

JOURNAL

de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Georges GRAS

On the structure of the Galois group of the Abelian closure of a number field

Tome 26, n° 3 (2014), p. 635-654.

http://jtnb.cedram.org/item?id=JTNB_2014__26_3_635_0

© Société Arithmétique de Bordeaux, 2014, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://jtnb.cedram.org/legal/>). Toute reproduction en tout ou partie de cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

On the structure of the Galois group of the Abelian closure of a number field

par GEORGES GRAS

RÉSUMÉ. A partir d'un article de A. Angelakis et P. Stevenhagen sur la détermination d'une famille de corps quadratiques imaginaires K ayant des groupes de Galois Abéliens absolus A_K isomorphes, nous étudions une telle question pour les corps de nombres K quelconques. Nous montrons que ce type de propriété n'est probablement pas facilement généralisable, en dehors des corps quadratiques imaginaires, en raison d'obstructions p -adiques provenant des unités globales de K . En se restreignant aux p -sous-groupes de Sylow de A_K et en admettant la conjecture de Leopoldt nous montrons que l'étude correspondante est liée à une généralisation de la notion classique de corps p -rationnel que nous approfondissons, y compris au point de vue numérique pour les corps quadratiques.

Cependant nous obtenons (Théorèmes 2.1 et 3.1) des informations non triviales sur la structure de A_K , pour tout corps de nombres K , par application de résultats de notre livre sur la théorie p -adique du corps de classes global.

ABSTRACT. From a paper by A. Angelakis and P. Stevenhagen on the determination of a family of imaginary quadratic fields K having isomorphic absolute Abelian Galois groups A_K , we study any such issue for arbitrary number fields K . We show that this kind of property is probably not easily generalizable, apart from imaginary quadratic fields, because of some p -adic obstructions coming from the global units of K . By restriction to the p -Sylow subgroups of A_K and assuming the Leopoldt conjecture we show that the corresponding study is related to a generalization of the classical notion of p -rational field that we deepen, including numerical viewpoint for quadratic fields.

However we obtain (Theorems 2.1 and 3.1) non-trivial information about the structure of A_K , for any number field K , by application of results of our book on the p -adic global class field theory.

Manuscrit reçu le 25 mars 2013, révisé le 28 novembre 2013, accepté le 3 décembre 2013.

Mots clefs. Class field theory; Abelian closures of number fields; p -ramification; p -rational fields; Abelian profinite groups; Group extensions.

Classification math. 11R37, 11R29, 20K35.

1. Introduction – Notation

Let K be a number field of signature (r_1, r_2) , so that $r_1 + 2r_2 = [K : \mathbb{Q}]$, and let A_K be the Galois group $\text{Gal}(K^{\text{ab}}/K)$ where K^{ab} is the maximal Abelian pro-extension of K .

1.1. Statement of the problem. The question that was asked was the following: in what circumstances the groups A_{K_1} and A_{K_2} are isomorphic profinite groups when K_1 and K_2 are two non-conjugate number fields ?

A first paper on this subject was published in [15] by M. Onabe from the work of T. Kubota [12] using the difficult approach with Ulm invariants. In [1], using class field theory, A. Angelakis and P. Stevenhagen show that $A_K \simeq \widehat{\mathbb{Z}}^2 \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$ for a specific family of imaginary quadratic fields, conjecturally infinite. In this paper we prove that for any number field K (under the Leopoldt conjecture for all primes), A_K contains a subgroup isomorphic to

$$\widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathbf{w}n\mathbb{Z} \right),$$

where $\delta = 1$ if K contains $\sqrt{\pm 2}$ but not $\sqrt{-1}$, $\delta = 0$ otherwise, and where $\mathbf{w} = \prod_{p \text{ prime}} \mathbf{w}_p$ is an integer whose local factors \mathbf{w}_p depend simply on the intersections $K \cap \mathbb{Q}(\mu_{p^\infty})$ (see Definition 2.3); then we give a class field theory interpretation of the quotient of A_K by this subgroup, by showing that this quotient is isomorphic to $\prod_p \mathcal{T}_p$ where each p -group \mathcal{T}_p is finite and measures the defect of p -rationality of K (see Definition 2.1).

Such isomorphisms about A_K are only (non-unique) isomorphisms of Abelian profinite groups for which Galois theory and, a fortiori, description of arithmetical objects (e.g. decomposition and inertia groups) are not effective. When an isomorphism is canonical (essentially if it is induced by the reciprocity map of class field theory), we shall write $\overset{\text{can}}{\simeq}$ contrary to the non-canonical case denoted $\overset{\text{nc}}{\simeq}$ if necessary.

1.2. Local notation. Let p be a prime number. In a general setting, the notation $G_{(p)}$ (resp. $L_{(p)}$) refers to the p -Sylow subgroup of an Abelian profinite Galois group G (resp. the maximal p -subextension of an Abelian extension L), over K , and O_p refers to any other object depending on p . Let

$$H_{(p)}, H_{(p)}^{\text{pra}}, H_{(p)}^{\text{ta}}, \widehat{K}_{(p)},$$

be the p -Hilbert class field in ordinary sense¹, the maximal p -ramified (i.e., unramified outside p) Abelian pro- p -extension of K in ordinary sense, the

¹Maximal Abelian p -extension of K , unramified at finite places, in which (when $p = 2$) the finite real places do not complexify (= do not “ramify”).

maximal tamely ramified Abelian pro- p -extension of K in restricted sense², the compositum of the \mathbb{Z}_p -extensions of K , respectively.

Since we shall assume that the Leopoldt conjecture is satisfied in K for all p , the notation $\widehat{K}_{(p)}$ makes sense if we define \widehat{K} as the maximal $\widehat{\mathbb{Z}}$ -extension of K , for which we have by assumption $\text{Gal}(\widehat{K}/K) \simeq \widehat{\mathbb{Z}}^{r_2+1}$, with $\text{Gal}(\widehat{K}_{(p)}/K) \simeq \mathbb{Z}_p^{r_2+1}$ since $\widehat{\mathbb{Z}}_{(p)} \simeq \mathbb{Z}_p$ for all p .

Then let

$$\mathcal{T}_p := \text{Gal}(H_{(p)}^{\text{pra}}/\widehat{K}_{(p)}) \quad \text{and} \quad \mathcal{C}_{(p)} := \text{Gal}(H_{(p)}/K) ,$$

$\mathcal{C}_{(p)}$ being canonically isomorphic to the p -class group of K in ordinary sense. Note that a priori \mathcal{T}_p is not the localisation of a known arithmetical invariant similar as a class group. For some recalls about the finite group \mathcal{T}_p , see §3.4.

For any finite place v of K , we denote by K_v the completion³ of K at v , then by

$$U_v := \{u \in K_v, |u|_v = 1\} \quad \text{and} \quad U_v^1 := \{u \in U_v, |u - 1|_v < 1\},$$

the unit group and principal unit group of K_v , respectively. So, U_v/U_v^1 is isomorphic to the multiplicative group of the residue field F_v of K at v . We shall denote by ℓ the characteristic of F_v ; then U_v^1 is a \mathbb{Z}_ℓ -module.

If v is a real infinite place, we put $K_v = \mathbb{R}$, $U_v = \mathbb{R}^\times$, $U_v^1 = \mathbb{R}^{\times+}$, hence $F_v^\times = \{\pm 1\}$, according to [5], I.3.1.2.

Denote by $\mu(k)$ (resp. $\mu_p(k)$) the group of roots of unity (resp. the group of roots of unity of p -power order) of any field k .

It is well known (using Hensel lemma) that, for a finite place v , we have $\mu(K_v) \simeq F_v^\times \times \mu_v^1$, where μ_v^1 is the torsion subgroup of the \mathbb{Z}_ℓ -module U_v^1 ; thus μ_v^1 is a finite ℓ -group.

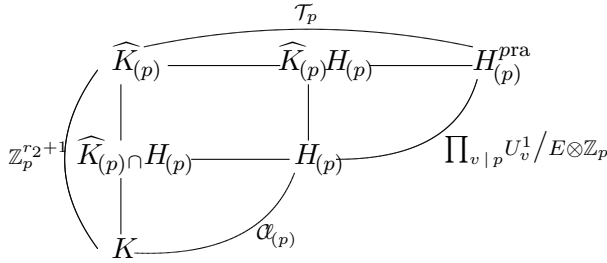
So $\mu_p(K_v) \simeq F_{v,(p)}^\times$ if and only if $v \nmid p$ and $\mu_p(K_v) = \mu_v^1$ if and only if $v|p$.

If v is a real infinite place, we then have $\mu(K_v) \simeq F_v^\times$, hence $\mu_v^1 = 1$.

With the above definitions, the structure of $\text{Gal}(H_{(p)}^{\text{pra}}/K)$ is summarized by the following diagram, from [5], III.2.6.1, Fig. 2.2, under the Leopoldt conjecture for p in K , where E is the group of global units of K and where $E \otimes \mathbb{Z}_p$ is diagonally embedded in $\prod_{v|p} U_v^1$ from the obvious map (injective under the Leopoldt conjecture) $i_p := (i_v)_v|_p$:

² i.e., the real infinite places may be complexified (= “ramified”) in $H_{(2)}^{\text{ta}}$.

³ As in [5], I, §2, we consider that $K_v = i_v(K) \mathbb{Q}_\ell \subset \mathbb{C}_\ell$ for a suitable embedding i_v of K in \mathbb{C}_ℓ (i_v is defined up to the \mathbb{Q}_ℓ -isomorphisms of K_v in \mathbb{C}_ℓ), where ℓ is the residue characteristic.



1.3. Some p -adic logarithms. To characterize the notion of p -rationality in a computational point of view (see Definition 2.1 and Remark 2.1), we shall make use of suitable p -adic logarithms as follows ([5], III.2.2):

(i) We consider the p -adic logarithm $\log_p : K^\times \rightarrow \prod_{v|p} K_v$ defined by $\log_p = \log \circ i_p$ on K^\times , where $\log : \mathbb{C}_p^\times \rightarrow \mathbb{C}_p$ is the Iwasawa extension of the usual p -adic logarithm.

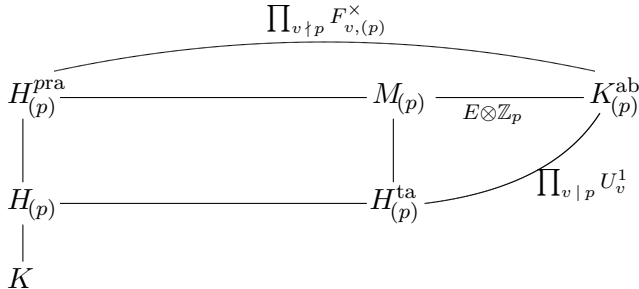
(ii) We then define the \mathbb{Q}_p -vector space $\mathcal{L}_p := \prod_{v|p} K_v / \mathbb{Q}_p \log_p(E)$. We have $\dim_{\mathbb{Q}_p}(\mathcal{L}_p) = r_2 + 1$ under the Leopoldt conjecture for p in K .

(iii) Finally, we denote by Log_p the map, from the group I_p of ideals of K prime to p , to \mathcal{L}_p , sending $\mathfrak{a} \in I_p$ to $\text{Log}_p(\mathfrak{a})$ defined as follows: let $m \neq 0$ be such that $\mathfrak{a}^m = (\alpha)$, $\alpha \in K^\times$; we set $\text{Log}_p(\mathfrak{a}) := \frac{1}{m} \log_p(\alpha) + \mathbb{Q}_p \log_p(E)$. This does not depend on the choices of m and α .

2. Structure of $A_K := \text{Gal}(K^{ab}/K)$

2.1. Class field theory – Fundamental diagram – p -rationality.

Let p be a prime number and let $K_{(p)}^{ab} \subset K^{ab}$ be the maximal Abelian pro- p -extension of K . From [9], § 2.7, we have given in [5], III.4.4.1, III.4.4.5 (assuming the Leopoldt conjecture for p in K) the following diagram for the structure of $\text{Gal}(K_{(p)}^{ab}/K)$ isomorphic to the p -Sylow subgroup of A_K :



where $F_{v,(p)}^\times$ is the p -Sylow subgroup of the multiplicative group of the residue field F_v of K at v , including real infinite places for which $F_v^\times = \{\pm 1\}$; $M_{(p)}$ is the direct compositum, over $H_{(p)}$, of $H_{(p)}^{pra}$ and $H_{(p)}^{ta}$.

Note that $\text{Gal}(K_{(p)}^{\text{ab}}/H_{(p)}^{\text{pra}}) \stackrel{\text{can}}{\simeq} \prod_{v \nmid p} F_{v,(p)}^\times$ is equivalent to the Leopoldt conjecture ([5], III.4.4.5.2). The diagonal embeddings $i_{\text{ta}} := (i_v)_{v \nmid p}$ and $i_p := (i_v)_{v | p}$ of $E \otimes \mathbb{Z}_p$ in $\prod_{v \nmid p} F_{v,(p)}^\times$ and $\prod_{v | p} U_v^1$, respectively, are injective (under the Leopoldt conjecture for i_p). Each $F_{v,(p)}^\times$ (for $v \nmid p$ finite or v real infinite) or U_v^1 (for $v | p$) is canonically isomorphic to the inertia group of v in $K_{(p)}^{\text{ab}}/K$.

Let $\mathcal{U}_{(p)} \simeq \prod_{v \nmid p} F_{v,(p)}^\times \times \prod_{v | p} U_v^1$ be the p -Sylow subgroup of the group of unit idèles $\mathcal{U} := \prod_v U_v$, and let ρ be the reciprocity map on $\mathcal{U}_{(p)}$. The kernel of ρ is $i(E \otimes \mathbb{Z}_p)$, where $i = (i_{\text{ta}}, i_p)$. This yields the isomorphisms:

- $\text{Gal}(K_{(p)}^{\text{ab}}/H_{(p)}) \stackrel{\text{can}}{\simeq} \mathcal{U}_{(p)}/i(E \otimes \mathbb{Z}_p)$,
- $\text{Gal}(K_{(p)}^{\text{ab}}/H_{(p)}^{\text{pra}}) = \rho\left(\prod_{v \nmid p} F_{v,(p)}^\times \times \{1\}\right) \stackrel{\text{can}}{\simeq} \prod_{v \nmid p} F_{v,(p)}^\times$,
 since $\left(\prod_{v \nmid p} F_{v,(p)}^\times \times \{1\}\right) \cap i(E \otimes \mathbb{Z}_p) = 1$,
- $\text{Gal}(K_{(p)}^{\text{ab}}/H_{(p)}^{\text{ta}}) = \rho\left(\{1\} \times \prod_{v | p} U_v^1\right) \stackrel{\text{can}}{\simeq} \prod_{v | p} U_v^1$ in the same way as above.

Definition 2.1. The number field K is said to be p -rational (see e.g. [13], [4], [10], [5], IV.3.4.4) if it satisfies the Leopoldt conjecture for p and if $\mathcal{T}_p = 1$.

Remark 2.1. Assuming the Leopoldt conjecture for p in K , we have:

(i) The p -rationality of K is equivalent to the following three conditions (from [5], IV.3.4.5 and III.2.6.1 (i)):

(i₁) $\prod_{v|p} \mu_p(K_v) = i_p(\mu_p(K))$.

(i₂) the p -Hilbert class field $H_{(p)}$ is contained in the compositum $\widehat{K}_{(p)}$ of the \mathbb{Z}_p -extensions of K , which is equivalent (refer to § 1.3), to $|\mathcal{C}_{(p)}| = \left(\mathbb{Z}_p \text{Log}_p(I_p) : \prod_{v|p} \log(U_v^1) + \mathbb{Q}_p \log_p(E)\right)$,

(i₃) $\mathbb{Z}_p \log_p(E)$ is a direct factor in the \mathbb{Z}_p -module $\prod_{v|p} \log(U_v^1)$, which expresses the “minimality” of the valuation of the p -adic regulator.

(ii) If K is p -rational, we have an isomorphism of the form

$$\text{Gal}(K_{(p)}^{\text{ab}}/K) \simeq \mathbb{Z}_p^{r_2+1} \times \prod_{v \nmid p} F_{v,(p)}^\times, \text{ in which } \text{Gal}(K_{(p)}^{\text{ab}}/\widehat{K}_{(p)}) \stackrel{\text{can}}{\simeq} \prod_{v \nmid p} F_{v,(p)}^\times.$$

(iii) Let \widehat{K} be the compositum, over p , of the $\widehat{K}_{(p)}$. By assumption (Leopoldt conjecture for all p), \widehat{K} is the maximal $\widehat{\mathbb{Z}}$ -extension of K for which $\text{Gal}(\widehat{K}/K) \simeq \widehat{\mathbb{Z}}^{r_2+1}$. A sufficient condition to get an isomorphism of the form $A_K \simeq \widehat{\mathbb{Z}}^{r_2+1} \times \prod_v F_v^\times$ is that K be p -rational for all p , i.e., $\prod_p \mathcal{T}_p = 1$.

2.2. Structure of $\prod_v F_v^\times$. Let $(F_v)_v$ be the family of residue fields of K at its finite or real infinite places v . We intend to give, for all p , the structure of the p -Sylow subgroup $\prod_v F_{v,(p)}^\times$ of $\prod_v F_v^\times$. If $v \nmid p$, then $F_{v,(p)}^\times = 1$; so we can restrict ourselves to $\prod_{v \nmid p} F_{v,(p)}^\times$. We shall prove (in Proposition 2.1) that there exist integers $\delta \in \{0, 1\}$ and $\mathbf{w} \geq 1$ such that

$$\prod_{v \nmid p} F_{v,(p)}^\times \stackrel{\text{nc}}{\simeq} \prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathbf{w}n\mathbb{Z} \right)_{(p)}, \text{ for all } p.$$

The property giving such an isomorphism is that for any given p -power p^m , $m \geq 1$, these two pro- p -groups (which are, by nature, explicit direct products of cyclic groups) have the “same number” of direct cyclic factors of order p^m in these writings (finite number or countable infinite number). It is obvious that for any p and any fixed $m \geq 1$, $\prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathbf{w}n\mathbb{Z} \right)_{(p)}$ has 0 or infinitely many direct cyclic factors of order p^m . More precisely, by the decomposition $\mathbb{N} \setminus \{0\} = \bigcup_{k \geq 0} p^k(\mathbb{N} \setminus p\mathbb{N})$ (with disjoint sets), we have

$$\left(\prod_{n \geq 1} \mathbb{Z}/\mathbf{w}n\mathbb{Z} \right)_{(p)} \simeq \prod_{k \geq 0} \left(\mathbb{Z}/\mathbf{w}_p p^k \mathbb{Z} \right)^{\mathbb{N} \setminus p\mathbb{N}}, \text{ where } \mathbf{w}_p \text{ is the } p\text{-part of } \mathbf{w}.$$

Remark 2.2. (i) The right hand side of this isomorphism shows that the isomorphy class of the group is the same for $\mathbf{w}_p = p$ and for $\mathbf{w}_p = 1$ and is uniquely determined by \mathbf{w}_p as soon as this number is taken different from p . By globalization, the isomorphy class of $\prod_{n \geq 1} \mathbb{Z}/\mathbf{w}n\mathbb{Z}$ is uniquely determined by \mathbf{w} as soon as this number has no “simple factor” (i.e., $\mathbf{w} = \prod_p \mathbf{w}_p$ with $\mathbf{w}_p \neq p$ for all p). Then in the sequel we can ensure that \mathbf{w} will be defined in such a way. In this manner, \mathbf{w} is unique.

(ii) In $\left(\prod_{n \geq 1} \mathbb{Z}/\mathbf{w}n\mathbb{Z} \right)_{(p)} \simeq \prod_{k \geq 0} \left(\mathbb{Z}/\mathbf{w}_p p^k \mathbb{Z} \right)^{\mathbb{N} \setminus p\mathbb{N}} \simeq \prod_{k \geq 0} \left(\mathbb{Z}/\mathbf{w}_p p^k \mathbb{Z} \right)^\mathbb{N}$, it is not difficult to see that there are no direct cyclic factors of order p^m , $m \geq 1$, if and only if $p^{m+1} | \mathbf{w}_p$.

Definition 2.2. For any $e \geq 2$ denote by μ_e the group of e th roots of unity in an algebraic closure of any field of characteristic 0 or $\ell \nmid e$.

(i) Let Q_{p^ν} , $\nu \geq 1$, be for any p the unique subfield of degree p^ν of the cyclotomic \mathbb{Z}_p -extension of \mathbb{Q} . Let Q'_{2^ν} , $\nu \geq 1$, be the non-real cyclic subfield of $\mathbb{Q}(\mu_{2^\infty})$ of degree 2^ν such that $Q'_{2^\nu} \mathbb{Q}(\mu_4) = \mathbb{Q}(\mu_{4 \cdot 2^\nu})$; in particular, $Q_2 = \mathbb{Q}(\sqrt{2})$ and $Q'_2 = \mathbb{Q}(\sqrt{-2})$. We put $Q_{2^0} = Q'_{2^0} = \mathbb{Q}$.

(ii) Let $\nu_p(K) =: \nu$ be the integer defined as follows:

- for $p \neq 2$, ν is the maximal integer such that $Q_{p^\nu} \subseteq K$;
- for $p = 2$, $K \cap \mathbb{Q}(\mu_{2^\infty}) \in \{Q_{2^\nu}, Q'_{2^\nu}, \mathbb{Q}(\mu_{4 \cdot 2^\nu})\}$, which defines $\nu \geq 0$.

Since $Q_{p^\nu}\mathbb{Q}(\mu_p) = \mathbb{Q}(\mu_{p^{\nu+1}})$ ($p \neq 2$) and $Q'_{2^\nu}\mathbb{Q}(\mu_4) = Q_{2^\nu}\mathbb{Q}(\mu_4) = \mathbb{Q}(\mu_{4 \cdot 2^\nu})$, the field $K(\mu_p)$ (resp. $K(\mu_4)$) contains $\mu_{p^{\nu+1}}$ (resp. $\mu_{4 \cdot 2^\nu}$) if $p \neq 2$ (resp. $p = 2$) and no more roots of unity of p -power order.

2.2.1. Analysis of the case $p \neq 2$. In the study of the product $\prod_{v \nmid p} F_{v,(p)}^\times$, we can restrict the index $v \nmid p$ to the places (infinite in number) such that $|F_v^\times| \equiv 0 \pmod{p}$ (i.e., splitting of v in $K(\mu_p)/K$, which includes the case where K contains μ_p).

a) If K contains μ_p , then $\mu_p(K) = \mu_{p^{\nu+1}}$ and necessarily $|F_v^\times| \equiv 0 \pmod{p^{\nu+1}}$ for all the places $v \nmid p$. We obtain the following tower of extensions (where \subset means a strict inclusion)

$$K = K(\mu_{p^{\nu+1}}) \subset K(\mu_{p^{\nu+2}}) \subset \dots$$

From Chebotarev's theorem (see e.g. [14], Ch. 7, § 3), for any $m \geq \nu + 1$ there exist infinitely many places v of K whose inertia group in $K(\mu_{p^{m+1}})/K$ is the subgroup $\text{Gal}(K(\mu_{p^{m+1}})/K(\mu_{p^m}))$, which is cyclic of order p ; so we get $|F_v^\times| \equiv 0 \pmod{p^m}$ and $|F_v^\times| \not\equiv 0 \pmod{p^{m+1}}$ for these places.

b) If K does not contain μ_p , we have the tower of extensions

$$K \subset K(\mu_p) = \dots = K(\mu_{p^{\nu+1}}) \subset K(\mu_{p^{\nu+2}}) \subset \dots$$

For any $m \geq \nu + 1$ there exist infinitely many places v whose inertia group in $K(\mu_{p^{m+1}})/K$ is the subgroup $\text{Gal}(K(\mu_{p^{m+1}})/K(\mu_{p^m}))$, cyclic of order p ; thus, $|F_v^\times| \equiv 0 \pmod{p^m}$ and $|F_v^\times| \not\equiv 0 \pmod{p^{m+1}}$ for these places, split in $K(\mu_p)/K$ as required (otherwise $|F_v^\times|$ is prime to p).

Whatever the assumption on the intersection $K \cap \mathbb{Q}(\mu_p)$, the case $p \neq 2$ leads to identical results from the knowledge of ν .

2.2.2. Analysis of the case $p = 2$. In that case, we always have $|F_v^\times| \equiv 0 \pmod{2}$ in the study of $\prod_{v \nmid 2} F_{v,(2)}^\times$ (v finite or real infinite).

a) If K contains μ_4 , hence $\mu_{4 \cdot 2^\nu}$, we have $|F_v^\times| \equiv 0 \pmod{4 \cdot 2^\nu}$ for all odd places, and the tower of extensions

$$K = K(\mu_{4 \cdot 2^\nu}) \subset K(\mu_{4 \cdot 2^{\nu+1}}) \subset \dots$$

From Chebotarev's theorem, for any $m \geq \nu$ there exist infinitely many places v whose inertia group in $K(\mu_{4 \cdot 2^{m+1}})/K$ is $\text{Gal}(K(\mu_{4 \cdot 2^{m+1}})/K(\mu_{4 \cdot 2^m}))$, cyclic of order 2; so $|F_v^\times| \equiv 0 \pmod{4 \cdot 2^m}$ and $|F_v^\times| \not\equiv 0 \pmod{4 \cdot 2^{m+1}}$ for these places.

b) If K does not contain μ_4 , we have two possible towers depending on the intersection $K \cap \mathbb{Q}(\mu_{2^\infty})$:

$$\begin{aligned} K \cap \mathbb{Q}(\mu_{2^\infty}) = \mathbb{Q} \ (\nu = 0) : & \quad K \subset K(\mu_4) \subset K(\mu_8) \subset \dots \\ K \cap \mathbb{Q}(\mu_{2^\infty}) \in \{Q_{2^\nu}, Q'_{2^\nu}\}, \ \nu \geq 1 : & \quad K \subset K(\mu_4) = K(\mu_8) = \dots \\ & \quad = K(\mu_{4 \cdot 2^\nu}) \subset K(\mu_{4 \cdot 2^{\nu+1}}) \subset \dots \end{aligned}$$

(i) In the first case ($\nu = 0$), for any $m \geq 1$ Chebotarev's theorem gives infinitely many places v whose inertia group in $K(\mu_{2^{m+1}})/K$ is the subgroup $\text{Gal}(K(\mu_{2^{m+1}})/K(\mu_{2^m}))$, cyclic of order 2; so $|F_v^\times| \equiv 0 \pmod{2^m}$ and $|F_v^\times| \not\equiv 0 \pmod{2^{m+1}}$ for these places. So, in this case we obtain an isomorphism of the form

$$\prod_{v \nmid 2} F_{v,(2)}^\times \simeq \prod_{m \geq 1} (\mathbb{Z}/2^m \mathbb{Z})^\mathbb{N}.$$

(ii) In the second case ($\nu \geq 1$), we will have two infinite disjoint sets of places $v \nmid 2$ of K for the structure of the product $\prod_{v \nmid 2} F_{v,(2)}^\times$:

– There exist infinitely many places v inert in $K(\mu_4)/K$. Then $|F_v^\times| \equiv 0 \pmod{2}$ and $|F_v^\times| \not\equiv 0 \pmod{4}$ for these places.

– For any $m \geq \nu$, there exist infinitely many places v whose inertia group in $K(\mu_{4 \cdot 2^{m+1}})/K$ is the subgroup $\text{Gal}(K(\mu_{4 \cdot 2^{m+1}})/K(\mu_{4 \cdot 2^m}))$, cyclic of order 2; a fortiori, these places are split in $K(\mu_4)/K$ and even in $K(\mu_8)/K$. So we get $|F_v^\times| \equiv 0 \pmod{4 \cdot 2^m}$ and $|F_v^\times| \not\equiv 0 \pmod{4 \cdot 2^{m+1}}$.

In the exceptional case $K \cap \mathbb{Q}(\mu_{2^\infty}) \in \{Q_{2^\nu}, Q'_{2^\nu}\}$, $\nu \geq 1$, we have a group isomorphism of the form

$$\prod_{v \nmid 2} F_{v,(2)}^\times \simeq (\mathbb{Z}/2 \mathbb{Z})^\mathbb{N} \times \prod_{m \geq \nu} (\mathbb{Z}/4 \cdot 2^m \mathbb{Z})^\mathbb{N}.$$

Definition 2.3. From the above discussion, we can define, in a unique way, the integers $\delta \in \{0, 1\}$ and $\mathbf{w} := \prod_p \mathbf{w}_p$, where \mathbf{w}_p depending on $\nu := \nu_p(K)$ (see Definition 2.2 (i), (ii)) is given as follows:

(i) Case $p \neq 2$. We know that $\mu_{p^{\nu+1}}$ is the maximal group of roots of unity of p -power order contained in $K(\mu_p)$, whether K contains μ_p or not; we put $\mathbf{w}_p = p^{\nu+1}$ if $\nu \geq 1$ and $\mathbf{w}_p = 1$ otherwise (from the use of Remark 2.2 (i)).

(ii) Case $p = 2$ and K contains μ_4 . Hence $\mu_{4 \cdot 2^\nu}$ is the maximal group of roots of unity of 2-power order contained in K ; we put $\mathbf{w}_2 = 4 \cdot 2^\nu$, $\nu \geq 0$.

(iii) Case $p = 2$ and K does not contain μ_4 . Thus $\mu_{4 \cdot 2^\nu}$ is the maximal group of roots of unity of 2-power order contained in $K(\mu_4)$; we put $\mathbf{w}_2 = 4 \cdot 2^\nu$ if $\nu \geq 1$ and $\mathbf{w}_2 = 1$ otherwise (from the use of Remark 2.2 (i)).

(iv) We put $\delta = 1$ in the case (iii) when $\nu \geq 1$, and $\delta = 0$ otherwise.

We can state the following result similar to that of [1], Lem. 3.2.

Proposition 2.1. *Let K be a number field. We have a group isomorphism of the form $\prod_v F_v^\times \stackrel{\text{nc}}{\simeq} \prod_{n \geq 1} ((\mathbb{Z}/2 \mathbb{Z})^\delta \times \mathbb{Z}/\mathbf{w} n \mathbb{Z})$ (see Definition 2.3).*

We have $\delta = 1$ if and only if K contains $\sqrt{\pm 2}$ but not $\sqrt{-1}$, $\delta = 0$ otherwise. If $\delta = 1$, then $\mathbf{w} \equiv 0 \pmod{8}$. If $\mathbf{w} = 1$, then $\prod_v F_v^\times \stackrel{\text{nc}}{\simeq} \prod_{n \geq 1} \mathbb{Z}/n \mathbb{Z}$.

Examples 2.1. (i) *Examples with $p = 3$.* Let K be the maximal real subfield of $\mathbb{Q}(\mu_9)$; we have $\mathbf{w} = 9$ since $K = \mathbb{Q}_3$. The prime $\ell = 5$ is totally inert in $\mathbb{Q}(\mu_9)$ (hence in K); then for $v \mid \ell$, F_v does not contain μ_3 since $\ell^3 = 125 \not\equiv 1 \pmod{3}$. But for $\ell = 7$, inert in K and split in $\mathbb{Q}(\mu_3)$, we get $F_v = \mathbb{F}_{343}$ which contains μ_9 as expected.

Note that for $K = \mathbb{Q}(\mu_3)$, we have $\mathbf{w} = 1$.

(ii) *Examples with $p = 2$.* For $K = \mathbb{Q}(\sqrt{2})$, we have $\delta = 1$ and $\mathbf{w} = 8$. The prime $\ell = 7$ splits in K and is inert in $\mathbb{Q}(\mu_4)$; so for $v \mid \ell$, $F_v = \mathbb{F}_7$ does not contain μ_4 . But for the prime $\ell = 5 \equiv 1 \pmod{4}$, inert in K and split in $\mathbb{Q}(\mu_4)$, we get $F_v = \mathbb{F}_{25}$ which contains μ_8 .

In conclusion, for $K = \mathbb{Q}(\sqrt{2})$, we get the extra direct factor $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ and there is no direct cyclic factor of order 4 in $\text{Gal}(K_{(2)}^{\text{ab}}/\widehat{K}_{(2)})$ (see Remark 2.2 (ii)).

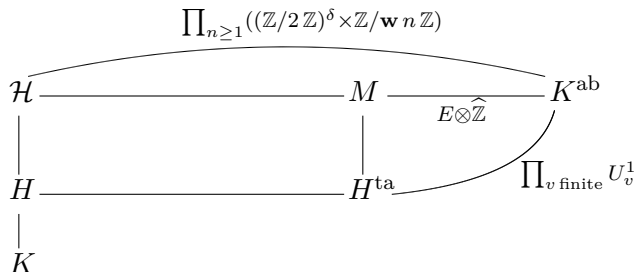
For $K = \mathbb{Q}(\mu_4)$, we have $\delta = 0$, $\mathbf{w} = 4$, and $F_v = \mathbb{F}_\ell$ (resp. $F_v = \mathbb{F}_{\ell^2}$) if $\ell \equiv 1 \pmod{4}$ (resp. $\ell \equiv -1 \pmod{4}$).

2.3. Consequences for the structure of \mathbf{A}_K . From Proposition 2.1 and the fundamental diagram (see §2.1), we can state, under the Leopoldt conjecture in K for all p :

Proposition 2.2. *Let \mathcal{H} be the compositum, over p , of the fields $H_{(p)}^{\text{pra}}$ (maximal p -ramified Abelian pro- p -extensions of K).⁴ We have a group isomorphism of the form $\text{Gal}(K^{\text{ab}}/\mathcal{H}) \stackrel{\text{nc}}{\simeq} \prod_{n \geq 1} ((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathbf{w}n\mathbb{Z})$.*

If $\mathbf{w} = 1$, then $\text{Gal}(K^{\text{ab}}/\mathcal{H}) \stackrel{\text{nc}}{\simeq} \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$.

We have obtained the following globalized diagram (under the Leopoldt conjecture for all p), where H^{ta} (compositum of the $H_{(p)}^{\text{ta}}$) is the maximal Abelian tamely ramified extension of K and $M = \mathcal{H}H^{\text{ta}}$ (direct compositum over the Hilbert class field H):



⁴A specific notation, for the compositum of the $H_{(p)}^{\text{pra}}$, is necessary to avoid confusions with H or with H^{pra} which depends on p . The extension H^{pra} does exist as pro-extension p -ramified and $H_{(p)}^{\text{pra}} = (H^{\text{pra}})_{(p)}$ as usual, but $H_{(p)}^{\text{pra}}$ depends on p with two different meanings.

Let $L_K =: L$ be the compositum, over p , of some finite extensions $L_{(p)}$ of K such that $H_{(p)}^{pra} = \widehat{K}_{(p)} L_{(p)}$ for each p (direct compositum over K , so that $\text{Gal}(L_{(p)}/K) \simeq \mathcal{T}_p$; see the diagram in § 1.2). Then $\text{Gal}(L/K) \simeq \prod_p \mathcal{T}_p$ and $\mathcal{H} = \widehat{K} L$ with $\text{Gal}(\mathcal{H}/K) \simeq \widehat{\mathbb{Z}}^{r_2+1} \times \prod_p \mathcal{T}_p$.

The Galois group $\text{Gal}(L/K)$ measures the defect of p -rationalities (for all p) which expresses a mysterious degree of complexity of A_K .

When they are non-trivial, the extensions $L_{(p)}/K$ are non-unique p -ramified p -extensions; numerical calculations of some of these exceptional extensions $L_{(p)}$ can be interesting, especially for totally real number fields K since in that case the finite subextensions of $\widehat{K}_{(p)}$ are cyclic and well known. For K totally real, $p = 2$, $\sqrt{2} \notin K$, $|\mathcal{T}_2| = 2$, then $L_{(2)} = K(\sqrt{\theta})$ for a suitable totally positive 2-unit θ defined up to multiplication by 2. For $K = \mathbb{Q}(\sqrt{17})$ one has $|\mathcal{T}_2| = 2$ (see § 3.3.2), the group of 2-units is $\langle -1, 2, 4 + \sqrt{17}, \frac{1}{2}(5 + \sqrt{17}) \rangle$; so $L_{(2)} = K\left(\sqrt{\frac{1}{2}(5 \pm \sqrt{17})}\right)$.

We can state, from Proposition 2.2, still assuming the Leopoldt conjecture in K for all p :

Theorem 2.1. *Let K be a number field and let K^{ab} be the maximal Abelian pro-extension of K . Let \mathcal{H} be the compositum, over p , of the maximal p -ramified Abelian pro- p -extensions $H_{(p)}^{pra}$ of K .*

Then there exists an Abelian extension L_K of K such that \mathcal{H} is the direct compositum over K of L_K and the maximal $\widehat{\mathbb{Z}}$ -extension \widehat{K} of K , and such that we have a group isomorphism of the form (see Definition 2.3)

$$\text{Gal}(K^{\text{ab}}/L_K) \stackrel{\text{nc}}{\simeq} \widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathfrak{w}n\mathbb{Z} \right),$$

with $\text{Gal}(K^{\text{ab}}/\mathcal{H}) \stackrel{\text{nc}}{\simeq} \prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathfrak{w}n\mathbb{Z} \right)$. If $\mathfrak{w} = 1$, then we have

$$\text{Gal}(K^{\text{ab}}/L_K) \stackrel{\text{nc}}{\simeq} \widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}, \quad \text{with } \text{Gal}(K^{\text{ab}}/\mathcal{H}) \stackrel{\text{nc}}{\simeq} \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}.$$

Corollary 2.1. *The Galois groups $\text{Gal}(K^{\text{ab}}/L_K)$ (up to non-canonical isomorphisms of profinite groups) are independent of the number fields K as soon as these fields satisfy the Leopoldt conjecture for all p , have the same number r_2 of complex places, and the same parameters δ, \mathfrak{w} .*

Thus, under the Leopoldt conjecture, for all number fields K satisfying the condition $K \cap \mathbb{Q}(\mu_{p^\infty}) \subseteq \mathbb{Q}(\mu_p)$ for all $p \mid [K : \mathbb{Q}]$ (i.e., $\nu_p(K) = 0$ for all $p \mid [K : \mathbb{Q}]$), we have $\text{Gal}(K^{\text{ab}}/L_K) \stackrel{\text{nc}}{\simeq} \widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$.

For example, all the subfields K of the maximal real and tame Abelian extension $H_{\mathbb{Q}}^{\text{ta}+}$ of \mathbb{Q} verify the above property with $r_2 = \delta = 0$ (note that $H_{\mathbb{Q}}^{\text{ta}+}$ is the maximal real subfield of the compositum of the $\mathbb{Q}(\mu_p)$, $p \neq 2$).

Of course, the groups $\text{Gal}(L_K/K) \simeq \prod_p \mathcal{T}_p$ strongly depend on K , even if the parameters r_2, δ, \mathbf{w} are constant. From Remark 2.1 (i), we see that the first two conditions (i₁), (i₂) of p -rationality involve an explicit finite set of primes p , but that the third condition (i₃) is the most intricate since all the primes are a priori concerned when K contains units of infinite order.

For instance, for $K = \mathbb{Q}(\sqrt{2})$, the condition (i₃) is not satisfied for the primes $p = 13, 31, 1546463$ up to 10^9 . The great rarity of the solutions (nothing between 31 and 1546463) is to point out. We shall give more examples in §3.4.1 and theoretical arguments in §3.4.2.

It is likely that for the fields K such that $r_1 + r_2 - 1 > 0$, L_K/K can be infinite, despite numerical experiments for increasing values of p ; but the existence of such number fields, p -rational for all p , remains an open question.

There are no serious conjectures about the finiteness or not of these extensions, except perhaps some arguments stronger than the ABC conjecture.

The case $r_1 + r_2 - 1 = 0$ corresponds to $K = \mathbb{Q}$ (p -rational for all p) and to K imaginary quadratic for which $\prod_p \mathcal{T}_p$ is finite and computable. So, an exceptional family is that of imaginary quadratic fields, studied in [1], for which the condition (i₃) is empty; the conditions (i₁), (i₂) can be verified (for all p) probably for infinitely many imaginary quadratic fields as suggested in [1], Conj. 7.1.

Remark 2.3. From the results of [6], III, or [5], IV.3.5.1, the 2-rational Abelian 2-extensions of \mathbb{Q} are the subfields (for ℓ prime) of $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\sqrt{-\ell})$, $\ell \equiv 3 \pmod{8}$, or of $\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\sqrt{\sqrt{\ell} \frac{a-\sqrt{\ell}}{2}})$, $\ell = a^2 + 4b^2 \equiv 5 \pmod{8}$.

So the 2-rational quadratic fields are $\mathbb{Q}(\sqrt{\pm 2})$, $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{\pm \ell})$, and $\mathbb{Q}(\sqrt{\pm 2\ell})$, ℓ prime, $\ell \equiv 3, 5 \pmod{8}$.

3. A generalization of p -rationality

As we shall see now, we can strengthen a few the previous results, for all number fields, by showing that the first condition (i₁), involved in the definition of p -rationality (Remark 2.1 (i)), is not an obstruction to get a straightforward structure for A_K , contrary to the conditions (i₂), (i₃).

This concerns the finite p -groups $\prod_{v|p} \mu_p(K_v) / i_p(\mu_p(K))$ whose globalization measures the gap between the Regular and Hilbert kernels in $K_2(K)$ (see e.g. [4] or [5], II.7.6.1).

3.1. Another consequence of the Leopoldt conjecture. Consider, for all finite place v of K , the decomposition $\mu(K_v) \simeq F_v^\times \times \mu_v^1$ (see §1.2). The places such that $\mu_v^1 \neq 1$ (called the irregular places of K) are finite in

number. Let

$$\Gamma_p := \prod_{v \nmid p} F_{v,(p)}^\times \times \prod_{v|p} \mu_v^1 \simeq \prod_v \mu_p(K_v).$$

Let $H_{(p)}^{1pra}$ be the subfield of $H_{(p)}^{pra}$ fixed by $\rho(\Gamma_p)$, where ρ is the reciprocity map on the p -Sylow subgroup $\mathcal{U}_{(p)} \simeq \prod_{v \nmid p} F_{v,(p)}^\times \times \prod_{v|p} U_v^1$ of the group of unit idèles $\mathcal{U} = \prod_v U_v$ of K . The kernel of ρ is $i(E \otimes \mathbb{Z}_p)$, where $i = (i_{\text{ta}}, i_p)$ (see § 2.1). Then from the (non-trivial) local-global characterization of the Leopoldt conjecture at p ([9], § 2.3, or [5], III.3.6.6), we get

$$\rho(\Gamma_p) \stackrel{\text{can}}{\simeq} \Gamma_p / i(E \otimes \mathbb{Z}_p) \cap \Gamma_p = \Gamma_p / i(\mu_p(K)).$$

Take, as in [1], Lem. 3.3, 3.4, v_0 such that the residue image of $\mu_p(K)$ is equal to $F_{v_0,(p)}^\times$ (for the existence of v_0 , use the results of §§ 2.2.1, 2.2.2); we get $\text{Gal}(K_{(p)}^{\text{ab}}/H_{(p)}^{1pra}) \stackrel{\text{can}}{\simeq} \Gamma_p / i(\mu_p(K)) \stackrel{\text{nc}}{\simeq} \prod_{v \nmid p, v \neq v_0} F_{v,(p)}^\times \times \prod_{v|p} \mu_v^1$.

To study the influence of the direct cyclic factors $\mu_v^1 = \mu_p(K_v)$ for $v|p$, on the structure of the component $\prod_{v \nmid p, v \neq v_0} F_{v,(p)}^\times$ still isomorphic to

$\prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathfrak{w}n\mathbb{Z} \right)_{(p)}$, we refer to Definitions 2.2, 2.3 defining $\nu, \delta, \mathfrak{w}_p$, and to Proposition 2.1.

(i) Case $p \neq 2$. If K contains μ_p , then $\mathfrak{w}_p = p^{\nu+1} = |\mu_p(K)|$ divides $|\mu_p(K_v)|$; so, for $v|p$, the direct cyclic factor $\mu_p(K_v) = \mu_v^1$ does not modify the global structure. If K does not contain μ_p , we have only to look at the case $\nu \geq 1$ for which $\mathfrak{w}_p = p^{\nu+1}$. If $\mu_p(K_v)$ is non-trivial ($v|p$ is split in $K(\mu_p)$), $|\mu_p(K_v)|$ is a multiple of $p^{\nu+1}$, giving the result.

(ii) Case $p = 2$. If K contains μ_4 , then $\mathfrak{w}_2 = 4 \cdot 2^\nu = |\mu_2(K)|$ divides $|\mu_2(K_v)|$, hence the result. If K does not contain μ_4 , we have only to consider the case $K \cap \mathbb{Q}(\mu_{2^\infty}) \in \{Q_{2^\nu}, Q'_{2^\nu}\}$, $\nu \geq 1$. Then $\delta = 1$ and $\mathfrak{w}_2 = 4 \cdot 2^\nu$; so $\mu_2(K_v) = \mu_2$ (if $v|2$ is not split in $K(\mu_4)$) or $\mu_{4 \cdot 2^m}$, $m \geq \nu$ (if $v|2$ is split in $K(\mu_4)$), hence the result.

We then have $\text{Gal}(K_{(p)}^{\text{ab}}/H_{(p)}^{1pra}) \stackrel{\text{nc}}{\simeq} \prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathfrak{w}n\mathbb{Z} \right)_{(p)}$ for all p .

Note that $\text{Gal}(H_{(p)}^{pra}/H_{(p)}^{1pra}) \stackrel{\text{can}}{\simeq} \prod_{v|p} \mu_v^1 / \mu_p(K)$ ([5], III.4.15.3).

We have obtained, as a consequence of the Leopoldt conjecture in K for all p , an analogue of the Theorem 2.1 using an extension L_K/K such that $\text{Gal}(L_K/K) \stackrel{\text{nc}}{\simeq} \prod_p \mathcal{T}_p$:

Theorem 3.1. *Let K be a number field and let K^{ab} be the maximal Abelian pro-extension of K . Let $\mathcal{H}^1 \subseteq \mathcal{H}$ be the compositum, over p , of the $H_{(p)}^{1pra}$ which are the subfields of the $H_{(p)}^{pra}$ fixed by $\prod_{v|p} \mu_v^1 / \mu_p(K)$.*

Then there exists an Abelian extension $L_K^1 \subseteq L_K$ of K such that \mathcal{H}^1 is the direct compositum over K of L_K^1 and the maximal $\widehat{\mathbb{Z}}$ -extension \widehat{K} of K , and such that (see Definition 2.3)

$$\text{Gal}(K^{\text{ab}}/L_K^1) \stackrel{\text{nc}}{\simeq} \widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathfrak{w}n\mathbb{Z} \right),$$

with $\text{Gal}(K^{\text{ab}}/\mathcal{H}^1) \stackrel{\text{nc}}{\simeq} \prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathfrak{w}n\mathbb{Z} \right)$

and $\text{Gal}(\mathcal{H}/\mathcal{H}^1) \stackrel{\text{can}}{\simeq} \prod_v \mu_v^1 / \mu(K)$. If $\mathfrak{w} = 1$, then we obtain

$$\text{Gal}(K^{\text{ab}}/L_K^1) \stackrel{\text{nc}}{\simeq} \widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}, \text{ with } \text{Gal}(K^{\text{ab}}/\mathcal{H}^1) \stackrel{\text{nc}}{\simeq} \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}.$$

In the following exact sequence, where $\mathcal{T}_p^1 := \text{Gal}(H_{(p)}^{1\text{pra}}/\widehat{K}_{(p)})$,

$$0 \rightarrow \prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathfrak{w}n\mathbb{Z} \right) \rightarrow \text{Gal}(K^{\text{ab}}/\widehat{K}) \rightarrow \prod_p \mathcal{T}_p^1 \rightarrow 1,$$

we do not know if the structure of $\text{Gal}(K^{\text{ab}}/\widehat{K})$ can be the same for various K because of the unknown groups $\prod_p \mathcal{T}_p^1 \stackrel{\text{nc}}{\simeq} \text{Gal}(L_K^1/K)$ (which non-trivially depend on the p -adic properties of the classes and units of the fields K) and the nature of the corresponding group extension.

3.2. Notion of weakly p -rational fields. We have an isomorphism of the form

$$A_K \stackrel{\text{nc}}{\simeq} \widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n \geq 1} \left((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathfrak{w}n\mathbb{Z} \right)$$

as soon as the conditions (i₂), (i₃) of p -rationality (Remark 2.1 (i)) are satisfied for all p , which is an extremely strong assumption. In an opposite manner, the conditions (i₂), (i₃) for fixed prime p are very common and leads to the following definition which may have some interest:

Definition 3.1. Let p be a prime number. The number field K is said to be *weakly p -rational* if it satisfies the Leopoldt conjecture for p and the two following conditions (equivalent to $\mathcal{T}_p^1 = 1$ or to $\mathcal{T}_p = \prod_{v|p} \mu_v^1 / \mu_p(K)$):

(i₂) The p -Hilbert class field is contained in the compositum of the \mathbb{Z}_p -extensions of K (i.e., $|\mathcal{C}_{(p)}| = (\mathbb{Z}_p \text{Log}_p(I_p) : \prod_{v|p} \log(U_v^1) + \mathbb{Q}_p \log_p(E))$),

(i₃) $\mathbb{Z}_p \log_p(E)$ is a direct factor in $\prod_{v|p} \log(U_v^1)$.

From [5], III.4.2.4, we can analyse $\text{Gal}(H_{(p)}^{\text{pra}}/\widehat{K}_{(p)}H_{(p)})$ as follows:

Lemma 3.1. Under the Leopoldt conjecture, we have the exact sequence:

$$1 \rightarrow \prod_{v|p} \mu_v^1 / \mu_p(K) \rightarrow \text{Gal}(H_{(p)}^{\text{pra}}/\widehat{K}_{(p)}H_{(p)}) \stackrel{\text{can}}{\simeq} \text{tor}_{\mathbb{Z}_p} \left(\prod_{v|p} U_v^1 / i_p(E \otimes \mathbb{Z}_p) \right) \rightarrow$$

$$\rightarrow \text{tor}_{\mathbb{Z}_p} \left(\prod_{v|p} \log(U_v^1) / \mathbb{Z}_p \log_p(E) \right) \rightarrow 0.$$

Thus we have, under the condition (i_2) $(H_{(p)} \subseteq \widehat{K}_{(p)})$, satisfied of course if $|\mathcal{C}_{(p)}| = 1$), a practical description of \mathcal{T}_p^1 :

Corollary 3.1. *When the condition (i_2) holds, we have the exact sequence*

$$1 \rightarrow \prod_{v|p} \mu_v^1 / \mu_p(K) \rightarrow \mathcal{T}_p \rightarrow \mathcal{T}_p^1 = \text{tor}_{\mathbb{Z}_p} \left(\prod_{v|p} \log(U_v^1) / \mathbb{Z}_p \log_p(E) \right) \rightarrow 0.$$

So, the conditions (i_2) and (i_3) give $\mathcal{T}_p = \prod_{v|p} \mu_v^1 / \mu_p(K)$ (weak p -rationality).

For imaginary quadratic fields $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})$, we find again that $A_K \stackrel{\text{nc}}{\simeq} \widehat{\mathbb{Z}}^2 \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$, as soon as $H_{(p)} \subseteq \widehat{K}_{(p)}$ for all $p \mid |\mathcal{C}_K|$, which is equivalent to $|\mathcal{C}_{(p)}| = (\mathbb{Z}_p \text{Log}_p(I_p) : \prod_{v|p} \log(U_v^1))$ for all these p .

Remark 3.1. From the results of [7], Th. 2.3, for an imaginary quadratic field K , the 2-Hilbert class field is contained in the compositum of its \mathbb{Z}_2 -extensions if and only if K is one of the following fields:

$$\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-\ell}) \ (\ell \text{ prime}, \ell \equiv 3, 5, 7 \pmod{8}), \mathbb{Q}(\sqrt{-2\ell}) \ (\ell \text{ prime}, \ell \equiv 3, 5 \pmod{8}), \mathbb{Q}(\sqrt{-\ell q}) \ (\ell, q \text{ primes}, \ell \equiv -q \equiv 3 \pmod{8}).$$

3.3. The case of quadratic fields. Give examples of non-trivial weakly p -rational quadratic fields K , i.e., such that $\mathcal{T}_p = \prod_{v|p} \mu_v^1 / \mu_p(K) \neq 1$, which supposes $p \in \{2, 3\}$ with the condition (i_2) .

3.3.1. Imaginary case. For $p = 2$, $K = \mathbb{Q}(\sqrt{-m})$, $m \neq 1$, we deduce from Remarks 2.3, 3.1 that $\mathcal{T}_2 = \mu_2 \times \mu_2 / \mu_2$, if and only if $m = \ell$ prime, $\ell \equiv -1 \pmod{8}$, or $m = \ell \cdot q$ (ℓ, q primes), $\ell \equiv -q \equiv 3 \pmod{8}$ (the case $\mathcal{T}_2 = \mu_4 / \mu_2$ for $m \equiv 1 \pmod{8}$ never occurs in this setting).

We have $\mathcal{T}_2 = \mu_2 \times \mu_2 / \mu_2$ for $m = 7, 15, 23, 31, 39, 47, 55, 71, 79, 87, 95, \dots$

For $p = 3$ and $K = \mathbb{Q}(\sqrt{-m})$, $m \neq 3$, $m \equiv 3 \pmod{9}$, $\mathcal{T}_3 = \mu_3$ occurs if the 3-Hilbert class field is contained in $\widehat{K}_{(3)}$, which gives (from [2]):

$$m = 21, 30, 39, 57, 66, 93, 102, 111, 138, 165, 183, 210, \dots \text{ (with } \mathcal{C}_{(3)} = 1),$$

$$m = 129, 174, 237, 246, 255, 327, 426, 453, 543, 597, \dots \text{ (with } |\mathcal{C}_{(3)}| = 3),$$

$$m = 1713, 1902, \dots \text{ (with } |\mathcal{C}_{(3)}| = 9).$$

3.3.2. Real case. For $p = 2$, $K = \mathbb{Q}(\sqrt{m})$, $m > 0$, the case $\mathcal{T}_2 = \mu_2 \times \mu_2 / \mu_2$ (resp. μ_4 / μ_2) holds for $m \equiv 1 \pmod{8}$ (resp. $m \equiv -1 \pmod{8}$).

Since in that cases $K(\sqrt{2})/K$ is ramified, the 2-Hilbert class field of K (in ordinary sense) is disjoint from $\widehat{K}_{(2)}$ and we must have $\mathcal{C}_{(2)} = 1$.

Let $\varepsilon = x + y\sqrt{m}$ be the fundamental unit ($m \equiv \pm 1 \pmod{8}$ implies $x, y \in \mathbb{Z}$ and ε of norm 1, so we can suppose ε totally positive). A local computation shows that the condition (i_3) of Definition 3.1 is equivalent to $\log_2(x + y\sqrt{m}) \equiv \pm 4\sqrt{m} \pmod{8}$.

The case $\mathcal{T}_2 = \mu_4/\mu_2$ does not exist. Indeed, $m \equiv -1 \pmod{8}$ under the assumption $\mathcal{C}_{(2)} = 1$, implies $m = \ell$ prime ([5], IV.4.2.9). Moreover y is odd, otherwise $4 \mid y$ and $\pm\varepsilon$ is 2-primary ([5], I.6.3.4 (ii)) giving $K(\sqrt{\pm\varepsilon})/K$ unramified at the finite places of K ; since the 2-Hilbert class field in restricted sense of K is $K(\sqrt{-1})$, this implies $\varepsilon \in K^{\times 2}$ (absurd). Furthermore, the relation $x^2 - \ell y^2 = 1$, with y odd and $\ell \equiv -1 \pmod{8}$ prime, implies $8 \mid x$, hence $\log_2(x + y\sqrt{\ell}) \equiv 0 \pmod{8}$ that is unsuitable. For example, for $m = 7$, \mathcal{T}_2 is of order 4 because of the exact sequence $1 \rightarrow \mu_4/\mu_2 \rightarrow \mathcal{T}_2 \rightarrow \mathcal{T}_2^1 \simeq \mathbb{Z}/2\mathbb{Z} \rightarrow 0$ (from Corollary 3.1).

These results probably come from general divisibility properties of the 2-adic L -function of K giving the valuation of the product $|\mathcal{C}_{(2)}| \cdot \frac{1}{\sqrt{4m}} \log_2(\varepsilon)$. So, a broader study of weak p -rationality may clarify the subject.

We have $\mathcal{T}_2 = \mu_2 \times \mu_2/\mu_2$ for $m = 17, 33, 57, 73, 89, 97, \dots$ but the case $m = 41$ fails since $\log_2(\varepsilon) = \log_2(32 + 5\sqrt{41}) \equiv 0 \pmod{32}$.

For $p = 3$, the 3-Hilbert class field is disjoint from $\widehat{K}_{(3)}$. So we must take $K = \mathbb{Q}(\sqrt{m})$, $m > 0$, $m \equiv -3 \pmod{9}$, with $\mathcal{C}_{(3)} = 1$ and ε such that $\log_3(\varepsilon) \equiv \pm 3\sqrt{m} \pmod{9}$. Then $\mathcal{T}_3 = \mu_3$ holds for $m = 6, 15, 33, 51, \dots$ but fails for $m = 42$ since $\log_3(\varepsilon) = \log_3(13 + 2\sqrt{42}) \equiv 0 \pmod{9}$.

3.4. Some comments about the torsion groups \mathcal{T}_p^1 . These groups represent an obstruction for a straightforward structure of Abelian profinite group for A_K and they are probably among the deepest invariants for class field theory over K . So we intend to recall some information on them.

3.4.1. Computational aspects. Numerical studies of the torsion groups \mathcal{T}_p (or of \mathcal{T}_p^1) essentially concern imaginary quadratic fields, which is reasonable since in that case the invariant $\prod_p \mathcal{T}_p$ is finite, easily computable, and behaves probably as a global class group.

In [2] is given a table of imaginary quadratic fields $\mathbb{Q}(\sqrt{-m})$ (m square-free up to 2000) giving the class number h and for each prime $p \mid h$ the numbers $[\widehat{K}_{(p)} \cap H_{(p)} : K] = (\mathbb{Z}_p \text{Log}_p(I_p) : \prod_{v \mid p} \log(U_v^1))$ and $|\mathcal{T}_p|$. When $p \nmid h$, $\mathcal{T}_p^1 = 1$ and $\mathcal{T}_p = \prod_{v \mid p} \mu_v^1/\mu_p(K)$, $p = 2, 3$ (from Corollary 3.1).

In [17], the viewpoint of Cohen-Lenstra heuristics is studied: the prime p is fixed (up to 47) and some tables give the proportion of real and imaginary quadratic fields $\mathbb{Q}(\sqrt{\pm m})$, $0 < m < 10^9$, such that $|\mathcal{T}_p| \neq 1$.

In [1], §7, the viewpoint is rather analogous to the previous ones for imaginary quadratic fields K (with primes $p \mid h$ up to 97), and some tables give a careful statistical study of the other invariants of p -ramification over the fields K of arbitrary discriminant.

These works are, in some sense, the opposite approach from ours with the numerical example of $\mathbb{Q}(\sqrt{2})$ recalled in § 2.3, where p is unbounded, to note the scarcity of non-trivial \mathcal{T}_p .

More generally, using PARI [16], for real quadratic fields $K = \mathbb{Q}(\sqrt{m})$ with fundamental unit $\varepsilon = a + b\sqrt{m}$, we can find some small solutions (trivial if $p^2 \mid ab$), and often few very large ones (for instance, for $m = 307$ with $\varepsilon = 2.233.189977 + 3.97^2.179\sqrt{307}$, we obtain $p = 97$ (trivial) and $p = 2179, 112663$, up to 2.10^8). But for $K = \mathbb{Q}(\sqrt{14})$ we find the only solution $p = 6707879$, up to 2.10^8 , but nothing (up to 10^{10}) for some fields as $K = \mathbb{Q}(\sqrt{5})$ or, taking at random some large discriminant, for $K = \mathbb{Q}(\sqrt{163489})$. This does not seem to depend on the size of m and ε .

It will be interesting to consider fields with larger groups of units of infinite order to see if this phenomenon is similar (fixed field, increasing p). To this end, for a practical computation, use the main formulas of [5], III.2.6.1 for the finite number of p such that $H_{(p)} \not\subseteq \widehat{K}_{(p)}$; otherwise, use the simplifications given by Lemma 3.1 and Corollary 3.1.

In the totally real Galois case we then have the more practical formula (where \sim means “up to a p -adic unit”)

$$|\mathcal{T}_p| \sim |\mathcal{C}_{(p)}| \cdot [K \cap \widehat{\mathbb{Q}}_{(p)} : \mathbb{Q}] \cdot p^{1-[K:\mathbb{Q}]/e_p} \cdot \frac{R_p}{\sqrt{D}},$$

where R_p is the p -adic regulator, D the discriminant of K , and e_p the ramification index of p ([5], III.2.6.5).

In particular, for a real quadratic field $K \neq \mathbb{Q}(\sqrt{2})$ and $p = 2$, we have $|\mathcal{T}_2| \sim |\mathcal{C}_{(2)}| \cdot \frac{\log_2(\varepsilon)}{2\sqrt{m}}$ in any case.

The general formula (totally real case) reduces to $|\mathcal{T}_p| \sim p^{1-[K:\mathbb{Q}]} \cdot R_p$ for p large enough (i.e., $\mathcal{C}_{(p)} = 1$, $p \nmid D$, $K \cap \widehat{\mathbb{Q}}_{(p)} = \mathbb{Q}$).

We have tested the case of the cyclic cubic fields K given by the polynomials $X^3 - tX^2 - (t+3)X - 1$ (“simplest cubic fields” of Shanks giving the independent units ε and $-(1 + \varepsilon^{-1})$), and the conclusion seems very similar to that of real quadratic fields; for instance, for $t = 11$ the conductor of K is 163 and the solutions p up to 10^8 are 3, 7, 73, 10113637. For $t = 14$ (conductor 13.19), we get the solutions 628261, 8659909. No solutions up to 10^8 for $t = 6$ (conductor 9.7).

In a more general context, it is sufficient to find the irreducible polynomial of a “Minkowski unit” ε , then to compute the p -adic regulator of the conjugates of ε ; the fact that these units are not necessarily fundamental does not matter for the study of the rarity of the solutions p for $\mathcal{T}_p \neq 1$ when p is increasing.

3.4.2. Theoretical aspects. The main fact is that \mathcal{T}_p is related to Galois cohomology: if G_p is the Galois group of the maximal p -ramified, non-complexified (real infinite places are “unramified”) pro- p -extension of K , then under the Leopoldt conjecture for p in K , G_p is pro- p -free (on $r_2 + 1$ generators) if and only if $H^2(G_p, \mathbb{F}_p) = 1$, knowing that the cohomology group $H^2(G_p, \mathbb{Z}_p)$ is canonically isomorphic to the dual of \mathcal{T}_p . For more details see [5], II.5.4.5, III.4.2.2, [11], Ch. 3, §§ 1.16, 2.6, 2.7, Th. 3.74.

The arithmetical nature of the group \mathcal{T}_p brings into play p -class groups via Kummer duality and reflection theorems, and p -adic L-functions: in the totally real case, \mathcal{T}_p is connected with the residue of the p -adic ζ -function of K as studied by J. Coates in [3], App. 1, and J-P. Serre in [18].

A means to realize the rarity of prime numbers p such that $\mathcal{T}_p \neq 1$ when $r_1 + r_2 - 1 > 0$, may be the following p -rank formula ([5], III.4.2.2), where for a Galois module T , T_ω denotes its ω -component, ω being the Teichmüller character (i.e., the p -adic character of the Galois action on μ_p):

$$\text{rk}_p(\mathcal{T}_p) := \dim_{\mathbb{F}_p}(\mathcal{T}_p/\mathcal{T}_p^p) = \text{rk}_p(\mathcal{C}_\omega^{\text{spl}}(K(\mu_p))) + \sum_{v|p} d_v - d,$$

where $\mathcal{C}_\omega^{\text{spl}}$ corresponds, by class field theory, to the Galois group of the subfield of the p -Hilbert class field (of $K(\mu_p)$) in which all the places above p totally split, where d_v (resp. d) = 1 or 0 according as K_v (resp. K) contains μ_p or not. Since $\sum_{v|p} d_v - d = 0$ for $p > [K : \mathbb{Q}] + 1$, we then have to satisfy the condition $\mathcal{C}_\omega^{\text{spl}}(K(\mu_p)) \neq 1$; but in general (e.g. the places $v|p$ of K are not totally split in $K(\mu_p)/K$), $\mathcal{C}_\omega^{\text{spl}} = \mathcal{C}_\omega$ for $K(\mu_p)$.

So the rarity comes perhaps from the fact that $\mathcal{C}_\omega(K(\mu_p))$ is a very particular part of the p -class group of $K(\mu_p)$ since $\text{Gal}(K(\mu_p)/K)$ has in general $p - 1$ distinct p -adic characters χ , a number that increases with p . Moreover, an analytic viewpoint seems to indicate that non-trivial p -classes of $K(\mu_p)$ “preferably” come from characters $\chi \neq 1, \omega$; this is well known for $K = \mathbb{Q}$ since $\mathcal{C}_\omega(\mathbb{Q}(\mu_p)) = 1$ (p -rationality of \mathbb{Q} for all p).

For a real quadratic field K of discriminant $D \not\equiv 0 \pmod{p}$, of Dirichlet character ψ , the condition $\mathcal{C}_\omega^{\text{spl}}(K(\mu_p)) \neq 1$ is equivalent to

$$\frac{1}{Dp} \sum_{a=1}^{Dp} \psi \omega^{-1}(a) a \equiv 0 \pmod{p} \text{ (summation over } a \text{ prime to } Dp).$$

See also the work of Kazuyuki Hatada [8] giving relationships between the p -adic regulator and the value $\zeta_K(2 - p)$, with statistical investigations.

4. Conclusion

Let us return to the group structure of A_K . Let $L_{(p)}^1$ be an extension of K such that $H_{(p)}^{1\text{pra}}$ is the direct compositum over K of $\widehat{K}_{(p)}$ and $L_{(p)}^1$. We know (see e.g. [5], III.4.15.8) that any cyclic extension $L' \subseteq L_{(p)}^1$ of K

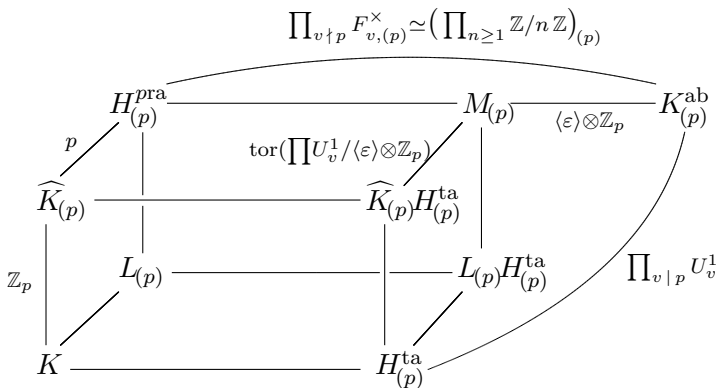
can be embedded in a cyclic p -extension of arbitrarily large degree (except perhaps in the special case $p = 2$, $K \cap \mathbb{Q}(\mu_{2^\infty}) = \mathbb{Q}_{2^\nu}$, $\nu \geq 2$, which needs specific study since $\delta = 1$).

The subgroup \mathcal{C}_p of \mathcal{T}_p corresponding to the compositum of the p -cyclically embeddable extensions of K is $\prod_{v|p} \mu_v^1 / \mu_p(K)$, except perhaps in the special case where $\prod_{v|p} \mu_v^1 / \mu_p(K)$ may be of index 2 in \mathcal{C}_p .

Thus, when $p \neq 2$ and $L_{(p)}^1 \neq K$, $\text{Gal}(K_{(p)}^{\text{ab}} / H_{(p)}^{1\text{pra}})$ cannot be a direct factor in $\text{Gal}(K_{(p)}^{\text{ab}} / \widehat{K}_{(p)})$, since \mathcal{T}_p^1 is finite. For any large p -power p^k , taking a suitable set of cyclic extensions $L'_i \subseteq L_{(p)}^1$, by composition with $\widehat{K}_{(p)}$ there exists $\widehat{L}_k \subset K_{(p)}^{\text{ab}}$, such that $\widehat{K}_{(p)} \subseteq H_{(p)}^{1\text{pra}} \subseteq \widehat{L}_k$, with $\text{Gal}(\widehat{L}_k / \widehat{K}_{(p)})$ of exponent p^k . We can even assume that $\text{Gal}(\widehat{L}_k / \widehat{K}_{(p)}) \simeq (\mathbb{Z}/p^k\mathbb{Z})^r$, where $r := \text{rk}_p(\mathcal{T}_p^1)$. It is possible that only numerical computations may help to describe the structure of $\text{Gal}(K_{(p)}^{\text{ab}} / \widehat{K}_{(p)})$ when $\mathcal{T}_p^1 \neq 1$.

An interesting case to go further is that of $K = \mathbb{Q}(\sqrt{2})$ for $p = 13$, $\prod_{v|13} U_v^1 = U_{13}^1 = 1 + 13(\mathbb{Z}_{13} \oplus \mathbb{Z}_{13}\sqrt{2})$, and $\log(U_{13}^1) = 13(\mathbb{Z}_{13} \oplus \mathbb{Z}_{13}\sqrt{2})$. In this case, $\mathcal{T}_{13} = \mathcal{T}_{13}^1$ is cyclic of order 13 since $\varepsilon = 1 + \sqrt{2}$ is such that $-\varepsilon^{14} \equiv 1 + 13^2 a \sqrt{2} \pmod{13^3}$ with a rational $a \not\equiv 0 \pmod{13}$, giving $\log(\varepsilon) \equiv 13^2 a \sqrt{2} \pmod{13^3}$, hence the result using Lemma 3.1.

With such similar numerical data for a real quadratic field $\mathbb{Q}(\sqrt{m})$ (i.e., $p \neq 2, 3$, $p \nmid m$, $\mathcal{C}_{(p)} = 1$, $\pm\varepsilon^{p+1}$ (p inert) or $\pm\varepsilon^{p-1}$ (p split) is, modulo p^3 , of the form $1 + p^2 a \sqrt{m}$ with a rational $a \not\equiv 0 \pmod{p}$), we get the same conclusion and the following diagram:



For $K = \mathbb{Q}(\sqrt{2})$, $p = 13$, we have no more information likely to give a result on the structure of the profinite group $\text{Gal}(K_{(13)}^{\text{ab}} / \widehat{K}_{(13)})$ containing a subgroup, of index 13, isomorphic to $\prod_{m \geq 0} (\mathbb{Z}/13^m \mathbb{Z})^{\mathbb{N}}$.

Despite the previous class field theory study, it remains possible that A_K be always non-canonically isomorphic to $\widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n \geq 1} ((\mathbb{Z}/2\mathbb{Z})^\delta \times \mathbb{Z}/\mathfrak{w}n\mathbb{Z})$, independently of additional arithmetic considerations about the unknown group $\prod_p \mathcal{T}_p^1$. If not (more probable), a description of the profinite group A_K may be very tricky. Any information will be welcome.

Acknowledgements

I thank Peter Stevenhagen who pointed out to me a common error, regarding the definition of the parameter \mathfrak{w} associated to the number field K , in [15] and in the first drafts of our previous versions, and for his remarks and cooperation in the improvement of this version.

Many thanks to Jean-François Jaulent for relevant advices and to the scientific committee of the JTNB for its patience. I sincerely thank an anonymous Referee for several valuable suggestions.

References

- [1] A. ANGELAKIS AND P. STEVENHAGEN, *Absolute abelian Galois groups of imaginary quadratic fields*, In: proceedings volume of ANTS-X, UC San Diego 2012, E. Howe and K. Kedlaya (eds), OBS 1 (2013).
- [2] A. CHARIFI, *Groupes de torsion attachés aux extensions Abéliennes p -ramifiées maximales (cas des corps totalement réels et des corps quadratiques imaginaires)*, Thèse de 3^e cycle, Mathématiques, Université de Franche-Comté (1982), 50 pp.
- [3] J. COATES, *p -adic L -functions and Iwasawa's theory*, In: Proc. Durham Symposium 1975, New York-London (1977), 269–353.
- [4] G. GRAS ET J-F. JAULENT, *Sur les corps de nombres réguliers*, Math. Z. **202**, (1989), 3, 343–365.
- [5] G. GRAS, *Class Field Theory: from theory to practice*, SMM, Springer-Verlag 2003, second corrected printing (2005).
- [6] G. GRAS, *Remarks on K_2 of number fields*, Jour. Number Theory **23**, (1986), 3, 322–335.
- [7] G. GRAS, *Sur les \mathbb{Z}_2 -extensions d'un corps quadratique imaginaire*, Ann. Inst. Fourier, **33**, (1983), 4, 1–18.
- [8] K. HATADA, *Mod 1 distribution of Fermat and Fibonacci quotients and values of zeta functions at $2 - p$* , Comment. Math. Univ. St. Paul. **36**, (1987), 1, 41–51.
- [9] J-F. JAULENT, *Théorie ℓ -adique globale du corps de classes*, J. Théorie des Nombres de Bordeaux **10**, (1998), 2, 355–397.
- [10] J-F. JAULENT ET T. NGUYEN QUANG DO, *Corps p -rationnels, corps p -réguliers et ramification restreinte*, J. Théorie des Nombres de Bordeaux **5**, (1993), 2, 343–363.
- [11] H. KOCH, (Parshin, A.N., Šafarevič, I.R., and Gamkrelidze, R.V., Eds.), *Number theory II, Algebraic number theory*, Encycl. of Math. Sci., vol. 62, Springer-Verlag 1992; second printing: *Algebraic Number Theory*, Springer-Verlag 1997.
- [12] T. KUBOTA, *Galois group of the maximal abelian extension of an algebraic number field*, Nagoya Math. J. **12**, (1957), 177–189.
- [13] A. MOVAHHEDI ET T. NGUYEN QUANG DO, *Sur l'arithmétique des corps de nombres p -rationnels*, Sém. Théorie des Nombres, Paris (1987/89), Progress in Math. **81**, Birkhäuser (1990), 155–200.
- [14] W. NARKIEWICZ, *Elementary and analytic theory of algebraic numbers*, P.W.N. 1974; second revised and extended edition: P.W.N. and Springer-Verlag 1990; third edition: Springer Monographs in Math., Springer-Verlag 2004.

- [15] M. ONABE, *On the isomorphisms of the Galois groups of the maximal Abelian extensions of imaginary quadratic fields*, Natur. Sci. Rep. Ochanomizu Univ. **27**, (1976), 2, 155–161.
- [16] PARI/GP, Version 2.5.3, K. Belabas and al., Laboratoire A2X, Université de Bordeaux I.
- [17] F. PITOUN AND F. VARESCON, *Computing the torsion of the p -ramified module of a number field*, Math. Comp., published electronically (2014), **84**, (2015), 371–383.
- [18] J-P. SERRE, *Sur le résidu de la fonction zêta p -adique d'un corps de nombres*, C.R. Acad. Sci. Paris **287**, (1978), Série I, 183–188.

Georges GRAS

Villa la Gardette

Chemin Château Gagnière

38520 Le Bourg d'Oisans

E-mail: g.mn.gras@wanadoo.fr

URL: <http://monsite.orange.fr/maths.g.mn.gras/>