_2 : k] < \infty.$$

Donc F_1F_2 est une extension galoisienne de degré fini et appartient ainsi à $\mathcal{F}$.

De plus, $K = \bigcup_{F \in \mathcal{F}} F$.

Théorème 1.5. *Soit* $\mathrm{Gal}(K/k)$ *le groupe de Galois de* K *sur* k *(*i.e.*, le groupe des* k*-automorphismes de* K*), alors on a :*

$$\mathrm{Gal}(K/k) \cong \varprojlim_{F \in \mathcal{F}} \mathrm{Gal}(F/k)$$

où les morphismes de liaison sont les morphismes de restriction
$\rho_{FF'} : \mathrm{Gal}(F/k) \to \mathrm{Gal}(F'/k)$ *pour* $F' \subseteq F$.

Lemme 1.6. *La structure de groupe topologique ainsi induite sur* $\mathrm{Gal}(K/k)$ *vérifie les propriétés suivantes :*

1. $\mathrm{Gal}(K/k)$ *est un goupe topologique séparé compact totalement discontinu ;*
2. *les sous-groupes ouverts de* $\mathrm{Gal}(K/k)$ *sont exactement les sous-groupes fermés d'indice fini ; ce sont les* $\mathrm{Gal}(K/F)$ *avec* $F \subseteq K$ *extension finie de* k *;*
3. *une base de voisinages de l'élément unité de* $\mathrm{Gal}(K/k)$ *est donnée par les sous-groupes* $\mathrm{Gal}(K/F)$ *avec* $F \in \mathcal{F}$ *;*
4. *une base de voisinages de l'élément* σ *de* $\mathrm{Gal}(K/k)$ *est donnée par les* $\sigma\,\mathrm{Gal}(K/F)$ *avec* $F \in \mathcal{F}$ *;*
5. *tout sous-groupe* $\mathrm{Gal}(K/L)$ *de* $\mathrm{Gal}(K/k)$*, où* L *est une extension quelconque de* k*, est fermé.*

Démonstration. 1. Cela résulte du corollaire 1.3.

2. Pour H sous-groupe de $\mathrm{Gal}(K/k)$, on écrit $\mathrm{Gal}(K/k)$ comme union disjointe des classes de $\mathrm{Gal}(K/k)$ modulo H.
3. Ces éléments sont ouverts d'après 2. et $\bigcup_{F\in\mathcal{F}} F = K$. Donc $\bigcap_{F\in\mathcal{F}} \mathrm{Gal}(K/F)$ contient seulement l'élément unité.
4. Cela découle de 3. et de la structure de groupe topologique de $\mathrm{Gal}(K/k)$.
5. L peut s'écrire comme l'union des extensions finies $k(x)/k$, où $x \in L$. Donc $\mathrm{Gal}(K/L) = \bigcap_{x\in L} \mathrm{Gal}(K/k(x))$ est une intersection de fermés et $\mathrm{Gal}(K/L)$ est bien un sous-groupe fermé de $\mathrm{Gal}(K/k)$.

□

Une réciproque du résultat 5. est donnée par le théorème suivant :

Théorème 1.7 (Krull). *On a une bijection entre* $\mathcal{H} := \{H$ *sous-groupes fermés de* $\mathrm{Gal}(K|k)\}$ *et* $\mathcal{M}_{K/k} := \{M$ *sous-corps de* $K \mid k \subseteq M \subseteq K\}$. *Cette bijection est donnée par les opérateurs*

$$\begin{array}{rrcl} \mathrm{inv}: & \mathcal{H} & \to & \mathcal{M}_{K/k}, \\ & H & \to & \{x \in K \mid \forall \sigma \in H, \sigma x = x\} := K^H, \end{array}$$

et

$$\begin{array}{rrcl} \mathrm{gr}: & \mathcal{M}_{K/k} & \to & \mathcal{H}, \\ & M & \to & \mathrm{Gal}(K/M). \end{array}$$

Démonstration. On montre successivement que pour tout $M \in \mathcal{M}_{K/k}$, $\mathrm{inv}(\mathrm{gr}(M)) = M$ et pour tout $H \in \mathcal{H}$, $\mathrm{gr}(\mathrm{inv}\, H) = H$.

- Soit $M' = \mathrm{inv}(\mathrm{gr}(M))$. On a trivialement $M \subseteq M'$. Réciproquement, soit σ un M-isomorphisme de M'. Alors $\sigma(M') \subseteq \sigma(K) \subseteq K$ et σ s'étend en un M-automorphisme de K : $\tilde{\sigma} \in \mathrm{Gal}(K/M)$. Donc $M' \subseteq \mathrm{inv}(\tilde{\sigma})$ et $\sigma_{|M'}$ vaut l'identité. Donc $[M' : M] = 1$ et $M = M'$.
- Soit $M = \mathrm{inv}\, H$ et $H' = \mathrm{gr}(M)$. On a trivialement $H \subseteq H'$. Réciproquement, comme H est fermé, il suffit de montrer que H est dense dans H'. Montrons que H intersecte tout voisinage $\sigma\,\mathrm{Gal}(K/F)$ de $\sigma \in H'$ (avec F/k extension galoisienne finie). L'extension FM/M est galoisienne finie et $\sigma_{|FM} \in \mathrm{Gal}(FM/M) = \rho_{K,FM}(H)$ par le théorème d'Artin pour les extensions finies. Donc $\sigma_{|FM}$ est la restriction de $\tau \in H$ et $\tau \in \sigma\,\mathrm{Gal}(K/FM) \subseteq \sigma\,\mathrm{Gal}(K/F)$.

□

Proposition 1.8. *Si L/k est une sous-extension de K/k alors on a l'équivalence suivante :*

$$L/K_0 \textit{ est galoisienne} \iff \mathrm{Gal}(K/L) \textit{ est un sous-groupe normal de } \mathrm{Gal}(K/K_0).$$

Dans ce cas, on a l'isomorphisme de groupes topologiques suivant :

$$\mathrm{Gal}(L/K_0) \cong \mathrm{Gal}(K/K_0)/\,\mathrm{Gal}(K/L).$$

Démonstration. La séparabilité de L est induite par celle de K. Donc L/k est galoisienne si et seulement si L/k est normale. On a $\mathrm{Gal}(K/L)$ est normal si et seulement si pour tout $\sigma \in \mathrm{Gal}(K/k)$, $\sigma \mathrm{Gal}(K/L)\sigma^{-1} = \mathrm{Gal}(K/L)$. Ce qui équivaut à dire que pour tout $\sigma \in \mathrm{Gal}(K/k)$ et pour tout $\tau \in \mathrm{Gal}(K/L)$, $\sigma\tau\sigma^{-1}_{|L} = \mathrm{Id}_{|L}$, soit pour tout $a \in L$, $\sigma^{-1}(a)$ est invariant par τ. Ceci revient à dire que pour tout $\sigma \in \mathrm{Gal}(K/k)$ et pour tout $a \in L$, $\sigma^{-1}(a)$ est invariant par $\mathrm{Gal}(K/L)$, et appartient donc à L par le théorème de Krull, soit pour tout $\sigma \in \mathrm{Gal}(K/k)$, $\sigma(L) \subseteq L$, c'est à dire finalement que L/k est une extension galoisienne.

Dans ce cas regardons le morphisme de restriction $\rho_{KL} : \mathrm{Gal}(K/k) \longrightarrow \mathrm{Gal}(L/k)$. On a $\ker(\rho_{KL}) = \mathrm{Gal}(L/k)$ et donc : $\mathrm{Gal}(L/k) \cong \mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)$ (On pose sur $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)$ la topologie quotient, c'est-à-dire la topologie la moins fine rendant continue l'application canonique : $\mathrm{Gal}(K/k) \longrightarrow \mathrm{Gal}(K/k)/\mathrm{Gal}(K/L)$). □

2 Exemples d'extensions infinies ayant pour groupe de Galois $\mathbb{Z}_p$

2.1 Description de $\mathbb{Z}_p$

Soit p un nombre premier, on définit $\mathbb{Z}_p$ comme le complété de $\mathbb{Z}$ pour la distance p-adique d_p (Rappel : $d_p(n) := p^{-v_p(n)}$ où $v_p(n)$ désigne la valuation p-adique de n).

Lemme 2.1. *$\mathbb{Z}_p$ est un groupe profini et on a :*

$$\mathbb{Z}_p \cong \varprojlim_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$$

où les morphismes de liaison sont les restrictions modulaires.

Démonstration. Tout élément $s \in \mathbb{Z}_p$ s'écrit comme suite d'éléments de $\mathbb{Z}$ (par construction du complété) : $s = (s_i)_{i\in\mathbb{N}}$. De plus $(s_i)_{i\in\mathbb{N}}$ vérifie $d_p(s_i - s_j) \underset{i,j\to+\infty}{\longrightarrow} 0$, soit pour tout $i \in \mathbb{N}$, il existe $j_i \in \mathbb{N}$, tel que pour tout $k \geqslant j_i$: $d_p(s_k - s_{j_i}) \leqslant p^{-i}$, *i.e.*, $p^i \mid (s_k - s_{j_i})$. Donc pour tout $k \geqslant j_i$, $s_k \equiv s_{j_i} \bmod p^i$. On peut donc écrire s sous la forme unique $s = (s_{j_i})_{i\in\mathbb{N}}$. Ceci nous donne une injection $\mathbb{Z}_p \hookrightarrow \varprojlim_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$. Réciproquement, tout élément de $\varprojlim Z/p^i\mathbb{Z}$ s'écrit comme suite $(s_i)_{i\in\mathbb{N}}$, où pour tout $j \geqslant i$, $s_j \equiv s_i \bmod p^i$. Donc pour tout $j \geqslant i$, $d_p(s_j - s_i) = p^{-i}$. Ainsi $(s_i)_{i\in\mathbb{N}}$ converge dans $\mathbb{Z}_p$. D'où l'isomorphisme $\mathbb{Z}_p \cong \varprojlim_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z}$ □

2.2 Un exemple d'extension galoisienne de groupe de Galois $\mathbb{Z}_p$

Soit k un corps fini, alors, pour p premier, il existe des extensions croissantes k_n/k telles que $[k_n : k] = p^n$. Soit $k_\infty = \bigcup_{n\geqslant 0} k_n$, alors on a le théorème suivant concernant le groupe de Galois de k_∞/k :

Théorème 2.2. $\mathrm{Gal}(k_\infty/k) \cong \mathbb{Z}_p$.

Démonstration. Pour $n \in \mathbb{N}$, on a l'isomorphisme $\mathrm{Gal}(k_n/k) \cong \mathbb{Z}/p^n\mathbb{Z}$, et pour $j \geqslant i$, on a le diagramme commutatif suivant :

$$\begin{tikzcd}
\mathbb{Z}/p^j\mathbb{Z} \arrow[r] \arrow[d, "\cong"'] & \mathbb{Z}/p^i\mathbb{Z} \arrow[d, "\cong"'] \\
\mathrm{Gal}(k_j/k) \arrow[r] & \mathrm{Gal}(k_i/k)
\end{tikzcd}$$

Par passage à la limite inverse, on trouve : $\mathrm{Gal}(k_\infty/k) \cong \varprojlim_{i\in\mathbb{N}} \mathrm{Gal}(k_i/k) \cong \varprojlim_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z} \cong \mathbb{Z}_p$. $\square$

Par exemple : $\mathrm{Gal}(\bigcup_{i\geqslant 0} \mathbb{F}_{p^{p^i}}/\mathbb{F}_p) \cong \mathbb{Z}_p$.

On voit apparaître ici l'importance de l'hypothèse sur la fermeture des sous-groupes de $\mathrm{Gal}(K/K_0)$ dans le théorème de Krull. En effet, $\mathbb{Z}$ n'est pas fermé dans $\mathbb{Z}_p$ donc $\mathbb{Z}$ n'est associé à aucun sous-corps de $\bigcup_{i\in\mathbb{N}} \mathbb{F}_{p^{p^i}}$.

2.3 Extensions galoisiennes de $\mathbb{Q}$ de groupe de Galois $\mathbb{Z}_p$

On essaie maintenant de construire une extension $\mathbb{Q}_\infty/\mathbb{Q}$ de groupe de Galois $\mathbb{Z}_p$. On essaye pour cela d'adjoindre à $\mathbb{Q}$ des racines de l'unité. Soit ζ_n une racine primitive n-ième de l'unité de $\mathbb{Q}$ dans $\mathbb{C}$, et considérons $\mathbb{Q}(\zeta_n)$ le corps engendré par ζ_n au-dessus de $\mathbb{Q}$.

On a le résultat suivant :

Proposition 2.3. *$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est une extension galoisienne et* $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Démonstration. On sait que $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^*|$.

L'extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est séparable car $\mathbb{Q}$ est de caractéristique 0. C'est une extension normale car c'est le corps de décomposition de ϕ_n (n-ième polynyôme cyclotomique). En effet, les racines de ϕ_n dans $\overline{\mathbb{Q}}$ sont les ζ^i avec $i \wedge n = 1$ donc elles appartiennent à $\mathbb{Q}(\zeta_n)$. Ainsi, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ est une extension galoisienne.

Soit $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$; alors $\phi_n(\sigma(\zeta_n)) = \sigma(\phi_n(\zeta_n)) = 0$. On en déduit que $\exists!\ i \in (\mathbb{Z}/n\mathbb{Z})^*$, $\sigma(\zeta_n) = \zeta_n^i$. Ceci nous donne un morphisme : $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$. Ce morphisme est injectif car $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ est uniquement défini par $\sigma(\zeta_n)$. C'est donc un isomorphisme par égalité des cardinaux. $\square$

Considérons maintenant $\{p^i \mid i \in \mathbb{N}\}$, sous-ensemble de $\mathbb{N}$ filtrant à droite pour la relation d'ordre ($j \leqslant k \Leftrightarrow j \mid k$) et regardons $\mathbb{Q}(\zeta_{p^\infty}) = \mathbb{Q}(\{\zeta_{p^i} \mid i \in \mathbb{N}\})$. Une sous-extension galoisienne finie de $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$ est engendrée sur $\mathbb{Q}$ par un nombre fini d'éléments. Elle est donc incluse dans un $\mathbb{Q}(\zeta_{p^i})$ (avec $i \in \mathbb{N}$). Il s'en suit par le théorème 1.5 et la propriété 1.4 que $\mathrm{Gal}(\mathbb{Q}_(\zeta_{p^\infty})/\mathbb{Q}) \cong \varprojlim_{i\in\mathbb{N}} \mathrm{Gal}(\mathbb{Q}(\zeta_{p^i})/\mathbb{Q})$. Pour p impair, la structure de $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ est donnée par le lemme suivant :

Lemme 2.4. $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^i})/\mathbb{Q}) \cong (\mathbb{Z}/p^i\mathbb{Z})^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{i-1}\mathbb{Z}$ *avec, pour* $j \geqslant i$, *le diagramme commutatif suivant :*

$$\begin{tikzcd} \mathrm{Gal}(\mathbb{Q}(\zeta_{p^j})/\mathbb{Q}) \arrow[r, "\simeq"] \arrow[d, "\rho_{ji}"'] & (\mathbb{Z}/p^j\mathbb{Z})^* \arrow[r, "\simeq", "\varphi_j"'] \arrow[d, "(\mathrm{mod}\ p^i)"'] & \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{j-1}\mathbb{Z} \arrow[d, "\pi_{ji}"] \\ \mathrm{Gal}(\mathbb{Q}(\zeta_{p^i})/\mathbb{Q}) \arrow[r, "\simeq"] & (\mathbb{Z}/p^i\mathbb{Z})^* \arrow[r, "\simeq", "\varphi_i"'] & \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{i-1}\mathbb{Z} \end{tikzcd}$$

où $\pi_{ji}(a,b) = (a, b \bmod p^{i-1})$. *On en déduit que*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \varprojlim_{i\in\mathbb{N}} \mathbb{Z}/p^i\mathbb{Z} \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p.$$

Démonstration. La proposition 2.3 donne la partie gauche du diagramme commutatif. Reste à démontrer la partie droite.

Tout d'abord, explicitons l'isomorphisme φ_j. Il est possible de vérifier que l'élément $(1+p) \in \mathbb{Z}/p^j\mathbb{Z}$ est d'ordre p^{j-1} (ceci n'est pas vrai pour $p=2$). De même, en considérant b une racine primitive modulo p (on choisit le même b pour tout $j \in \mathbb{N}$), on peut vérifier que $c_j = b^{p^{j-1}}$ est d'ordre $p-1$. Soit maintenant $a \in <c_j> \cap <1+p>$. L'ordre de a est une puissance de p et divise $p-1$, donc $a=1$. Il s'en suit que $<c_j, 1+p> \cong <c_j> \times <1+p>$ est d'ordre $p^{j-1}(p-1) = |(\mathbb{Z}/p^j\mathbb{Z})^*|$. On en déduit l'isomorphisme canonique

$$\varphi_j : (\mathbb{Z}/p^j\mathbb{Z})^* \longrightarrow <c_j> \times <1+p> \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{j-1}\mathbb{Z}.$$

Ainsi, tout élément de $(\mathbb{Z}/p^j\mathbb{Z})^*$ s'écrit, de façon unique, sous la forme $c_j^\alpha(1+p)^\beta$, avec $\alpha \in \mathbb{Z}/(p-1)\mathbb{Z}$ et $\beta \in \mathbb{Z}/p^{j-1}\mathbb{Z}$.

Le dernier point à vérifier concerne la commutativité du diagramme. C'est-à-dire, montrer que $c_j^\alpha(1+p)^\beta = c_i^\alpha(1+p)^{\beta \bmod p^{i-1}} \bmod p^i$. On obtient finalement cette dernière égalité en remarquant d'une part que $(1+p)$ est d'ordre p^{i-1} dans $(\mathbb{Z}/p^i\mathbb{Z})^*$ et d'autre part que $b^{p^{i-1}(p-1)} \equiv 1 \bmod p^i$, c'est-à-dire $b^{p^i} \equiv b^{p^{i-1}} \bmod p^i$ et par récurrence sur $j \geqslant i$: $c_j \equiv c_i \bmod p^i$. □

On identifie maintenant $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ avec $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$. En remarquant que $\mathbb{Z}/(p-1)\mathbb{Z} \times \{0\}$ est un sous-groupe normal fermé de $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$, le théorème de Krull affirme l'existence d'une sous-extension galoisienne $\mathbb{Q}_\infty/\mathbb{Q}$ de $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$ telle que $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}_\infty) = \mathbb{Z}/(p-1)\mathbb{Z} \times \{0\}$. Finalement on obtient :

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) &\cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) \,/\, \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}_\infty) \\ &\cong (\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p) \,/\, (\mathbb{Z}/(p-1)\mathbb{Z} \times \{0\}) \\ &\cong \mathbb{Z}_p. \end{aligned}$$

Remarque 2.5. *Le corps* $\mathbb{Q}_\infty$ *est réel.*

En effet, soit j la conjugaison complexe. On pose $j_\infty \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ la restriction de j à $\mathbb{Q}(\zeta_{p^\infty})$. Comme $\mathbb{Q}(\zeta_{p^\infty})$ n'est pas totalement réel, $j_\infty \neq \mathrm{Id}_{\mathbb{Q}(\zeta_{p^\infty})}$. On en déduit que j_∞ est d'ordre 2. Si on écrit maintenant $j_\infty = (n_1, n_2) \in \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$, alors (n_1, n_2) est d'ordre 2 dans $\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$. Comme $\mathbb{Z}_p$ n'a pas d'éléments de torsion, on en déduit que $n_2 = 0$ et donc $j_\infty \in \mathbb{Z}/(p-1)\mathbb{Z} \times \{0\}$ et $\mathbb{Q}_\infty \subseteq \mathrm{inv}(j)$. Donc $\mathbb{Q}_\infty$ est réel.

L'ensemble des résultats précédents peut être résumé par le diagramme suivant :

Diagramme 2.6.

$$\begin{tikzcd}
\mathbb{R} & & \mathbb{Q}(\zeta_{p^\infty}) \arrow[ddd, dash] \arrow[dddd, dash, bend left, "\mathbb{Z}_p"] \\
\cup & & \\
\mathbb{Q}_\infty \arrow[uurr, dash, "\parallel" marking] \arrow[ddd, dash] \arrow[ddd, dash, bend right, "\mathbb{Z}_p"'] & & \\
& & \mathbb{Q}(\zeta_{p^i}) \arrow[d, dash] \arrow[d, dash, bend right, "\mathbb{Z}/p^{i-1}\mathbb{Z}"'] \\
& & \mathbb{Q}(\zeta_p) \\
\mathbb{Q} \arrow[urr, dash, "\parallel" marking] \arrow[urr, dash, bend right, "\mathbb{Z}/(p-1)\mathbb{Z}"'] & &
\end{tikzcd}$$

Intéressons-nous maintenant au cas $p = 2$. Le diagramme du lemme 2.4 devient :

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}(\zeta_{2^j})/\mathbb{Q}) \arrow[r, "\simeq"] \arrow[d, "\rho_{ji}"'] & (\mathbb{Z}/2^j\mathbb{Z})^* \arrow[r, "\simeq", "\varphi_j"'] \arrow[d, "(\mathrm{mod}\ 2^i)"'] & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{j-2}\mathbb{Z} \arrow[d, "\pi_{ji}"] \\
\mathrm{Gal}(\mathbb{Q}(\zeta_{2^i})/\mathbb{Q}) \arrow[r, "\simeq"] & (\mathbb{Z}/2^i\mathbb{Z})^* \arrow[r, "\simeq", "\varphi_i"'] & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{i-2}\mathbb{Z}
\end{tikzcd}$$

où $\pi_{ji}(a, b) = (a, b \bmod 2^{i-2})$.

Démonstration. On peut démontrer que 5 est un élément d'ordre 2^{j-2} dans $(\mathbb{Z}/2^j\mathbb{Z})^*$. Donc $<5> = \{a \in \mathbb{Z}/2^j\mathbb{Z} \mid a \equiv 1 \bmod 4\}$ est un sous-groupe cyclique d'ordre 2^{j-2}. En remarquant que

$$\varphi_j : \begin{array}{ccc} (\mathbb{Z}/2^j\mathbb{Z})^* & \longrightarrow & \{-1,1\} \times <5> \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{j-2}\mathbb{Z} \\ a & \longmapsto & (a \bmod 4, (a \bmod 4)a) \end{array}$$

définit un morphisme de groupes injectif (si $\varphi_j(a) = (a_1, a_2)$, alors $a = a_1 a_2$) donc surjectif, on voit que tout élément de $(\mathbb{Z}/2^j\mathbb{Z})^*$ s'écrit de manière unique sous la forme $\varepsilon 5^\alpha$ avec $\varepsilon \in \{-1, 1\}$ et $\alpha \in \mathbb{Z}/2^{j-2}\mathbb{Z}$. Reste à démontrer la commutativité du diagramme, c'est-à-dire montrer que $(a \bmod 4, 5^\alpha) = ((a \bmod 4), 5^{\alpha \bmod 2^{i-2}} \bmod 2^i)$. Ceci est immediat car 5 est d'ordre 2^{i-2} dans $(\mathbb{Z}/2^i\mathbb{Z})^*$. $\square$

On obtient donc $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^\infty})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$. La conjugaison complexe j est un élément de $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^\infty})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ d'ordre 2. C'est donc $(1, 0)$. On définit $\mathbb{Q}_\infty = \mathrm{inv}(j) = \mathrm{inv}(\mathbb{Z}/2\mathbb{Z} \times \{0\})$, ce qui nous donne : $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \mathbb{Z}_2$ et $\mathbb{Q}_\infty$ est réel.

Le diagramme 2.6 devient :

Diagramme 2.7.

$$
\begin{tikzcd}[arrows=dash]
\mathbb{R} & & \mathbb{Q}(\zeta_{2^\infty}) \arrow[ddd] \arrow[dddd, bend left, "\mathbb{Z}_2"] \\
\cup & & \\
\mathbb{Q}_\infty \arrow[uurr, "\shortparallel" marking] \arrow[ddd] \arrow[ddd, bend right, "\mathbb{Z}_2"'] & & \\
 & & \mathbb{Q}(\zeta_{2^i}) \arrow[d] \arrow[d, bend right, "\mathbb{Z}/2^{i-2}\mathbb{Z}"'] \\
 & & \mathbb{Q}(\zeta_4) \\
\mathbb{Q} \arrow[urr, "\shortparallel" marking] \arrow[urr, bend right, "\mathbb{Z}/2\mathbb{Z}"'] & &
\end{tikzcd}
$$

Regardons maintenant de plus près les sous-extensions $\mathbb{Q}_n/\mathbb{Q}$ de $\mathbb{Q}_\infty/\mathbb{Q}$ où $\mathbb{Q}_n = \mathbb{Q}_\infty \cap \mathbb{Q}(\zeta_{2^{n+2}})$. On a donc $\mathbb{Q}_n = \mathrm{inv}(j) \cap \mathbb{Q}(\zeta_{2^{n+2}})$. On peut alors voir $\mathbb{Q}_n$ comme le sous-corps de $\mathbb{Q}(\zeta_{2^{n+2}})$ fixe par $\mathbb{Z}/2\mathbb{Z} \times \{0\}$. Donc $\mathbb{Q}_n/\mathbb{Q}$ est une extension totalement réelle de degré 2^n et $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) = \mathbb{Z}/2^n\mathbb{Z}$. De plus, on vérifie bien que $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \varprojlim \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) = \mathbb{Z}_2$. Le lemme suivant permet de décrire explicitement $\mathbb{Q}_n$.

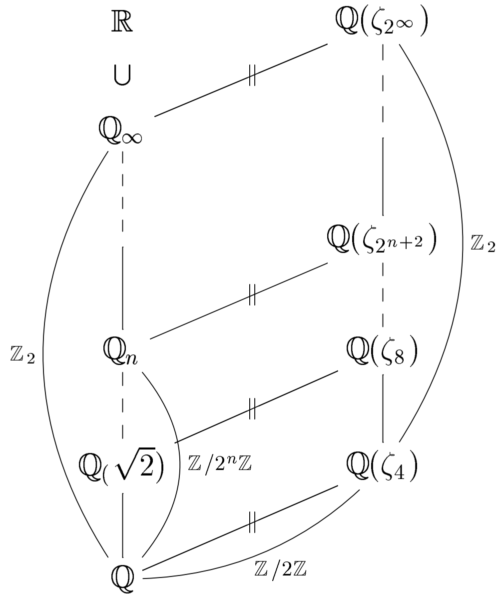
Lemme 2.8. $\mathbb{Q}_n = \mathbb{Q}(\theta_n)$ *où* θ_n *est défini par récurrence sur* n *:* $\theta_0 = 0$, $\theta_n = \sqrt{\theta_{n-1} + 2}$. *En particulier,* $\mathbb{Q}_1 = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}_2 = \mathbb{Q}(\sqrt{2+\sqrt{2}})$, $\mathbb{Q}_3 = \mathbb{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$, *etc.*

Démonstration. Soit P_n le polynôme défini par récurrence par $P_0(X) = X$ et $P_{n+1}(X) = P_n(X^2 - 2)$. Alors P_n est un polynôme annulateur de θ_n. On vérifie aisément par récurrence sur n que P_n s'écrit sous la forme : $P_n(X) = X^{2^n} + (2\sum_{i=1}^{2^n-1} a_{n,i}X^i) - 2$ où les $a_{n,i}$ sont des entiers relatifs. On en déduit, par le critère d'Eisenstein, que P_n est irréductible. C'est donc le polynôme minimal de θ_n et $\mathbb{Q}(\theta_n)/\mathbb{Q}$ est une extension de degré 2^n.

Soit maintenant ξ_n une racine de l'équation $x^2 - \theta_n x + 1 = 0$ dans $\mathbb{C}$. Alors $\theta_n\xi_n = \xi_n^2 + 1$, donc $\theta_n^2\xi_n^2 = \xi_n^4 + 2\xi_n^2 + 1$, soit $\xi_n^4 - \theta_{n-1}\xi_n^2 + 1 = 0$. On en déduit par récurrence sur n que ξ_n est une racine primitive de l'unité d'ordre 2^{n+2}. Donc $\theta_n = \dfrac{\xi_n^2+1}{\xi_n}$ appartient à $\mathbb{R} \cap \mathbb{Q}(\zeta_{2^{n+2}}) = \mathbb{Q}_n$. Finalement, $\mathbb{Q}_n = \mathbb{Q}(\theta_n)$. $\square$

En résumé, on a le diagramme :

Diagramme 2.9.



Références

[1] P. Ribenboim, *L'arithmétique des corps*, Hermann, Paris (1972).

[2] M. D. Fried, M. Jarden, *Field Arithmetic*, Springer-Verlag Berlin Heidelberg (1986).

[3] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag Berlin Heidelberg (1999).