Journal of Algebra 441 (2015) 1–20

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Minimalité et abyssalité des extensions abéliennes et projectives de $\mathbb{Q}$

Bruno Deschamps *

Laboratoire de Mathématiques Nicolas Oresme, CNRS UMR 6139, France

INFO ARTICLE

Historique de l'article :
Reçu le 28 septembre 2014
Disponible sur Internet le xxxx
Communiqué par Eva Bayer-Fluckiger

Keywords:
Inverse Galois theory
Shafarevich conjecture
Galois cohomology
Projective groups

RÉSUMÉ

Dans cet article nous classifions complètement les sous-corps projectifs minimaux de $\mathbb{Q}^{ab}$. Nous nous intéressons ensuite à l'existence d'extensions abéliennes et projectives de $\mathbb{Q}$ qui ne contiennent aucun sous-corps projectif minimal. En marge de ce travail nous faisons le lien entre ces questions et les conjectures de Shafarevich, Fried–Völklein et Dèbes–Deschamps pour proposer une description simple du groupe de Galois absolu du corps des rationnels.

ABSTRACT

In this article we classify all the minimal projective subfields of $\mathbb{Q}^{ab}$. We then focus on the existence of a projective abelian extension of $\mathbb{Q}$ which contains no minimal projective subfield. Alongside this work we make the link between these issues and the conjectures of Shafarevich, Fried–Völklein and Dèbes–Deschamps, to propose a simple description of the absolute Galois group of the field of rational numbers.

* Auteur correspondant à : Département de Mathématiques, Université du Maine, Avenue Olivier Messiaen, 72085 Le Mans cedex 9, France.
Adresse e-mail : Bruno.Deschamps@univ-lemans.fr.

http://dx.doi.org/10.1016/j.jalgebra.2015.04.047
0021-8693/

1. Introduction

En 1964, Shafarevich a émis une importante conjecture, à ce jour toujours non démontrée, qui prévoit que le groupe de Galois absolu de la clôture abélienne $\mathbb{Q}^{\mathrm{ab}}$ de $\mathbb{Q}$ est isomorphe au groupe prolibre de rang dénombrable $\widehat{F}_\omega$ (ici $\omega = \aleph_0$ désigne le cardinal du dénombrable). Il existe une généralisation notable de la conjecture de Shafarevich, due à Fried et Völklein, et qui prévoit que le groupe de Galois absolu d'un corps hilbertien, projectif et dénombrable est prolibre. Cette conjecture a été elle-même étendue par Dèbes et Deschamps, en une conjecture très générale (voir [1] pour le détail). Si Shafarevich a focalisé son attention sur le corps $\mathbb{Q}^{\mathrm{ab}}$ en ce qui concerne la liberté de certaines extensions de $\mathbb{Q}$, nous allons voir dans ce texte qu'il est légitime pour cette question, de considérer de bien plus petites extensions abéliennes de $\mathbb{Q}$.

Le caractère projectif du corps $\mathbb{Q}^{\mathrm{ab}}$ est souvent présenté comme une conséquence de la théorie du corps de classe. Son caractère hilbertien découle d'un théorème de Kuyk qui assure que toute extension abélienne d'un corps hilbertien est encore un corps hilbertien. De ce point de vue, tout sous-corps strict de $\mathbb{Q}^{\mathrm{ab}}$ est donc hilbertien et, sous la conjecture de Fried–Völklein, dès qu'un tel corps est projectif, son groupe de Galois absolu se révèle être prolibre et devient donc un candidat plus petit que $\mathbb{Q}^{\mathrm{ab}}$ à la conjecture de Shafarevich.

Sous la conjecture de Shafarevich, on a la suite exacte

$$1 \longrightarrow \widehat{F}_\omega \longrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \widehat{\mathbb{Z}}^* \longrightarrow 1$$

dont il est mal aisé de tirer une description de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ à proprement parler. Par exemple, cette suite n'est pas scindée : si c'était le cas, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ contiendrait des éléments de torsion non involutifs, ce qui est impossible d'après la théorie d'Artin–Schreier. Si, dans cette suite exacte, on est en mesure de changer le facteur $\widehat{\mathbb{Z}}^*$ en quelque chose d'un peu plus proche d'un groupe projectif, on peut espérer en dire plus sur le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. A cet effet, l'étude des sous-corps projectifs minimaux de $\mathbb{Q}^{\mathrm{ab}}$ menée dans le §1.1. nous amène dans le §2.3 à montrer que, sous une forme un peu optimisée de la conjecture de Shafarevich (conjecture qui reste beaucoup moins générale que celles de Fried–Völklein et Dèbes–Deschamps), on peut montrer qu'il existe un isomorphisme de la forme

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \simeq \left(\widehat{F}_\omega \rtimes \widehat{\mathbb{Z}}\right) \rtimes \mathbb{Z}/2$$

La remarque 11 de ce texte apporte quelques précisions sur la nature des actions considérées dans ces produits.

L'objet principal de cet article est d'explorer la famille des sous-corps projectifs de $\mathbb{Q}^{\mathrm{ab}}$ et de tenter de les cataloguer. Dans le §2.1 nous décrivons explicitement les extensions abéliennes projectives minimales (pour ces deux propriétés) de $\mathbb{Q}$. Il s'agit en fait des plus petit sous-corps totalement imaginaires de $\mathbb{Q}^{\mathrm{ab}}$ qui contiennent la $\widehat{\mathbb{Z}}$-extension

de $\mathbb{Q}$ (théorème 6). Dans le §3 nous nous intéressons aux sous-corps projectifs de $\mathbb{Q}^{\mathrm{ab}}$ qui ne sont extensions d'aucun sous-corps projectif minimal (que nous appelons corps *abyssaux* dans ce texte). Nous montrons qu'il en existe et nous en explicitons certains (théorème 13), la proposition 14 montrant que l'on peut en trouver qui sont, d'une certaine manière, aussi proches que l'on veut de $\mathbb{Q}$.

2. Extensions abéliennes projectives minimales

Rappelons pour commencer qu'un corps K est dit projectif, si son groupe de Galois absolu $\Gamma = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ est un groupe (profini) projectif, c'est-à-dire si tout problème de plongement fini pour Γ possède une solution faible. Il existe une série de caractérisations de la projectivité d'un corps, que l'on pourra par exemple trouver dans [4]. La plus notable est sans doute celle qui assure que le corps K est projectif si et seulement la dimension cohomologique de Γ est ≤ 1. On en déduit que, si K est projectif, alors toutes ses extensions algébriques L/K le sont aussi. Dans cette situation, les groupes de Brauer des extensions algébriques L de K vérifient tous $\mathrm{Br}(L) = 0$. En caractéristique 0, cette dernière propriété caractérise réciproquement le fait pour K d'être projectif.

Pour ce qui est des extensions abéliennes projectives de $\mathbb{Q}$, il est relativement facile de construire des sous-corps projectifs stricts de $\mathbb{Q}^{\mathrm{ab}}$. A cet effet, rappelons le lemme classique de cohomologie galoisienne :

Lemme 1. *(Voir [4, Proposition I.3.3.14].) Si H est un sous-groupe ouvert d'un groupe profini G et que pour un nombre premier p donné on a $\mathrm{cd}_p(G) < +\infty$ alors $\mathrm{cd}_p(G) = \mathrm{cd}_p(H)$.*

Dans l'isomorphisme usuel

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \simeq \mathbb{Z}/2 \times \prod_{p \neq 2} \mathbb{Z}/(p-1) \times \widehat{\mathbb{Z}}$$

le premier facteur $\mathbb{Z}/2$ correspond à l'extension $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ qui est totalement imaginaire. Ainsi, si l'on considère le sous-corps M_q de $\mathbb{Q}^{\mathrm{ab}}$ laissé fixe par le facteur $\mathbb{Z}/(q-1)\mathbb{Z}$ pour un premier $q \neq 2$, ce corps est alors lui aussi totalement imaginaire et vérifie, par conséquent, que son groupe de Galois absolu est de dimension cohomologique ≤ 2. On peut donc appliquer le lemme 1 pour tout premier p et obtenir finalement la projectivité du corps M_q.

2.1. Classification

Pour tout premier p, on notera $\mathbb{Q}(\mu_{p^\infty})$ l'extension galoisienne engendrée par les racines p^n-ièmes de l'unité quand n varie. Il est classique que

$$\mathrm{Gal}(\mathbb{Q}(\mu_{2^\infty})/\mathbb{Q}) \simeq \mathbb{Z}/2 \times \mathbb{Z}_2 \text{ et } \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}/(p-1) \times \mathbb{Z}_p \text{ pour } p \neq 2$$

Dans cet isomorphisme, pour $p \neq 2$, le facteur $\mathbb{Z}/(p-1)$ correspond au groupe de Galois de l'extension $\mathbb{Q}(\xi_p)/\mathbb{Q}$ où ξ_p désigne une racine primitive p-ième de l'unité. Le facteur $\mathbb{Z}/2$ correspond lui à l'extension $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$. Quant au facteur $\mathbb{Z}_p$, il correspond au groupe de Galois de l'unique $\mathbb{Z}_p$-extension de $\mathbb{Q}$ que nous noterons $\mathscr{Z}_p$ dans la suite de ce texte. Il s'agit d'une extension totalement réelle de $\mathbb{Q}$ qui est totalement ramifiée en p. On notera aussi $\mathscr{Z}$ le compositum pour tous les premiers p des corps $\mathscr{Z}_p$, c'est l'unique $\widehat{\mathbb{Z}}$-extension de $\mathbb{Q}$. Le théorème de Kronecker–Weber assure que le corps $\mathbb{Q}^{\mathrm{ab}}$ est égal au compositum des corps $\mathbb{Q}(\mu_{p^\infty})$. Chacun de ces derniers étant linéairement disjoints du compositum des autres, on retrouve l'isomorphisme usuel

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \simeq \mathbb{Z}/2 \times \prod_{p\neq 2} \mathbb{Z}/(p-1) \times \widehat{\mathbb{Z}}$$

annoncé plus haut.

Pour l'étude des sous-corps projectifs de $\mathbb{Q}^{\mathrm{ab}}$ commençons par exploiter le lemme 1 :

Proposition 2. *Soit $\Omega/\mathbb{Q}$ une extension galoisienne. Si Ω est projectif, alors il est totalement imaginaire et si Ω' est un sous-corps totalement imaginaire d'indice fini sous Ω alors, Ω' est projectif.*

En conséquence de quoi, si Ω est un corps projectif, extension abélienne de $\mathbb{Q}$, et si $\mathrm{Gal}(\Omega/\mathbb{Q})$ contient un élément de torsion d'ordre impair ou au moins deux involutions, alors Ω n'est pas un corps projectif minimal.

Preuve. Puisque l'extension $\Omega/\mathbb{Q}$ est galoisienne, si Ω n'est pas totalement imaginaire alors il est totalement réel. Dans ces conditions, la conjugaison complexe est élément de $\mathrm{Gal}(\overline{\mathbb{Q}}/\Omega)$, groupe qui, possédant de la torsion, ne peut pas alors être projectif.

Pour montrer la suite de la proposition, nous appliquons le lemme 1 en posant $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\Omega')$ et $H = \mathrm{Gal}(\overline{\mathbb{Q}}/\Omega)$. Par hypothèse, $\mathrm{cd}_p(H) \leq 1$ pour tout premier p, mais comme Ω' est supposé totalement imaginaire sa dimension cohomologique est ≤ 2 et donc, en vertu de ce que l'on vient de rappeler, pour tout premier p on a $\mathrm{cd}_p(G) = \mathrm{cd}_p(H) \leq 1$. Ceci prouve que Ω' est projectif.

Supposons maintenant que Ω soit un corps projectif, extension abélienne de $\mathbb{Q}$ et considérons un élément $\sigma \in \mathrm{Gal}(\Omega/\mathbb{Q})$ d'ordre impair ou alors qui est une involution qui n'est pas égale à la restriction à Ω de la conjugaison complexe. Le corps $\Omega' = \Omega^{<\sigma>}$ est alors un sous-corps strict d'indice fini de Ω, extension galoisienne de $\mathbb{Q}$, qui vérifie que la restriction de la conjugaison complexe à Ω' n'est pas triviale. Le corps Ω' est donc totalement imaginaire et en appliquant ce qui précède, on voit que Ω' est projectif. □

En appliquant cette proposition, on voit que si $\mathscr{P}_0$ désigne un ensemble fini de nombres premiers impairs alors le sous-corps M de $\mathbb{Q}^{\mathrm{ab}}$ des éléments laissés fixes par le facteur $\prod_{p\in\mathscr{P}_0} \mathbb{Z}/(p-1)$ de $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ est projectif.

On est donc en mesure d'exhiber une suite strictement décroissante $(M_n)_{n\geq 1}$ de sous-corps de $\mathbb{Q}^{\mathrm{ab}}$ qui sont tous projectifs. Par exemple, on considère, pour $n \geq 1$, le sous-corps

de $\mathbb{Q}^{\mathrm{ab}}$ des éléments laissés fixes par le facteur $\prod_{p\leq p_n}\mathbb{Z}/(p-1)$ (p_n désignant ici le n-ième nombre premier). Il vérifie

$$\mathrm{Gal}(M_n/\mathbb{Q})\simeq\mathbb{Z}/2\times\prod_{p>p_n}\mathbb{Z}/(p-1)\times\widehat{\mathbb{Z}}$$

et l'on voit alors que, si l'on est mesure de passer à la limite, on pourrait se débarrasser du facteur infini $\prod_{p\neq 2}\mathbb{Z}/(p-1)$ de $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ et préserver le caractère projectif du corps ainsi obtenu.

On peut, en effet, faire une telle chose. Le corps ainsi obtenu est même un sous-corps projectif minimal de $\mathbb{Q}^{\mathrm{ab}}$. Pour démontrer cela on va utiliser une importante propriété de projectivité des extensions algébriques de $\mathbb{Q}$: considérons une extension algébrique $k/\mathbb{Q}$ filtrée par une famille $(k_i/\mathbb{Q})_i$ de sous-extensions finies. Pour une place v de k, on note $(k_i)_v$ le complété de k_i pour la place induite par v sur k_i et l'on définit le *degré local de k en v* comme étant le nombre surnaturel suivant :

$$n_v(k)=\mathrm{ppcm}[(k_i)_v:\mathbb{Q}_v]$$

On a alors :

Théorème 3. *(Voir [4, Proposition II.3.3.9].) Soit $k/\mathbb{Q}$ une extension algébrique et p un nombre premier. On suppose que $p\neq 2$ ou que k est totalement imaginaire. On a $\mathrm{cd}_p(k)\leq 1$ si et seulement si pour toute place ultramétrique v de k, l'exposant de p dans $n_v(k)$ est infini.*

Appliqué au cas des extensions cyclotomiques, cela donne :

Corollaire 4. *Soient p un nombre premier et $L/\mathbb{Q}$ une extension algébrique tels que, soit $p\neq 2$, soit L est totalement imaginaire. Si $\mathscr{Z}_p\subset L$ alors $\mathrm{cd}_p(L)\leq 1$.*

Preuve. La preuve de ce corollaire repose sur la parfaite connaissance des données de ramification dans les extensions cyclotomiques. Rappelons à cet effet le très classique lemme :

Lemme 5. *Soient m un entier et ℓ un premier. On écrit $m=\ell^k a$ avec $(a,\ell)=1$. Dans l'extension $\mathbb{Q}(\xi_m)/\mathbb{Q}$, l'indice de ramification de ℓ est égal à $e=\varphi(\ell^k)$ et son degré résiduel est égal à $f=\omega_a(\ell)$, l'ordre (multiplicatif) de ℓ modulo a.*

Pour tout entier $n\geq 1$ nous noterons $\mathscr{Z}_{p,n}$ la sous-extension de $\mathscr{Z}_p$ qui vérifie $\mathrm{Gal}(\mathscr{Z}_{p,n}/\mathbb{Q})=\mathbb{Z}/p^n\mathbb{Z}$. Considérons alors une place v de L.

Si v relève le premier p, alors l'extension $\mathscr{Z}_p/\mathbb{Q}$ étant totalement ramifiée en p on voit que $[(\mathscr{Z}_{p,n})_v:\mathbb{Q}_p]=p^n$ et donc l'exposant de p dans le degré local $n_v(L)$ est infini.

Si v relève le premier $q\neq p$, alors q ne se ramifiant pas dans $\mathscr{Z}_p$, le degré $[(\mathscr{Z}_{p,n})_v:\mathbb{Q}_q]$ est égal au degré résiduel de q dans $\mathscr{Z}_{p,n}$. Comme rappelé dans le lemme 5, le degré

résiduel de q dans $\mathbb{Q}(\xi_{p^{n+1}})$ est égal à l'ordre multiplicatif $\omega_{p^{n+1}}(q)$. Puisque $q^{\omega_{p^{n+1}}(q)} \geq p^{n+1}$, on voit que $\lim_n \omega_{p^{n+1}}(q) = +\infty$ et comme $\omega_{p^{n+1}}(q)$ divise $(p-1)p^n$, on en déduit que l'exposant de p dans $\omega_{p^{n+1}}(q)$ tend vers $+\infty$ avec n. Puisque $\mathbb{Q}(\xi_{p^{n+1}}) = \mathscr{Z}_{p,n}.\mathbb{Q}(\xi_p)$, on voit que l'exposant de p dans le degré résiduel de q dans $\mathscr{Z}_{p,n}$ tend aussi vers $+\infty$ avec n. Ainsi, l'exposant de p dans le degré local $n_v(L)$ est infini et l'on peut donc appliquer le théorème 3 pour conclure. □

On est maintenant en mesure de caractériser les sous-corps projectifs minimaux de $\mathbb{Q}^{\mathrm{ab}}$:

Théorème 6. *Soit $\Omega \subset \mathbb{Q}^{ab}$ un corps. Les propositions suivantes*

i) Ω *est un corps projectif minimal,*
ii) Ω *est égal au compositum du corps $\mathscr{Z}$ et d'un corps de nombres totalement imaginaire C, extension 2-cyclique de $\mathbb{Q}$,*
iii) Ω *est un corps totalement imaginaire et il existe un entier $r \geq 1$ tel que* $\mathrm{Gal}(\Omega/\mathbb{Q}) \simeq \mathbb{Z}/2^r \times \widehat{\mathbb{Z}}$,
iv) Ω *est un corps minimal pour les deux propriétés suivantes : il est totalement imaginaire et contient le corps $\mathscr{Z}$,*

sont équivalentes.

Preuve. *ii)* $\Longrightarrow$ *iii)* Le corps Ω est certainement totalement imaginaire puisqu'il contient C qui est totalement imaginaire. Maintenant, puisque $\mathrm{Gal}(\mathscr{Z}/\mathbb{Q}) \simeq \widehat{\mathbb{Z}}$ est un groupe projectif, il se relève dans le groupe $\mathrm{Gal}(C.\mathscr{Z}/\mathbb{Q})$ et comme ce dernier groupe est abélien, on en déduit que $\mathrm{Gal}(C.\mathscr{Z}/\mathbb{Q}) \simeq \mathrm{Gal}(\Omega/\mathscr{Z}) \times \widehat{\mathbb{Z}}$. Par un argument galoisien classique, on voit que le groupe $\mathrm{Gal}(\Omega/\mathscr{Z})$ est le relevé d'un sous-groupe de $\mathrm{Gal}(C/\mathbb{Q})$ et est donc, par suite, un 2-groupe cyclique.

iii) $\Longrightarrow$ *ii)* Puisque $\mathrm{Gal}(\Omega/\mathbb{Q}) \simeq \mathbb{Z}/2^r \times \widehat{\mathbb{Z}}$, le corps Ω est le compositum de deux extensions galoisiennes linéairement disjointes sur $\mathbb{Q}$, C et L, vérifiant respectivement $\mathrm{Gal}(C/\mathbb{Q}) \simeq \mathbb{Z}/2^r$ et $\mathrm{Gal}(L/\mathbb{Q}) \simeq \widehat{\mathbb{Z}}$.

Maintenant, le corps $\mathbb{Q}$ ne possède qu'une seule $\widehat{\mathbb{Z}}$-extension qui est $L = \mathscr{Z}$. Par ailleurs, L étant totalement réelle, si C était totalement réelle il en serait de même de Ω ce qui est contraire aux hypothèses. Ainsi, C n'est pas totalement réelle et est donc nécessairement totalement imaginaire, en tant qu'extension galoisienne de $\mathbb{Q}$.

ii) $\Longrightarrow$ *i)* Le corps Ω est certainement totalement imaginaire, puisqu'il contient un corps totalement imaginaire. Le fait que Ω soit projectif est alors une conséquence immédiate du corollaire 4. Montrons maintenant qu'il est minimal.

Supposons qu'il existe un sous-corps strict $L \subset \Omega$ qui soit projectif. Puisque par hypothèse il existe un entier $r \geq 1$ tel que $\mathrm{Gal}(\Omega/\mathbb{Q}) \simeq \mathbb{Z}/2^r \times \widehat{\mathbb{Z}}$, le groupe $H = \mathrm{Gal}(\Omega/L)$ est alors un sous-groupe fermé non trivial de $\mathbb{Z}/2^r \times \widehat{\mathbb{Z}}$. Il ne peut être inclus dans le facteur $\mathbb{Z}/2^r$ car sinon, H contiendrait l'unique involution de $\mathrm{Gal}(\Omega/\mathbb{Q})$ laquelle est la

restriction de la conjugaison complexe à Ω. Dans ces conditions, L serait invariant par la conjugaison complexe et alors le groupe $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ contiendrait un élément de torsion ce qui contredirait son caractère projectif. Le groupe H contient donc un élément $g \notin \mathbb{Z}/2^r$ et comme $\widehat{\mathbb{Z}}$ est sans torsion, $2^r g$ est alors un élément non trivial de $H \cap \widehat{\mathbb{Z}}$.

Ainsi, $H_0 = H \cap \widehat{\mathbb{Z}}$ est un sous-groupe non trivial de $\widehat{\mathbb{Z}}$ et donc

$$H_0 = \prod_{p \in \mathcal{P}_0} p^{n_p}\mathbb{Z}_p$$

où $\mathcal{P}_0$ désigne un certain ensemble non vide de nombres premiers et $(n_p)_{p\in\mathcal{P}_0}$ une collection d'entiers. Si l'on considère le corps L_0 des invariants de Ω par H_0, on a

$$\mathrm{Gal}(L_0/\mathbb{Q}) = \mathbb{Z}/2^r \times \prod_{p\in\mathcal{P}_0} \mathbb{Z}/p^{n_p} \times \prod_{p\notin\mathcal{P}_0} \mathbb{Z}_p$$

et, par ailleurs, L_0 en tant qu'extension de L est un corps projectif. Ceci est impossible, car si $p \in \mathcal{P}_0$ alors l'exposant de p dans le degré $[L_0 : \mathbb{Q}]$ est fini (égal à n_p si $p \neq 2$ et $2^r + n_2$ si $p = 2$). Puisque le degré local de L_0 en n'importe quelle place divise $[L_0 : \mathbb{Q}]$, on en déduit par le théorème 3 que $\mathrm{cd}_p(L_0) \geq 2$.

Remarque. Une autre manière de voir la non projectivité du corps L_0 repose sur la bonne connaissance de $\mathrm{Br}(\mathbb{Q})$: si l'on suppose que L_0 est projectif, alors son groupe de Brauer est nul et la suite exacte d'inflation-restriction relative aux groupes de Brauer montre que $\mathrm{Br}(\mathbb{Q}) \simeq \mathrm{H}^2(L_0/\mathbb{Q})$.

Si $p \in \mathcal{P}_0$, alors la composante p-primaire de $\mathrm{Br}(\mathbb{Q})$ s'identifie à celle du groupe $\mathrm{H}^2(\mathrm{Gal}(L_0/\mathbb{Q}), L_0^*)$. La composante p-primaire de $\mathrm{Gal}(L_0/\mathbb{Q})$ est égale à $A = \mathbb{Z}/p^{n_p}$ (resp. $A = \mathbb{Z}/2^r \times \mathbb{Z}/2^{n_2}$ si $p = 2$). Ainsi, si l'on pose $B = \mathbb{Z}/2^r \times \prod_{q\in\mathcal{P}_0,\ q\neq p} \mathbb{Z}/q^{n_q} \times \prod_{q\notin\mathcal{P}_0} \mathbb{Z}_q$ (resp. $B = \prod_{q\in\mathcal{P}_0,\ q\neq 2} \mathbb{Z}/q^{n_q} \times \prod_{q\notin\mathcal{P}_0} \mathbb{Z}_q$ si $p = 2$) alors $\mathrm{Gal}(L_0/\mathbb{Q}) = A \times B$. La suite exacte d'inflation-restriction appliquée aux composantes p-primaires donne la suite exacte suivante

$$0 \longrightarrow \mathrm{H}^2(B, L_0^{*A})_p \xrightarrow{\inf} \mathrm{H}^2(A \times B, L_0^*)_p \xrightarrow{\mathrm{res}} \mathrm{H}^2(A, L_0^*)_p$$

mais comme B est un groupe profini d'ordre premier à p, on a $\mathrm{H}^2(B, L_0^{*A})_p = 0$. Ainsi, le groupe $\mathrm{H}^2(A \times B, L_0^*)_p$, c'est-à-dire $\mathrm{Br}(\mathbb{Q})_p$, s'injecte dans le groupe $\mathrm{H}^2(A, L_0^*)_p = \mathrm{H}^2(A, L_0^*)$.

Maintenant, A étant fini, le groupe $\mathrm{H}^2(A, L_0^*)$ est d'exposant. Il est pourtant célèbre que $\mathrm{Br}(\mathbb{Q})_p$ contient un sous-groupe divisible non trivial, ce qui conduit à une absurdité.

i) $\Longrightarrow$ *iii)* Pour un nombre premier $p \neq 2$ donné, on pose $p - 1 = 2^{r_p} m_p$ avec m_p impair de sorte que l'on peut écrire $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \simeq \Gamma_0 \times \Gamma_1 \times \widehat{\mathbb{Z}}$ où Γ_0 et Γ_1 sont des sous-groupes fermés vérifiant :

$$\Gamma_0 \simeq \mathbb{Z}/2 \times \prod_{p\neq 2} \mathbb{Z}/2^{r_p} \quad \text{et} \quad \Gamma_1 \simeq \prod_{p\neq 2} \mathbb{Z}/m_p$$

On considère $\theta : \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\Omega/\mathbb{Q})$ l'épimorphisme de restriction. Pour un nombre premier $p \neq 2$ donné l'image par θ du sous-groupe $\mathbb{Z}/m_p$ de Γ_1 est un sous-groupe d'ordre impair de $\mathrm{Gal}(\Omega/\mathbb{Q})$. En application de la proposition 2 et puisque Ω est supposé minimal, on peut affirmer que $\theta(\mathbb{Z}/m_p) = 1$. Maintenant, les sous-groupes $\mathbb{Z}/m_p$ engendrent topologiquement le groupe Γ_1, on en déduit donc finalement que $\theta(\Gamma_1) = 1$.

Pour un entier $n \geq 1$ fixé, l'image par θ du sous-groupe $\mathbb{Z}/2 \times \prod_{p\leq n} \mathbb{Z}/2^{r_p}$ est un 2-groupe abélien fini. Il est nécessairement cyclique car sinon, il contiendrait au moins deux involutions ce qui contredirait, par la proposition 2, le caractère minimal de Ω. Ainsi, il existe un entier h_n tel que

$$\theta(\mathbb{Z}/2 \times \prod_{p\leq n} \mathbb{Z}/2^{r_p}) \simeq \mathbb{Z}/2^{h_n}$$

La suite des sous-groupes $\theta(\mathbb{Z}/2 \times \prod_{p\leq n} \mathbb{Z}/2^{r_p})$ est croissante, de sorte que la suite $(h_n)_{n\geq 1}$ est une suite croissante d'entiers.

Si cette suite n'est pas stationnaire, on voit que $\varinjlim_n \mathbb{Z}/2^{h_n}$ s'identifie au 2-groupe de Prüfer, $\mu_{2^\infty} \simeq \mathbb{Q}_2/\mathbb{Z}_2$, qui est un 2-groupe abélien 2-divisible. Ce groupe est isomorphe à $A = \theta(\mathbb{Z}/2 \bigoplus_p \mathbb{Z}/2^{r_p})$ et puisque $\mathbb{Z}/2 \oplus_p \mathbb{Z}/2^{r_p}$ est dense dans Γ_0, on voit que $\theta(\Gamma_0) = \overline{A}$. Dans $\mathrm{Gal}(\Omega/\mathbb{Q})$, $\overline{A}$ est un pro-2-groupe abélien. Nous allons montrer qu'il est aussi 2-divisible.

Les groupes profinis que l'on considère sont de rang dénombrable, ils sont donc métrisables et l'on peut alors utiliser le critère séquentiel pour caractériser l'adhérence. Soit $g \in \overline{A}$ et $(g_n)_{n\geq 1}$ une suite d'éléments de A qui converge vers g. Par hypothèse, il existe pour tout $n \geq 0$, un élément $h_n \in A$ tel que $2h_n = g_n$. Puisque $\overline{A}$ est compact, la suite $(h_n)_{n\geq 1}$ possède une valeur d'adhérence $h \in \overline{A}$ et cette dernière vérifie alors, par passage à la limite, $2h = g$. Ceci prouve le caractère 2-divisible de $\overline{A}$.

Par ailleurs, un pro-2-groupe non trivial G ne peut jamais être 2-divisible. En effet, si U désigne un sous-groupe ouvert de G alors $[G : U] = 2^n$ pour un certain entier n. Mais alors, pour tout $g \in G$, il existe $h \in G$ tel que $g = 2^n h \in U$. Ainsi, $U = G$, ce qui implique que G est trivial.

Ainsi, le groupe $\overline{A} = \theta(\Gamma_0)$ est trivial, ce qui est absurde car dans ces conditions $\theta(\Gamma_0 \times \Gamma_1 \times \widehat{\mathbb{Z}}) = \theta(\widehat{\mathbb{Z}})$ et donc Ω est un sous-corps de $\mathscr{Z}$, qui est un corps totalement réel.

Il existe donc un entier r tel que $\varinjlim_n \mathbb{Z}/2^{h_n} \simeq \mathbb{Z}/2^r$. Ce sous-groupe étant fini, il est fermé et l'on peut donc conclure que $\overline{\theta(\Gamma_0)} \simeq \mathbb{Z}/2^r$.

Le sous-groupe $\widehat{\mathbb{Z}}$ de $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ s'envoie par θ sur un groupe de la forme $\prod_{p\in\mathcal{P}_0} \mathbb{Z}/p^{n_p} \times \prod_{p\notin\mathcal{P}_0} \mathbb{Z}_p$ où $\mathcal{P}_0$ désigne un certain sous-ensemble de nombres premiers et $(n_p)_{p\in\mathcal{P}_0}$ une collection d'entiers.

Si $2 \notin \mathcal{P}_0$, alors la pro-2-partie de $\mathrm{Gal}(\Omega/\mathbb{Q})$ est engendrée par $\mathbb{Z}/2^r$ et $\mathbb{Z}_2$, mais comme elle est abélienne et que l'un des facteurs est de torsion alors que l'autre est sans torsion, on en déduit qu'elle est égale à $\mathbb{Z}/2^r \times \mathbb{Z}_2$, de sorte que l'on a

$$\mathrm{Gal}(\Omega/\mathbb{Q}) \simeq \mathbb{Z}/2^r \times \prod_{p\in\mathcal{P}_0} \mathbb{Z}/p^{n_p} \times \prod_{p\notin\mathcal{P}_0} \mathbb{Z}_p$$

Si $2 \in \mathcal{P}_0$ alors la pro-2-partie de $\mathrm{Gal}(\Omega/\mathbb{Q})$ est engendrée par $\mathbb{Z}/2^r$ et $\mathbb{Z}/2^{n_2}$ et est donc un 2-groupe abélien fini D. On a alors

$$\mathrm{Gal}(\Omega/\mathbb{Q}) \simeq D \times \prod_{p\in\mathcal{P}_0,\ p\neq 2} \mathbb{Z}/p^{n_p} \times \prod_{p\notin\mathcal{P}_0} \mathbb{Z}_p$$

Si $\mathcal{P}_0 \neq \emptyset$ alors dans les deux cas, la proposition 2 conduit à une absurdité. Ceci prouve donc que l'image par θ du facteur $\widehat{\mathbb{Z}}$ est égale à $\widehat{\mathbb{Z}}$. Le groupe $\widehat{\mathbb{Z}}$ est sans torsion, alors que $\mathbb{Z}/2^r$ est de torsion et ainsi, l'image de θ, c'est-à-dire le groupe $\mathrm{Gal}(\Omega/\mathbb{Q})$, est isomorphe à $\mathbb{Z}/2^r \times \widehat{\mathbb{Z}}$.

iv) $\Longrightarrow$ *ii)* Puisque $\Omega/\mathbb{Q}$ est totalement imaginaire il existe un élément $\alpha \in \Omega - \mathbb{Q}$ totalement imaginaire (voir le lemme 8 à venir). Si l'on pose $C = \mathbb{Q}(\alpha)$ alors C et $\mathscr{Z}$ sont des corps linéairement disjoints sur $\mathbb{Q}$ et $C.\mathscr{Z}$ est un corps totalement imaginaire contenant $\mathscr{Z}$. Par minimalité de Ω on a donc $\Omega = C.\mathscr{Z}$. L'extension $C/\mathbb{Q}$ est abélienne et finie et l'on a donc $\mathrm{Gal}(C/\mathbb{Q}) = \prod_{i=1}^{n} \mathbb{Z}/2^{k_i} \times G$ où G est un groupe abélien d'ordre impair. Dire que C est totalement imaginaire équivaut ici à dire que la restriction de la conjugaison complexe à $\mathrm{Gal}(C/\mathbb{Q})$ est non triviale. Il existe donc un indice i_0 tel que la restriction de la conjugaison complexe au facteur $\mathbb{Z}/2^{k_{i_0}}$ soit non triviale. Si l'on considère $C'/\mathbb{Q}$ la sous-extension de C vérifiant $\mathrm{Gal}(C'/\mathbb{Q}) = \mathbb{Z}/2^{k_{i_0}}$ alors le corps C' est totalement imaginaire, tout comme $C'.\mathscr{Z}$. Par minimalité de Ω, on en déduit que $C = C'$ et le *ii)*.

iii) $\Longrightarrow$ *iv)* Si $\Omega' \subset \Omega$ est un corps totalement imaginaire qui contient $\mathscr{Z}$, alors $\mathrm{Gal}(\Omega/\Omega')$ a une intersection nulle avec le facteur $\widehat{\mathbb{Z}}$. Comme $\mathbb{Z}/2^r$ est de torsion et que $\widehat{\mathbb{Z}}$ est sans torsion, cela implique finalement que $\mathrm{Gal}(\Omega/\Omega')$ est complètement inclus dans le facteur $\mathbb{Z}/2^r$. Si $\mathrm{Gal}(\Omega/\Omega')$ n'était pas trivial alors il contiendrait l'élément d'ordre 2 de $\mathbb{Z}/2^r$, qui est l'unique élément d'ordre 2 de $\mathbb{Z}/2^r \times \widehat{\mathbb{Z}}$. Cet élément correspondant à la conjugaison complexe, on en déduirait que Ω' est totalement réel, ce qui est contraire aux hypothèses. □

Dans la preuve du théorème 6, la propriété de minimalité est intimement liée au fait de contenir le corps $\mathscr{Z}$. Plus généralement, on a :

Proposition 7. *Soit $\Omega \subset \overline{\mathbb{Q}}$ un corps contenant le corps $\mathscr{Z}$ (on ne suppose pas que $\Omega/\mathbb{Q}$ soit abélienne, pas même galoisienne a priori).*

a) Si $\Omega/\mathscr{Z}$ est finie, alors tout sous-corps projectif de Ω contient $\mathscr{Z}$.

b) Le corps Ω est projectif si et seulement si Ω est totalement imaginaire. En conséquence de quoi, si le corps Ω est projectif alors il est extension d'un corps projectif minimal contenant $\mathscr{Z}$. Les corps projectifs minimaux contenant le corps $\mathscr{Z}$ sont exactement les extensions finies totalement imaginaires minimales de $\mathscr{Z}$.

Preuve. a) 1/ Cas particulier où $\Omega/\mathbb{Q}$ est galoisienne. Notons $\Gamma = \mathrm{Gal}(\Omega/\mathbb{Q})$ et $N = \mathrm{Gal}(\Omega/\mathscr{Z})$. Puisque $\Gamma/N \simeq \mathrm{Gal}(\mathscr{Z}/\mathbb{Q}) = \widehat{\mathbb{Z}}$ et que ce groupe est projectif, on en déduit que $\Gamma \simeq N \rtimes \widehat{\mathbb{Z}}$. Soit $\Omega_0 \subset \Omega$ un sous-corps projectif et $N_0 = \mathrm{Gal}(\Omega/\Omega_0)$. Raisonnons

par l'absurde et supposons que $N_0 \not\subset N$. Il existe donc $(t,x) \in N \rtimes \widehat{\mathbb{Z}}$ avec $x \neq 0$ tel que $(t,x) \in N_0$. Si $\varphi \in \mathrm{Aut}(N)$ désigne l'action de x sur N, on a alors pour tout $n \geq 1$,

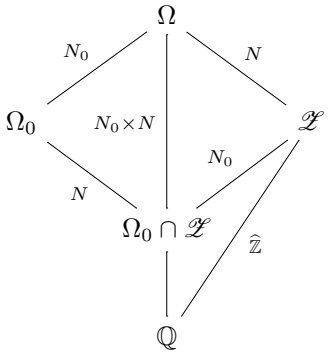
$$(t,x)^n = (t\varphi(t)\cdots\varphi^{n-1}(t), nx) \in N_0$$

Puisque N est fini, il existe $n_0 > m_0$ tels que

$$t\varphi(t)\cdots\varphi^{n_0}(t) = t\varphi(t)\cdots\varphi^{m_0}(t)$$

et l'on a donc $t\varphi(t)\cdots\varphi^{n_0-m_0-1}(t) = e$. Il existe donc $n = n_0 - m_0$ tel que $(t,x)^n = (e,nx) \in N_0$. Dans le facteur $\widehat{\mathbb{Z}}$ de Γ, on peut écrire $\overline{< nx >} = \prod_{p\in\mathscr{P}_0\neq\emptyset} p^{n_p}\mathbb{Z}_p$ où $\mathcal{P}_0$ désigne un certain ensemble non vide de nombres premiers et $(n_p)_{p\in\mathcal{P}_0}$ une collection d'entiers. Quitte à considérer un sous-groupe de N_0 (ce qui revient à considérer une extension de Ω_0 qui reste alors projective), on peut supposer que $N_0 = p^{n_p}\mathbb{Z}_p \subset \widehat{\mathbb{Z}}$ pour un certain premier p et un entier n_p arbitrairement grand.

Si l'on note $\Theta : \widehat{\mathbb{Z}} \longrightarrow \mathrm{Aut}(N)$ l'action de $\widehat{\mathbb{Z}}$ sur N, alors on a $\ker(\Theta) = h\widehat{\mathbb{Z}}$ où h est un entier qui désigne l'ordre de $\Theta(1)$ dans le groupe fini $\mathrm{Aut}(N)$. Comme h ne dépend ni de p ni de n_p, on peut donc choisir n_p de sorte que $N_0 \subset \ker(\Theta)$. Dans cette situation, on a $N \rtimes N_0 = N \times N_0$ et le diagramme d'extensions suivant :



La théorie de Galois assure que $\mathrm{Gal}(\Omega_0 \cap \mathscr{Z}/\mathbb{Q}) = \widehat{\mathbb{Z}}/N_0 = \mathbb{Z}/p^{n_p} \times \prod_{q\neq p}\mathbb{Z}_q$ et donc l'exposant de p dans le degré de $[\Omega_0 : \mathbb{Q}]$ est fini (il vaut exactement $n_p.o_p$ où o_p désigne l'exposant de p dans $o(N)$). Ceci rend impossible le fait que $\mathrm{cd}_p(\Omega_0) \leq 1$ et donc que Ω_0 soit projectif.

2/ Cas général. Il se déduit du cas particulier en considérant la clôture galoisienne de Ω sur $\mathbb{Q}$ et en remarquant que cette dernière est nécessairement de dimension finie sur $\mathscr{Z}$ car $\Omega/\mathscr{Z}$ est finie et $\mathscr{Z}/\mathbb{Q}$ est galoisienne.

b) Si Ω est totalement imaginaire, son caractère projectif découle immédiatement du corollaire 4. Réciproquement, un corps projectif, extension algébrique de $\mathbb{Q}$, est nécessairement totalement imaginaire, car un plongement réel impliquerait par isomorphisme une 2-dimension cohomologique infinie.

Pour montrer la suite de l'énoncé, établissons le lemme suivant :

Lemme 8. *Si $L \subset \overline{\mathbb{Q}}$ est un corps totalement imaginaire, alors il existe un corps de nombres $K \subset L$ qui est totalement imaginaire.*

Preuve. Considérons une filtration croissante, $\mathbb{Q} = L_0 \subset L_1 \subset \cdots \subset L$, de L par des corps de nombres. Supposons qu'aucun des corps L_n ne soit totalement imaginaire et, pour $n \geq 0$ fixé, notons $\mathscr{I}_n$ l'ensemble des plongements de L_n dans $\mathbb{R}$. L'inclusion $L_n \subset L_{n+1}$ définit, par restriction des plongements, une application naturelle $\varphi_{n+1} : \mathscr{I}_{n+1} \longrightarrow \mathscr{I}_n$ pour tout n. On voit alors que $(\mathscr{I}_n, \varphi_n)_{n\geq 0}$ est un système projectif et que $\varprojlim_n \mathscr{I}_n$ correspond à l'ensemble des plongements réels du corps L (qui est vide par hypothèse). Par hypothèse, l'ensemble $\mathscr{I}_n$ est non vide et il est par ailleurs fini puisque $L_n/\mathbb{Q}$ est fini. L'argument classique de compacité assure alors que $\varprojlim_n \mathscr{I}_n \neq \emptyset$, ce qui constitue une absurdité. □

D'après le lemme 8, il existe un corps de nombres $K \subset \Omega$ totalement imaginaire. Le corps $L = K.\mathscr{Z}$ est alors un corps totalement imaginaire de dimension finie sur $\mathscr{Z}$. Puisque $L/\mathscr{Z}$ est finie, elle possède un nombre fini d'extensions intermédiaires et donc il existe une extension intermédiaire $\mathscr{Z} \subset L_0 \subset L$ totalement imaginaire qui soit minimale. Le a) de la proposition montre alors que L_0 est un corps projectif minimal dont Ω est extension.

La fin de la proposition découle alors des arguments donnés précédemment. □

Une application immédiate du théorème 6 assure que le corps $\Omega_2 = \mathbb{Q}(\sqrt{-1}).\mathscr{Z}$ est projectif minimal. Dans cette situation, on a

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\Omega_2) \simeq \prod_{p\neq 2} \mathbb{Z}/(p-1) \text{ et } \mathrm{Gal}(\Omega_2/\mathbb{Q}) \simeq \mathbb{Z}/2 \times \widehat{\mathbb{Z}}$$

D'un point de vue galoisien, le corps Ω_2 est obtenu en ne conservant que le facteur direct $\mathbb{Z}/2$ du facteur $\mathbb{Z}/2 \times \prod_{p\neq 2} \mathbb{Z}/(p-1)$. On peut opérer la même chose sur les autres facteurs : pour un nombre premier $q \neq 2$, on écrit $q - 1 = 2^r.m$ avec m impair de sorte que l'on dispose de la décomposition $\mathbb{Z}/(q-1) = \mathbb{Z}/2^r \times \mathbb{Z}/m$. On considère alors le sous-corps Ω_q de $\mathbb{Q}^{\mathrm{ab}}$ constitué des éléments invariants par le sous-groupe $\mathbb{Z}/m \times \mathbb{Z}/2 \times \prod_{p\neq q} \mathbb{Z}/(p-1)$, de sorte que

$$\mathrm{Gal}(\Omega_q/\mathbb{Q}) \simeq \mathbb{Z}/2^r \times \widehat{\mathbb{Z}}$$

Le corps Ω_q est alors projectif minimal et est obtenu en ne conservant que le facteur de 2-torsion du facteur direct $\mathbb{Z}/(q-1)$ du groupe $\mathbb{Z}/2 \times \prod_{p\neq 2} \mathbb{Z}/(p-1)$.

Décrire tous les sous-corps projectifs minimaux de $\mathbb{Q}^{\mathrm{ab}}$ revient à décrire tous les corps de nombres imaginaires purs, extensions 2-cycliques de $\mathbb{Q}$, c'est-à-dire à décrire tous

les épimorphismes continus $\theta : \Gamma_0 \longrightarrow \mathbb{Z}/2^r$ avec r arbitraire, qui ne contienne pas la conjugaison complexe dans leur noyau.

Le groupe $\mathbb{Z}/2^r$ étant fini est discret et, comme θ est continu, il est localement constant. On en déduit qu'il existe une famille finie de nombres premiers impairs $q_1, \cdots, q_n$ telle que $\prod_{p\neq 2, q_1, \cdots, q_n} \mathbb{Z}/2^{r_p} \subset \ker(\theta)$. Ainsi, tout revient à chercher des épimorphismes

$$\theta : \mathbb{Z}/2 \times \mathbb{Z}/2^{r_{q_1}} \times \cdots \times \mathbb{Z}/2^{r_{q_n}} \longrightarrow \mathbb{Z}/2^r$$

qui ne contiennent pas l'involution diagonale dans leur noyau.

Considérons $g, g_0, g_1, \cdots, g_n$ des générateurs respectifs des groupes $\mathbb{Z}/2^r$, $\mathbb{Z}/2$ et $\mathbb{Z}/2^{r_{q_i}}$ pour $i = 1, \cdots, n$. Pour chaque indice $i = 0, \cdots, n$, il existe un unique $a_i \in \{0, \cdots, 2^r - 1\}$ tel que $\theta(g_i) = g^{a_i}$. En ayant pris soin de poser $r_{q_0} = 1$, on voit alors que θ existe si et seulement si on a les trois conditions suivantes :

(C1) : Pour tout $i = 0, \cdots, n$, on a $a_i 2^{r_{q_i}} \equiv 0 \bmod(2^r)$ (assure le caractère morphique de θ).
(C2) : Au moins un des a_i est inversible modulo 2^r (assure le caractère surjectif de θ).
(C3) : $a_0 + a_1 2^{r_{q_1}-1} + \cdots + a_n 2^{r_{q_n}-1} \not\equiv 0 \bmod(2^r)$ (assure que l'involution diagonale n'est pas dans le noyau).

Remarque 9. La "grosse" partie du groupe $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \simeq \mathbb{Z}/(p-1) \times \mathbb{Z}_p$ est $\mathbb{Z}_p$ et l'on pense souvent, à cause de cela, que la partie la plus importante de $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \simeq \mathbb{Z}/2 \times \prod_{p\neq 2} \mathbb{Z}/(p-1) \times \widehat{\mathbb{Z}}$ est $\widehat{\mathbb{Z}}$. C'est pourtant, d'une certaine manière, l'inverse.

Le groupe $\widehat{\mathbb{Z}}$ est de rang 1 alors que celui de $\prod_{p\neq 2} \mathbb{Z}/(p-1)$ est infini. Par ailleurs, étant donné un nombre premier q et un entier n, le théorème de progression arithmétique de Dirichlet montre qu'il existe une infinité de premiers p tel que la valuation q-adique de $p-1$ soit égale à n. Ainsi, on en déduit que

$$\prod_{p\neq 2} \mathbb{Z}/(p-1) \simeq \left(\prod_q \prod_n \mathbb{Z}/q^n \right)^\omega$$

mais comme le groupe $\mathbb{Z}_q$ est un sous-groupe fermé de $\prod_n \mathbb{Z}/q^n$, on voit que le groupe $\widehat{\mathbb{Z}}^\omega$ est un sous-groupe fermé de $\prod_{p\neq 2} \mathbb{Z}/(p-1)$ et il existe donc un corps K tel que

$$\Omega_2 \longrightarrow K \xrightarrow{\widehat{\mathbb{Z}}^\omega} \mathbb{Q}^{\mathrm{ab}}$$

2.2. Une description simple des groupes de Galois absolus des corps de nombres

Revenons maintenant à la conjecture de Shafarevich et aux différentes conjectures qui l'impliquent. Comme on l'a annoncé dans l'introduction de ce texte, au regard des

résultats du §2, la conjecture de Shafarevich n'est pas la plus optimale sous la conjecture de Fried–Völklein. Par ailleurs, la conjecture de Shafarevich ne permet pas de décrire simplement le groupe de Galois absolu de $\mathbb{Q}$. On s'aventure ici à proposer deux autres conjectures :

$\mathscr{Z}$-conjecture. *Les extensions finies et totalement imaginaires du corps $\mathscr{Z}$ possèdent un groupe de Galois absolu prolibre.*

En utilisant les résultats précédents, on voit que la $\mathscr{Z}$-conjecture entraine l'énoncé suivant : *les sous-corps projectifs minimaux de $\mathbb{Q}^{ab}$ possèdent un groupe de Galois absolu prolibre.* Cet énoncé est une version de la conjecture de Shafarevich minimisant le corps $\mathbb{Q}^{\mathrm{ab}}$, par exemple en remplacant ce dernier par le corps $\mathscr{Z}(i)$. On l'appelera la **conjecture de Shafarevich minimisée**.

Conjecture de Shafarevich généralisée. *Les sous-corps projectifs de $\mathbb{Q}^{ab}$ possèdent un groupe de Galois absolu prolibre.*

L'intérêt de la $\mathscr{Z}$-conjecture est que le groupe $\widehat{\mathbb{Z}}$ est un groupe projectif et qui donc se relève dans tout groupe profini dont il est le quotient.

Proposition 10. *Sous la $\mathscr{Z}$-conjecture, si C désigne un corps de nombres alors*

a) Si C est totalement imaginaire, on a $\mathrm{Gal}(\overline{\mathbb{Q}}/C) \simeq \widehat{F}_\omega \rtimes \widehat{\mathbb{Z}}$.
b) Si C n'est totalement imaginaire, on a $\mathrm{Gal}(\overline{\mathbb{Q}}/C) \simeq \left(\widehat{F}_\omega \rtimes \widehat{\mathbb{Z}}\right) \rtimes \mathbb{Z}/2$.

En particulier, sous la $\mathscr{Z}$-conjecture, on a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \simeq \left(\widehat{F}_\omega \rtimes \widehat{\mathbb{Z}}\right) \rtimes \mathbb{Z}/2$.

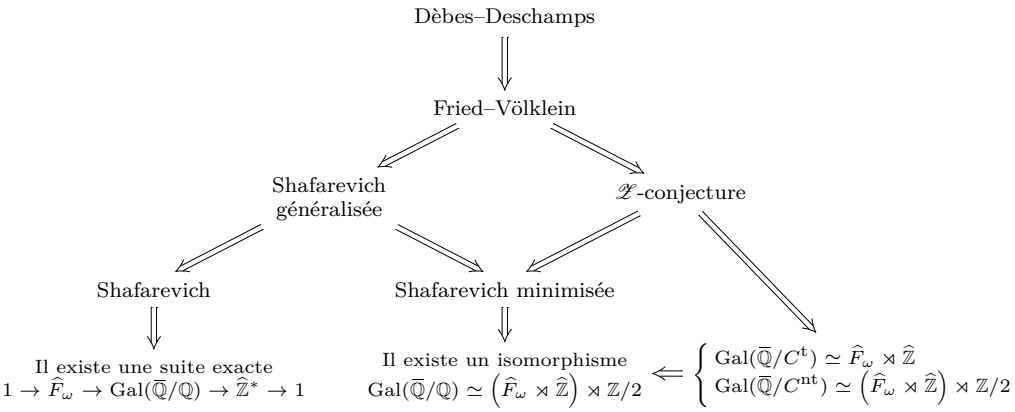
Preuve. Si C n'est pas totalement imaginaire, alors $C(i)$ l'est et comme l'élément non trivial de $\mathrm{Gal}(C(i)/C) = \mathbb{Z}/2\mathbb{Z}$ correspond à la restriction de la conjugaison complexe, on en déduit que $\mathrm{Gal}(\overline{\mathbb{Q}}/C) \simeq \mathrm{Gal}(\overline{\mathbb{Q}}/C(i)) \rtimes \mathbb{Z}/2$. On peut donc supposer que C est totalement imaginaire. Dans ces conditions, le corps $C.\mathscr{Z}$ est une extension finie totalement imaginaire de $\mathscr{Z}$ et donc $\mathrm{Gal}(\overline{\mathbb{Q}}/C.\mathscr{Z}) \simeq \widehat{F}_\omega$. On a alors la suite exacte

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{Q}}/C.\mathscr{Z}) & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{Q}}/C) & \longrightarrow & \mathrm{Gal}(C.\mathscr{Z}/C) & \longrightarrow & 1 \\ & & \downarrow \simeq & & & & \downarrow \simeq & & \\ 1 & \longrightarrow & \widehat{F}_\omega & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{Q}}/C) & \longrightarrow & \widehat{\mathbb{Z}} & \longrightarrow & 1 \end{array}$$

qui, compte-tenu du caractère projectif du groupe $\widehat{\mathbb{Z}}$, est scindée et assure donc un isomorphisme de la forme $\mathrm{Gal}(\overline{\mathbb{Q}}/C) \simeq \widehat{F}_\omega \rtimes \widehat{\mathbb{Z}}$. □

On voit que l'on peut remplacer la $\mathscr{Z}$-conjecture par la conjecture de Shafarevich minimisée dans la proposition 10 à condition de ne considérer pour C que des extensions abéliennes de $\mathbb{Q}$. En particulier, on voit que la conjecture de Shafarevich minimisée entraine l'existence d'un isomorphisme $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \simeq \left(\widehat{F}_\omega \rtimes \widehat{\mathbb{Z}}\right) \rtimes \mathbb{Z}/2$.

La $\mathscr{Z}$-conjecture et la conjecture de Shafarevich généralisée sont en fait contenues dans la conjecture de Fried–Völklein. En effet, les corps considérés dans ces deux conjectures sont projectifs et dénombrables, leur caractère hilbertien découle du théorème de Kuyk pour la conjecture de Shafarevich généralisée et du théorème de Weissauer pour la $\mathscr{Z}$-conjecture (ce dernier théorème assure qu'une extension finie et stricte d'une extension galoisienne d'un corps hilbertien est un corps hilbertien, voir [3]). En résumé, pour ce qui est des différentes conjectures dont on a parlé, on a la hiérarchie suivante :



(C^{t} (resp. C^{nt}) désigne n'importe quel corps de nombres totalement imaginaire (resp. non totalement imaginaire).)

Remarque 11. La théorie anabélienne assure que deux corps de nombres ont des groupes de Galois absolus isomorphes si et seulement si ces corps sont eux-même isomorphes. De ce point de vue l'isomorphisme avec le produit semi-direct $\widehat{F}_\omega \rtimes \widehat{\mathbb{Z}}$ donné dans la proposition 10 peut prêter à confusion. En fait, dans l'écriture $\widehat{F}_\omega \rtimes \widehat{\mathbb{Z}}$ la chose indéterminée (et à mieux comprendre) reste l'action de $\widehat{\mathbb{Z}}$ sur $\widehat{F}_\omega$. Une conséquence de la $\mathscr{Z}$-conjecture à ce sujet est l'existence d'une correspondance injective entre les classes d'isomorphismes des corps de nombres et les classes d'équivalence des $\widehat{\mathbb{Z}}$-actions de $\widehat{F}_\omega$ pour la relation d'équivalence $\alpha \sim \beta \iff \widehat{F}_\omega \rtimes_\alpha \widehat{\mathbb{Z}} \simeq \widehat{F}_\omega \rtimes_\beta \widehat{\mathbb{Z}}$.

Considèrons $\alpha : \widehat{\mathbb{Z}} \longrightarrow \mathrm{Aut}(\widehat{F}_\omega)$ une action qui, sous la $\mathscr{Z}$-conjecture, définit un isomorphisme $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \simeq \left(\widehat{F}_\omega \rtimes_\alpha \widehat{\mathbb{Z}}\right) \rtimes \mathbb{Z}/2$ et notons Q le corps des invariants par le facteur $\widehat{F}_\omega \rtimes_\alpha \widehat{\mathbb{Z}}$ (Q est donc une extension quadratique de $\mathbb{Q}$). Certaines propriétés arithmétiques de $\mathbb{Q}$, permettent de préciser plusieurs choses sur α :

a) Notons que, puisque $\widehat{\mathbb{Z}}$ est monogène et que l'action est continue (elle correspond dans $\mathrm{Gal}(\overline{\mathbb{Q}}/Q)$ à des conjugaisons), la donnée de l'action est entièrement déterminée

par l'action de $1 \in \widehat{\mathbb{Z}}$ sur le groupe $\widehat{F}_\omega$, c'est-à-dire par la donnée d'un automorphisme $\theta \in \mathrm{Aut}(\widehat{F}_\omega)$. Maintenant, les éléments de $\mathrm{Aut}(\widehat{F}_\omega)$ sont entièrement déterminés par leurs images sur une base $\mathscr{B}$ de $\widehat{F}_\omega$ donnée. L'automorphisme θ envoie $\mathscr{B}$ sur une autre base. La théorie d'Iwasawa permet de préciser une chose sur cette donnée : **l'automorphisme θ n'envoie aucune base $\mathscr{B}$ sur elle-même.**

Pour montrer ce fait, supposons qu'il existe une telle base $\mathscr{B}$ et considérons alors les orbites des éléments de $\mathscr{B}$ sous l'action de θ. Elles forment une partition de $\mathscr{B}$ et, si $\{x_i\}_{i\in I}$ désigne une classe de représentants des orbites $\mathscr{O}_\theta(x)$, alors on a nécessairement $\sharp I \leq 2$. En effet, supposons qu'il existe trois indices $i_1, i_2, i_3 \in I$ disctincts. Notons alors $\alpha_1, \alpha_2, \alpha_3$ une base du groupe prolibre de rang 3, $\widehat{F}_3$. L'application $\pi : \mathscr{B} \longrightarrow \widehat{F}_3$ définie par

$$\begin{aligned}\pi(x) &= \alpha_j \text{ pour tout } x \in \mathscr{O}_\theta(x_{i_j}) \ (j = 1, 2, 3)\\ &= e \text{ pour tout } x \notin \mathscr{O}_\theta(x_{i_1}) \cup \mathscr{O}_\theta(x_{i_2}) \cup \mathscr{O}_\theta(x_{i_3})\end{aligned}$$

définit un unique épimorphisme $\pi : \widehat{F}_\omega \longrightarrow \widehat{F}_3$ qui vérifie que, pour tout $t \in \widehat{F}_\omega$, $\pi(\theta(t)) = \pi(t)$. Il s'ensuit que π se relève à $\widehat{F}_\omega \rtimes \widehat{\mathbb{Z}}$ tout entier en posant $\pi(\widehat{\mathbb{Z}}) = e$ et donc que le groupe $\widehat{F}_3$ se réalise sur Q ce qui est impossible (voir par exemple la remarque 1.6. de [2] sur le degré de liberté d'un corps de nombres).

Ainsi, $I = \{i_1, i_2\}$ (ou $I = \{i_1\}$, l'argument qui suit s'adaptant facilement à ce cas). Prenons alors un groupe abélien G de rang ≥ 4. En tant que groupe abélien, il se réalise sur Q et donc il existe un épimorphisme $\pi : \widehat{F}_\omega \rtimes \widehat{\mathbb{Z}} \longrightarrow G$. Posons $g_1 = \pi(x_{i_1})$, $g_2 = \pi(x_{i_2})$ et $g_3 = \pi(1)$ (1 désignant ici le neutre multiplicatif de $\widehat{\mathbb{Z}}$, qui est un générateur topologique du groupe additif). Puisque pour tout $t \in \widehat{F}_\omega$, on a $\pi(\theta(t)) = \pi(1)\pi(t)\pi(1)^{-1} = \pi(t)$, on en déduit que pour tout $x \in \mathscr{B}$, $\pi(x) = g_1$ ou g_2. Ainsi, l'image par π de $\widehat{F}_\omega \rtimes \widehat{\mathbb{Z}}$ est le groupe $< g_1, g_2, g_3 >$ qui, étant de rang ≤ 3, ne peut être égal à G tout entier.

b) Si $x \in \ker(\alpha)$, on a alors $\alpha(x)(\gamma) = x\gamma x^{-1} = \gamma$ pour tout $\gamma \in \widehat{F}_\omega$. Puisque $\widehat{\mathbb{Z}}$ est lui-même abélien, on en déduit que x est central dans $\mathrm{Gal}(\overline{\mathbb{Q}}/Q)$ et donc que $x = 0$. On vient ici de justifier que **l'action α est fidèle**.

c) Une autre propriété de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ montre que **l'action α ne possède pas de point fixe** : si $\gamma \in \widehat{F}_\omega$ est un point fixe de $\alpha(x)$ pour un certain $x \in \widehat{\mathbb{Z}}$ non nul, alors x et γ commutent et donc $< x, \gamma >$ est un sous-groupe abélien de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Il est alors nécessairement de rang 1 (cf [4, ex.2 §II.3.3.]) et donc, les ordres $o(x)$ et $o(\gamma)$ sont premiers entre eux. Puisque $o(\widehat{\mathbb{Z}}) = \prod_p p^\infty$ on en déduit, en particulier, que α n'a pas de point fixe.

2.3. Digressions arithmétiques

On note $p_1, p_2, \cdots$ la suite croissante des nombres premiers et l'on fixe un isomorphisme $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) = \mathbb{Z}/2 \times \prod_{n\geq 2} \mathbb{Z}/(p_n - 1) \times \widehat{\mathbb{Z}}$. Pour $n \geq 2$, on note $\mathscr{K}_n$ le corps des invariants de $\mathbb{Q}^{\mathrm{ab}}$ par le sous-groupe $\mathbb{Z}/2 \times \prod_{i=2}^{n} \mathbb{Z}/(p_i - 1)$. On a donc

$$\mathrm{Gal}(\mathscr{K}_n/\mathbb{Q}) = \prod_{i>n} \mathbb{Z}/(p_i - 1) \times \widehat{\mathbb{Z}}$$

La suite $(\mathscr{K}_n)_{n\geq 2}$ a alors les propriétés suivantes :

P_1) $(\mathscr{K}_n)_{n\geq 2}$ est une suite strictement décroissante de corps projectifs.
P_2) Pour tout entier $n \geq 2$, $\mathscr{K}_n/\mathscr{K}_{n+1}$ est finie.
P_3) Le corps $\mathscr{Z} = \bigcap_{n\geq 2} \mathscr{K}_n$ n'est pas projectif et les $\mathscr{K}_n$ sont des extensions algébriques de $\mathscr{Z}$.

Nous allons voir trois conséquences à ce constat.

a) *Une conséquence géométrique.*

La non projectivité du corps $\mathscr{Z}$ équivaut à l'existence d'une extension finie $\mathscr{Z}(\alpha)/\mathscr{Z}$ telle que l'application de norme $N : \mathscr{Z}(\alpha) \longrightarrow \mathscr{Z}$ ne soit pas surjective (cf [4, Proposition II.3.1.5]). Puisque $\bigcap_{n\geq 2} \mathscr{K}_n = \mathscr{Z}$, il existe donc un rang à partir duquel $\mathscr{K}_n \cap \mathscr{Z}(\alpha) = \mathscr{Z}$. On peut donc supposer que ce rang est $n = 2$, de sorte que $[\mathscr{K}_n(\alpha) : \mathscr{K}_n] = [\mathscr{Z}(\alpha) : \mathscr{Z}] = h$ pour tout $n \geq 2$. Si $\underline{b} = (b_1, \cdots, b_h)$ désigne une $\mathscr{Z}$-base de $\mathscr{Z}(\alpha)$, alors $\underline{b}$ est aussi une $\mathscr{K}_n$-base de $\mathscr{K}_n(\alpha)$ pour tout n. Relativement à $\underline{b}$, la norme N s'exprime comme un polynôme homogène $P \in \mathscr{Z}[x_1, \cdots, x_n]$. Pour des raisons évidentes l'application de norme $N_n : \mathscr{K}_n(\alpha) \longrightarrow \mathscr{K}_n$ s'exprime dans $\underline{b}$ par le même polynôme P. Les corps $\mathscr{K}_n$ étant projectifs, toutes les applications N_n sont surjectives (cf [4, Proposition II.3.1.5]). Si $\lambda \in \mathscr{Z}$ désigne un élément qui n'est pas atteint par N, alors la variété V définie par le polynôme $P - \lambda$ possède des points $\mathscr{K}_n$-rationnels pour tout $n \geq 2$, mais aucun point $\mathscr{Z}$ rationnel.

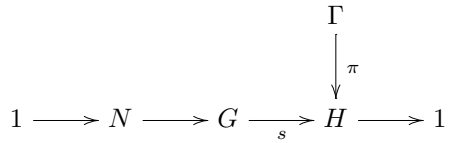
Conséquence. *Il existe un corps k, une suite décroissante $(L_n)_{n\geq 1}$ d'extensions algébriques de k telle que $k = \bigcap_{n\geq 1} L_n$ et L_n/L_{n+1} soit finie pour tout $n \geq 1$ et une k-variété V tels que $V(L_n) \neq \emptyset$ pour tout $n \geq 1$ et $V(k) = \emptyset$.*

b) *Une conséquence sur les groupes profinis.*

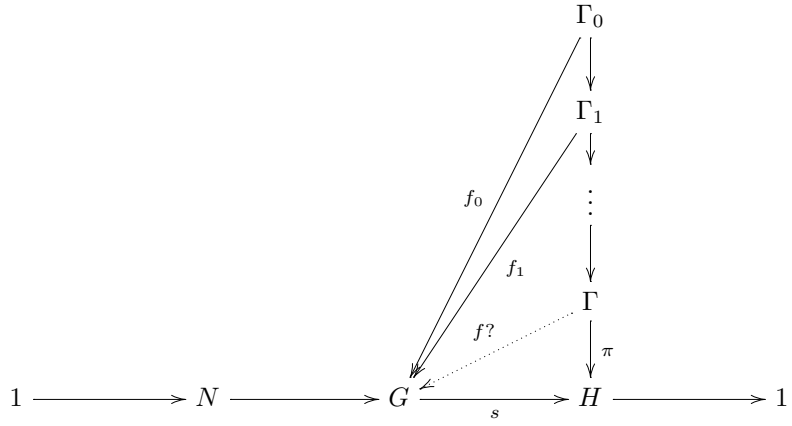
Si l'on pose $\Gamma = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathscr{Z})$ et, pour tout $n \geq 2$, $\Gamma_n = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathscr{K}_n)$, alors les groupes Γ_n sont des sous-groupes fermés du groupe Γ et l'hypothèse $\mathscr{Z} = \bigcap_{n\geq 2} \mathscr{K}_n$ dit que Γ est (topologiquement) engendré par la réunion des Γ_n. Les quotients Γ_{n+1}/Γ_n s'identifie aux groupes $\mathrm{Gal}(\mathscr{K}_n/\mathscr{K}_{n+1})$ et sont donc finis. Par hypothèse, chaque Γ_n est projectif et Γ ne l'est pas.

Conséquence. *Il existe un groupe profini Γ non projectif qui est engendré par une suite croissante de sous-groupes distingués fermés projectifs $(\Gamma_n)_{n\geq 1}$ telle que Γ_{n+1}/Γ_n soit fini pour tout n.*

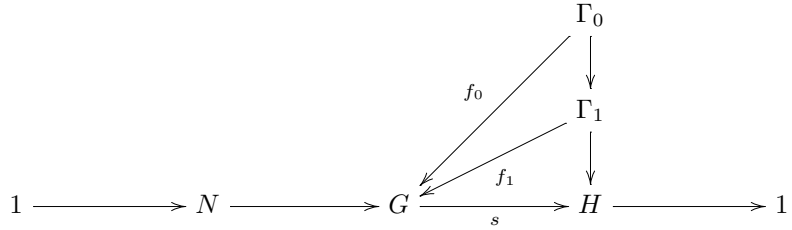
Traduit en termes de problème de plongement, la question se ramène à relever des solutions : on considère un problème de plongement de groupes finis à noyau abélien pour Γ



Ce problème induit, par restriction, sur chaque sous-groupe Γ_n un problème de plongement qui, par projectivité de Γ_n possède une solution f_n. Et l'on cherche une solution $f : \Gamma \longrightarrow G$:



Si chaque flêche f_n relève la flêche f_{n-1}, l'hypothèse $\overline{\bigcup_n \Gamma_n} = \Gamma$, permet alors, par continuité, de construire la flêche f recherchée. Réciproquement, la donnée d'une solution f induit l'existence de solutions $f_0, f_1, \cdots$ telles que f_n relève f_{n-1} pour tout $n \geq 1$. On est donc amené à étudier le problème suivant : on se donne un problème de plongement



avec des solutions respectives f_0 et f_1 et l'on se demande s'il existe une solution $f_1' : \Gamma_1 \longrightarrow G$ qui relève f_0 ? Cette question est en fait une pure question de cohomologie des groupes. En effet, on fait agir Γ_0 sur N *via* la restriction de f_1 à Γ_0 : $t^x = f_1(x^{-1})tf_1(x)$

et l'on considère N comme Γ_0-module pour cette action. Un petit calcul montre alors que l'application $\mu : x \longmapsto f_0(x)f_1(x^{-1})$ est un 1-cocycle à valeurs dans N. On constate alors que f_0 se relève à Γ_1 si et seulement si μ se relève en un 1-cocyle de Γ_1. Cette propriété étant invariante par cobordisme, elle équivaut encore à dire que l'élément du $\mathrm{H}^1(\Gamma_0, N)$ défini par μ est dans l'image du morphisme de restriction $\mathrm{H}^1(\Gamma_1, N) \longrightarrow \mathrm{H}^1(\Gamma_0, N)$ ou encore, compte-tenu de la suite exacte

$$1 \longrightarrow \mathrm{H}^1(\Gamma_1/\Gamma_0, N^{\Gamma_0}) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(\Gamma_1, N) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(\Gamma_0/, N)^{\Gamma_1/\Gamma_0} \xrightarrow{\mathrm{Trans}} \mathrm{H}^2(\Gamma_1/\Gamma_0, N^{\Gamma_0})$$

qu'il est dans le noyau du morphisme de transgression.

L'exemple donné précédemment, montre que ce n'est pas toujours le cas.

c) *Une conséquence cohomologique.*

La non projectivité du corps $\mathscr{Z}$ équivaut à l'existence d'une extension finie $\mathscr{Z}(\alpha)/\mathscr{Z}$ telle que $\mathrm{Br}(\mathscr{Z}(\alpha)) \neq 0$ (cf [4, Proposition II.3.1.5]). Les corps $\mathscr{K}_n(\alpha)$ sont des extensions de corps projectifs et sont donc projectifs eux-même, ce qui implique en particulier qu'ils vérifient $\mathrm{Br}(\mathscr{K}_n(\alpha)) = 0$. La suite $(\mathscr{K}_n(\alpha))_{n\geq 2}$ vérifie en outre : $\bigcap_{n\geq 2} \mathscr{K}_n(\alpha) = \mathscr{Z}(\alpha)$.

Conséquence. *Il existe un corps k tel que $\mathrm{Br}(k) \neq 0$ et une suite décroissante $(L_n)_{n\geq 1}$ d'extensions algébriques de k telles que $k = \bigcap_{n\geq 1} L_n$ et vérifiant, pour tout $n \geq 1$, $[L_n : L_{n+1}] < +\infty$ et $\mathrm{Br}(L_n) = 0$.*

3. Extensions abéliennes projectives abyssales

Nous venons de classifier les extensions abéliennes projectives minimales de $\mathbb{Q}$. Leurs extensions algébriques restant des corps projectifs, on peut se demander s'il existe d'autres extensions abéliennes projectives de $\mathbb{Q}$, c'est-à-dire des extensions abéliennes projectives de $\mathbb{Q}$ qui ne contiennent en leur sein aucun corps projectif minimal. Ces extensions particulières seront appelées *abyssales*. L'objet de cette partie est de montrer qu'il existe des corps abyssaux et d'en exhiber certains explicitement.

En premier lieu, remarquons que si $\Omega/\mathbb{Q}$ désigne une extension abélienne abyssale alors le corps Ω ne peut contenir le corps $\mathscr{Z}$ comme le montre la proposition 7. Réciproquement, le théorème 6 montre qu'une extension abélienne projective de $\mathbb{Q}$ qui ne contient pas $\mathscr{Z}$ est certainement abyssale. Ainsi, la recherche de corps abyssaux nous incite à considérer des corps ne contenant pas certains corps $\mathscr{Z}_l$ et à leur rajouter un certain nombre de racines p-ièmes de l'unité afin d'assurer que leur l-dimensions cohomologiques reste ≤ 1 pour les premiers l considérés.

Considérons un ensemble de nombres premiers $\mathscr{P}_0 \subset \mathscr{P}$ et notons

$$\ell(\mathscr{P}_0) = \left\{ l \in \mathscr{P} / \ \forall q \in \mathscr{P}, \ \sup_{p\in\mathscr{P}_0} \{v_l(\omega_q(p))\} = +\infty \right\}$$

où $v_l(\omega_q(p))$ désigne la valuation l-adique de l'ordre multiplicatif de p modulo q. On a alors :

Proposition 12. *Si $\mathscr{P}_0 \subset \mathscr{P}$ est une partie non vide et différente du singleton $\{2\}$, alors le corps*

$$K = \mathbb{Q}(\xi_p/\ p \in \mathscr{P}_0) \bullet_{l \notin \ell(\mathscr{P}_0)} \mathscr{Z}_l$$

est projectif.

Preuve. Puisque le corps K contient un ξ_p pour $p \neq 2$, il est totalement imaginaire. Pour tout $l \notin \ell(\mathscr{P}_0)$, on a $\mathscr{Z}_l \subset K$ et donc $\mathrm{cd}_l(K) \leq 1$, d'après le corollaire 4. Si $l \in \ell(\mathscr{P}_0)$ alors puisque pour tout q premier on a $\sup\{v_l(\omega_q(p))/\ p \in \mathscr{P}_0\} = +\infty$, le lemme 5 et le théorème 3 assure que $\mathrm{cd}_l(K) \leq \mathrm{cd}_l(\mathbb{Q}(\xi_p/\ p \in \mathscr{P}_0)) \leq 1$. □

En particulier, si $\mathscr{P}_0 \subset \mathscr{P}$ est tel que $\ell(\mathscr{P}_0) \neq \emptyset$, alors le corps défini dans la proposition 12 est abyssal. Une telle partie $\mathscr{P}_0$ est alors nécessairement infinie.

Théorème 13. *Si $\mathscr{P}_0 \subset \mathscr{P}$ est une partie cofinie alors on a $\ell(\mathscr{P}_0) = \mathscr{P}$. En particulier, pour toute partie cofinie $\mathscr{P}_0 \subset \mathscr{P}$, le corps $\mathbb{Q}(\xi_p/\ p \in \mathscr{P}_0)$ est abyssal.*

Preuve. Une application directe des théorèmes 1 et 2 de [5] montre que pour tout premier l, tout premier q et tout entier r, il existe une constante $C > 0$ telle que

$$\sharp\{p \in \mathscr{P}/\ p \leq x,\ v_l(\omega_p(q)) \geq r\} \simeq C\frac{x}{\log x}$$

En particulier pour l premier fixé, pour tout premier q et tout entier r, il existe une infinité de premiers p tel que $v_l(\omega_p(q)) \geq r$. Puisque $\mathscr{P}_0$ est cofinie, on a $l \in \ell(\mathscr{P}_0)$. □

Comme nous l'avons suggéré dans la remarque 9, le corps $\mathbb{Q}(\xi_p/\ p \in \mathscr{P}_0)$ est une "grosse" extension de $\mathbb{Q}$. En raffinant un peu l'argument, on peut d'un point de vue existentiel passer du cas cofini au cas de la densité relative aussi petite que l'on veut :

Proposition 14. *Pour toute fonction continue strictement croissante $f : [1, +\infty[\longrightarrow \mathbb{R}^+$ telle que $\lim\limits_{x \longrightarrow +\infty} f(x) = +\infty$, il existe une partie $\mathscr{P}_0 \subset \mathscr{P}$ telle que :*

1/ $\forall x \geq 1$, $\sharp\{p \in \mathscr{P}_0, p \leq x\} \leq f(x)$.
2/ $\ell(\mathscr{P}_0) = \mathscr{P}$.

et donc, il existe une partie $\mathscr{P}_0$ vérifiant la condition 1/ et telle que $\mathbb{Q}(\xi_p/\ p \in \mathscr{P}_0)$ soit un corps abyssal.

Preuve. Posons $\mathscr{P} = \{l_1, l_2, \cdots\} = \{q_1, q_2, \cdots\}$ et fixons-nous deux indices $n, m \geq 1$. D'après le théorème 13, $\sup\{v_{l_n}(\omega_{q_m}(p))/\ p \in \mathscr{P}\} = +\infty$. Il existe donc une suite croissante de nombres premiers $(p_k)_k$ telle que $(v_{l_n}(\omega_{q_m}(p_k)))_k$ tende vers $+\infty$. Toute sous-suite de $(p_k)_k$ garde la même propriété.

Si l'on pose $f_{n,m}(x) = \frac{f(x)}{2^{n+m}}$, alors la fonction $f_{n,m}$, en tant que fonction continue strictement croissante, possède une réciproque $f_{n,m}^{-1}$ qui est, elle aussi, une fonction croissante. Considérons alors une suite strictement croissante d'indices $(\varphi(k))_k$ telle que, pour tout $k \geq 1$ on ait $\varphi(k) \geq [f_{n,m}^{-1}(k)]+1$ et considérons la partie $A_{n,m} = \{p_{\varphi(k)}/\ k \geq 1\}$. Comme pour tout k, $p_{\varphi(k)} \geq \varphi(k)$ alors pour tout $x \geq 0$, on a

$$\sharp\{p \in A_{n,m}, p \leq x\} \leq \max\{k/\ \varphi(k) \leq x\} \leq f_{n,m}(x) = \frac{f(x)}{2^{n+m}}$$

puisque $\varphi(k) \leq x \Longrightarrow f_{n,m}^{-1}(k) \leq x \Longrightarrow k \leq f_{n,m}(x)$.

La partie $A_{n,m}$ vérifie $\sup\{v_{l_n}(\omega_{q_m}(p))/\ p \in A_{n,m}\} = +\infty$, si bien que, si l'on pose $\mathscr{P}_0 = \bigcup_{n,m} A_{n,m}$, alors $\mathscr{P}_0$ vérifie la condition 2/ de l'énoncé. Par ailleurs, pour tout $x \geq 1$, on a

$$\sharp\{p \in \mathscr{P}_0, p \leq x\} \leq \sum_{n,m \geq 1} \sharp\{p \in A_{n,m}, p \leq x\} \leq f(x) \sum_{n,m \geq 1} \frac{1}{2^{n+m}} = f(x)$$

ce qui achève la preuve. □

Références

[1] P. Dèbes, B. Deschamps, The regular inverse Galois problem over large fields, in : Geometric Galois Actions. 2. The Inverse Galois Problem, Moduli Spaces and Mapping Class Groups, in : Lond. Math. Soc. Lect. Note Ser., vol. 243, Cambridge University Press, 1997, pp. 119–138.
[2] P. Dèbes, B. Deschamps, Corps Ψ-libres et théorie inverse de Galois infinie, J. Reine Angew. Math. 574 (2004) 197–218.
[3] M. Fried, M. Jarden, Field Arithmetic, third edition, Ergeb. der Math. 3. Folge, vol. 11, Springer, 2008.
[4] J.-P. Serre, Cohomologie galoisienne, 5, cinquième édition, Lecture Notes in Math., Springer-Verlag, 1994.
[5] K. Wiertelak, On the density of some sets of primes, I, Acta Arith. 34 (1978) 183–196.