



HAL
open science

Number fields whose Abelian closures have isomorphic Galois groups

Georges Gras

► **To cite this version:**

Georges Gras. Number fields whose Abelian closures have isomorphic Galois groups. 2012. hal-00764649v1

HAL Id: hal-00764649

<https://hal.science/hal-00764649v1>

Preprint submitted on 13 Dec 2012 (v1), last revised 18 Feb 2013 (v4)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

NUMBER FIELDS WHOSE ABELIAN CLOSURES HAVE ISOMORPHIC GALOIS GROUPS

by

Georges GRAS

Abstract. — Following a paper by Athanasios Angelakis and Peter Stevenhagen on the determination of imaginary quadratic fields having the same absolute Abelian Galois group (arXiv:1209.6005), we study this property for arbitrary number fields. We show that such a property is probably not generalizable to fields not imaginary quadratic, because of some p -adic obstructions about the units. By restriction to the p -parts of the Galois groups, we show that the corresponding study is related to the classical notion of p -rational fields. All this is a consequence of results yet published in our Springer book on class field theory.

Résumé. — A partir d'un article de Athanasios Angelakis et Peter Stevenhagen sur la détermination de corps quadratiques imaginaires ayant le même groupe de Galois Abélien absolu (arXiv:1209.6005), nous étudions cette propriété pour les corps de nombres quelconques. Nous montrons qu'une telle propriété est probablement non généralisable aux corps non quadratiques imaginaires en raison d'obstructions p -adiques au niveau des unités. En se restreignant aux p -parties des groupes de Galois, nous montrons que l'étude correspondante est liée à la notion classique de corps p -rationnels. Tout ceci est une conséquence de résultats déjà publiés dans notre livre chez Springer sur la théorie du corps de classes.

1. Introduction – Notations

Let K be a number field of degree $n =: r_1 + 2r_2$, and let A_K be the Galois group $\text{Gal}(\overline{K}^{\text{ab}}/K)$ where \overline{K}^{ab} is the maximal Abelian pro-extension of K . The question is the following: in what circumstances the groups A_{K_1} and A_{K_2} are isomorphic groups when K_1 and K_2 are two distinct number fields? Of course such isomorphisms are only isomorphisms of Abelian profinite groups in which the arithmetical invariants (decomposition groups, inertia groups) are not respected. A first work on this subject was published in [O] by Midori Onabe.

Let p be a fixed prime number and let H^{ord} , H_p^{ord} , $H_{\text{ta}}^{\text{res}}$, \tilde{K}_p , be the p -Hilbert class field, the maximal p -ramified (i.e. unramified outside p) Abelian pro- p -extension of K (in ordinary senses), the maximal tamely ramified Abelian pro- p -extension of K (in restricted sense), the compositum of the \mathbb{Z}_p -extensions of K , respectively.

Then let $\mathcal{T}_p^{\text{ord}} := \text{Gal}(H_p^{\text{ord}}/\tilde{K}_p)$ and $\mathcal{C}_p^{\text{ord}} := \text{Gal}(H^{\text{ord}}/K)$ isomorphic to the p -class group of K . The groups $\mathcal{T}_p^{\text{ord}}$ and $\mathcal{C}_p^{\text{ord}}$ are finite groups.

For any finite place v of K , we denote by K_v the corresponding completion of K , then by $U_v := \{u \in K_v, |u|_v = 1\}$ and $U_v^1 := \{u \in U_v, |u - 1|_v < 1\}$, the unit group and principal unit group of K_v , respectively.

Key words and phrases. — Class field theory, Abelian Galois groups, p -rational fields.

These definitions can be summarized by the following diagram [Gr1, III.2.6.1, Fig. 2.2]:

$$\begin{array}{ccccc}
 & & \mathcal{T}_p^{\text{ord}} & & \\
 & & \text{-----} & & \\
 \tilde{K}_p & \xrightarrow{\quad} & \tilde{K}_p H_p^{\text{ord}} & \xrightarrow{\quad} & H_p^{\text{ord}} \\
 | & & | & & \nearrow \\
 \tilde{K}_p \cap H_p^{\text{ord}} & \xrightarrow{\quad} & H_p^{\text{ord}} & \xrightarrow{\quad} & \mathcal{B}_p \\
 | & & \nearrow & & \\
 K & \xrightarrow{\quad} & \mathcal{C}_p^{\text{ord}} & &
 \end{array}$$

where $\mathcal{B}_p \simeq \bigoplus_{v|p} U_v^1 / i_p(E \otimes \mathbb{Z}_p)$, where E is the group of global units of K and $i_p = (i_v)_{v|p}$ the diagonal embedding.

We shall make use of some p -adic logarithms as follows:

(i) We consider the \mathbb{Q}_p -vector space $\bigoplus_{v|p} K_v$, and we denote by \log_p the p -adic logarithm:

$$\begin{array}{ccc}
 K^\times & \longrightarrow & \bigoplus_{v|p} K_v \\
 x & \longmapsto & (\log_v(x))_{v|p}
 \end{array}$$

where $\log_v(x) := \log(i_v(x))$ for all $v|p$, and where $\log : \mathbb{C}_p^\times \rightarrow \mathbb{C}_p$ is the Iwasawa extension of the usual p -adic logarithm defined on the group of principal units $u =: 1 + x$ of \mathbb{C}_p by the convergent series $\log(1 + x) := \sum_{i \geq 1} (-1)^{i+1} \frac{x^i}{i}$, and by $\log(p) := 0$.

We still denote by \log the map $\bigoplus_{v|p} K_v^\times \rightarrow \bigoplus_{v|p} K_v$ defined by $\log((x_v)_{v|p}) := (\log(x_v))_{v|p}$.

We then have $\log_p = \log \circ i_p$ on K^\times .

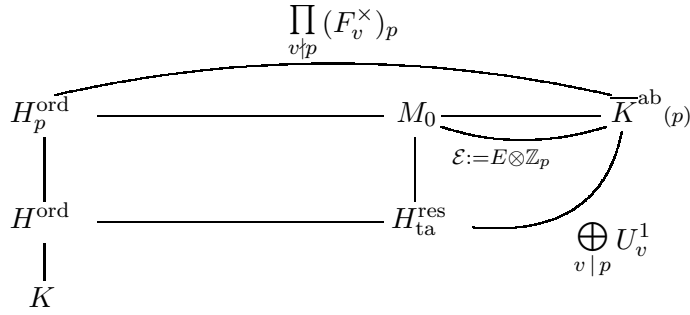
(ii) We then define the quotient \mathbb{Q}_p -vector space $\mathcal{L}_p := \left(\bigoplus_{v|p} K_v \right) / \mathbb{Q}_p \log_p(E)$. We have, under the Leopoldt conjecture for p in K , $\dim_{\mathbb{Q}_p}(\mathcal{L}_p) = r_2 + 1$.

(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. If m is such that $\mathfrak{a}^m = (\alpha)$ with $\alpha \in K^\times$, we set $\text{Log}_p(\mathfrak{a}) := \frac{1}{m} \log_p(\alpha) \bmod \mathbb{Q}_p \log_p(E)$.

It is clear that if we also have $\mathfrak{a}^{m'} = (\alpha')$ with $\alpha' \in K^\times$, then $(\alpha)^{m'} = (\alpha')^m$, hence $\alpha^{m'} = \alpha'^m \varepsilon$ with $\varepsilon \in E$, so that $\frac{1}{m} \log_p(\alpha) = \frac{1}{m'} \log_p(\alpha') + \frac{1}{m m'} \log_p(\varepsilon)$, showing that Log_p is defined in \mathcal{L}_p .

2. Class field study of the Abelian closure

In [Gr1, III.4.4.1], we have given the following fundamental diagram for the structure of the p -part of the Galois group A_K (assuming the Leopoldt conjecture for p), where $\overline{K}^{\text{ab}}(p)$ is the maximal Abelian pro- p -extension of K :



where F_v is the residue field of v in K and $(F_v^\times)_p \simeq F_v^\times \otimes \mathbb{Z}_p$ the p -part of its multiplicative group. This also concerns the real infinite places for which $F_v^\times = \{\pm 1\}$ (see [Gr1, I.3.1.2]). For the definition of the embeddings of $\mathcal{E} := E \otimes \mathbb{Z}_p$ in $\prod_{v \nmid p} (F_v^\times)_p$ and in $\bigoplus_{v|p} U_v^1$, respectively, see [Gr1, III.4.4.5.1].

Definition 2.1. — The number field K is said to be p -rational (see [MN], [GJ], [JN]) if it satisfies the Leopoldt conjecture for p and if $\mathcal{T}_p^{\text{ord}} = 1$.

Remarks 2.2. — (i) By [Gr1, III.2.6.1 (ii₂)], using [Gr1, III.4.2.4, III.4.2.5], and assuming the Leopoldt conjecture, the p -rationality of K is equivalent to the following three conditions:

- the p -Hilbert class field H^{ord} is contained in the compositum \tilde{K}_p of the \mathbb{Z}_p -extensions of K (this point is equivalent to the fact that $\mathcal{C}_p^{\text{ord}} \simeq \mathbb{Z}_p \text{Log}_p(I_p) / \bigoplus_{v|p} \log(U_v^1) \bmod \mathbb{Q}_p \log_p(E)$, which can be nontrivial),
- $\bigoplus_{v|p} \mu_p(K_v) = i_p(\mu_p(K))$, where $\mu_p(k)$ denotes, for any field k , the group of roots of unity in k of p -power order,
- $\mathbb{Z}_p \log_p(E)$ is a direct summand in $\bigoplus_{v|p} \log(U_v^1)$, which expresses the minimality of the valuation of the p -adic regulator.

(ii) If K is p -rational, then all its subfields are p -rational. By [Gr1, III.4.1.11], \mathbb{Q} is p -rational for all p .

(iii) For a p -rational field K , we have (noncanonically, see [Gr1, III.4.1.10]):

$$\text{Gal}(\overline{K}^{\text{ab}}(p)/K) \simeq \mathbb{Z}_p^{r_2+1} \times \prod_{v \nmid p} (F_v^\times)_p.$$

So, a sufficient condition to get $\text{Gal}(\overline{K}^{\text{ab}}/K) \simeq \widehat{\mathbb{Z}}^{r_2+1} \times \prod_v F_v^\times$ is that K be p -rational for all p .

We have the following result, valid for any number field K .

Proposition 2.3. — Let K be a number field. We denote by μ_K the group of roots of unity in K and by w_K its order. Let F_v be the residue field of the place v (finite or real infinite) in K . Then we have the group isomorphism

$$\prod_v F_v^\times \simeq \prod_{n \geq 1} \mathbb{Z}/w_K n \mathbb{Z}.$$

Proof. — Since $\mathbb{Q}(\mu_K) \subseteq K$, we know that $|F_v^\times| \equiv 0 \pmod{w_K}$ for all v . Then, following [AS, Lemma 3.2], we consider in the two groups the ℓ -parts for fixed prime ℓ . We have to prove that in the left member there exist infinitely many places v of K for which the norm $N_v := |F_v|$ is congruent to 1 modulo ℓ^m but not modulo ℓ^{m+1} , where $m \geq 0$ is the ℓ -valuation

of w_K . Let ζ be a primitive ℓ^{m+1} th root of unity; then $K(\zeta)/K$ is a nontrivial extension since $\mathbb{Q}(\zeta) \not\subseteq K$, and there exist infinitely many finite places v of K totally split in K/\mathbb{Q} and non totally split in $K(\zeta)/K$; so the prime q under v is non totally split in $\mathbb{Q}(\zeta)/K \cap \mathbb{Q}(\zeta)$ and totally split in $\mathbb{Q}(\zeta^\ell)/\mathbb{Q}$. From classical class field theory in cyclotomic fields, we get the result. \square

Corollary 2.4. — *Let \mathcal{H}^{ord} be the compositum of the fields H_p^{ord} (maximal p -ramified Abelian pro- p -extensions of K) for all prime numbers p . Then we have the group isomorphism*

$$\text{Gal}(\overline{K}^{\text{ab}}/\mathcal{H}^{\text{ord}}) \simeq \prod_{n \geq 1} \mathbb{Z}/w_K n\mathbb{Z}.$$

So we can resume with the following diagram:

$$\begin{array}{ccccc}
 & & \prod_{n \geq 1} \mathbb{Z}/w_K n\mathbb{Z} & & \\
 & & \curvearrowright & & \\
 \mathcal{H}^{\text{ord}} & \xrightarrow{\quad} & \mathcal{M}_0 & \xrightarrow{\quad} & \overline{K}^{\text{ab}} \\
 | & & | & \xrightarrow{\quad \varepsilon := E \otimes \widehat{\mathbb{Z}} \quad} & | \\
 H^{\text{ord}} & \xrightarrow{\quad} & \mathcal{H}_{\text{ta}}^{\text{res}} & \xrightarrow{\quad} & \prod_v U_v^1 \\
 | & & & & \\
 K & & & &
 \end{array}$$

where $\mathcal{H}_{\text{ta}}^{\text{res}}$ is the compositum of the tame extensions $H_{\text{ta}}^{\text{res}}$ and $\mathcal{M}_0 = \mathcal{H}^{\text{ord}} \mathcal{H}_{\text{ta}}^{\text{res}}$ (direct compositum over H^{ord}). So we can summarize these results in the following theorem:

Theorem 2.5. — *Let \overline{K}^{ab} be the maximal Abelian pro-extension of K . We suppose that the p -adic Leopoldt conjecture is verified in K for all prime number p . There exists an Abelian extension \mathcal{F}_K of K such that \mathcal{H}^{ord} is the direct compositum of \mathcal{F}_K and the maximal $\widehat{\mathbb{Z}}$ -extension, $\widehat{\mathcal{K}}$, of K and such that*

$$\text{Gal}(\overline{K}^{\text{ab}}/\mathcal{F}_K) \simeq \widehat{\mathbb{Z}}^{r_2+1} \times \prod_{n \geq 1} \mathbb{Z}/w_K n\mathbb{Z}.$$

Remark 2.6. — Write $w_K = \prod_{\ell \text{ prime}} \ell^{\lambda_\ell}$ and put $w_K^1 := \prod_{\lambda_\ell \geq 2} \ell^{\lambda_\ell}$. Then we can replace w_K by w_K^1 in the above formulas.

Corollary 2.7. — *The Galois groups $\text{Gal}(\overline{K}^{\text{ab}}/\mathcal{F}_K)$ (up to non canonical isomorphisms) are independant of the number fields K as soon as these fields have the same number of complex places and the same w_K^1 .*

Thus, for all totally real number fields K (satisfying the Leopoldt conjecture for all p) we have

$$\text{Gal}(\overline{K}^{\text{ab}}/\mathcal{F}_K) \simeq \widehat{\mathbb{Z}} \times \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}.$$

Of course the extension \mathcal{F}_K/K is in general non canonical and infinite. It is the compositum of finite extensions F_p such that $H_p^{\text{ord}} = \widehat{K}_p F_p$; we then have $\text{Gal}(F_p/K) \simeq \mathcal{T}_p$ for each p , and $\text{Gal}(\mathcal{F}_K/K)$ measures a mysterious degree of complexity of $\text{Gal}(\overline{K}^{\text{ab}}/K)$.

We have $\mathcal{F}_K = K$ if and only if K is p -rational for all p , which is a very strong condition.

From Remark 2.2, we see that the first two conditions involve a finite number of primes p , but that the third condition is the most ugly. For instance, for $K = \mathbb{Q}(\sqrt{2})$, it is not satisfied for $p = 13, 31, 1546463, \dots$ and perhaps for infinitely many primes p (see [Gr1, III.4.14]).

So, we are only concerned with the imaginary quadratic fields studied in [AS] since in Remarks 2.2, the third point is empty; the first and second ones can be verified probably for infinitely many imaginary quadratic fields as suggested in [AS, Conjecture 7.1].

For example (after [Gr2, III]), for $p = 2$, the 2-rational Abelian 2-extensions of \mathbb{Q} are the subfields of the fields

$$\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}(\sqrt{-\ell}), \quad -\ell \equiv 5 \pmod{8},$$

or of the fields

$$\mathbb{Q}(\mu_{2^\infty})\mathbb{Q}\left(\sqrt{\sqrt{\ell} \frac{a - \sqrt{\ell}}{2}}\right), \quad \ell = a^2 + 4b^2 \equiv 5 \pmod{8}.$$

For $p = 3$, the 3-rational Abelian 3-extensions of \mathbb{Q} are the subfields of the fields

$$\tilde{\mathbb{Q}}_3 k_\ell, \quad \ell \equiv 4, 7 \pmod{9},$$

where $\tilde{\mathbb{Q}}_3$ is the cyclotomic \mathbb{Z}_3 -extension of \mathbb{Q} and k_ℓ the cyclic cubic field of conductor ℓ .

References

- [AS] A. Angelakis and P. Stevenhagen, *Absolute abelian Galois groups of imaginary quadratic fields*, arXiv:1209.6005, to appear in the proceedings volume of ANTS-X, San Diego 2012.
- [GJ] Gras, G. et Jaulent, J-F., *Sur les corps de nombres réguliers*, Math. Z. 202 (1989), 343–365.
- [Gr1] G. Gras, *Class Field Theory: from theory to practice*, SMM, Springer-Verlag, 2003; second corrected printing 2005.
- [Gr2] Gras, G., *Remarks on K_2 of number fields*, Jour. Number Theory 23 (1986), 322–335.
- [JN] Jaulent, J-F. et Nguyen Quang Do, T., *Corps p -rationnels, corps p -réguliers et ramification restreinte*, J. Théorie des Nombres de Bordeaux 5 (1993), 343–363.
- [MN] Movahhedi, A. et Nguyen Quang Do, T., *Sur l'arithmétique des corps de nombres p -rationnels*, Sémin. Théorie des Nombres, Paris (1987/89), Progress in Math. 81, Birkhäuser (1990), 155–200.
- [O] M. Onabe, *On the isomorphisms of the Galois groups of the maximal Abelian extensions of imaginary quadratic fields*, Natur. Sci. Rep. Ochanomizu Univ. 27, 2 (1976), 155–161.

December 12, 2012

GEORGES GRAS, Villa la Gardette, chemin Château Gagnière, F-38520 Le Bourg d'Oisans
E-mail : g.mn.gras@wanadoo.fr • Url : <http://monsite.orange.fr/math.g.mn.gras/>