Journal of Number Theory 129 (2009) 495–498

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Note on 2-rational fields

Georges Gras [a,*], Jean-François Jaulent [b]

[a] *Villa la Gardette, Chemin Château Gagnière, F-38520 Le Bourg d'Oisans, France*
[b] *Université de Bordeaux, Institut de Mathématiques de Bordeaux, 351, cours de la libération, F-33405 Talence Cedex, France*

ARTICLE INFO

Article history:
Received 6 May 2008
Revised 1 June 2008
Available online 10 October 2008
Communicated by David Goss

Keywords:
ℓ-Rational fields
ℓ-Regular fields
ℓ-Ramification
Class field theory
2-Rational fields
2-Regular fields
p-Rational fields
p-Regular fields

ABSTRACT

We give an alternative computation of the Galois group of the maximal 2-ramified and complexified pro-2-extension of any 2-rational number field (Theorem 2), a particular case of results of Movahhedi–Nguyen Quang Do. This short Note is motivated by the paper [J. Jossey, Galois 2-extensions unramified outside 2, J. Number Theory 124 (2007) 42–76] and, at this occasion, we bring into focus some classical technics of abelian ℓ-ramification which, unfortunately, are often ignored, especially those developed by J.-F. Jaulent with the ℓ-adic class field theory, and by G. Gras in his book on class field theory, and which considerably simplify the study of such subjects; for instance, our proof of Theorem 2 generalizes the purpose of Jossey's paper in such a way using a result of Herfort–Zalesskii. This Note is mainly an attempt of clarification about ℓ-rationality.

1. Introduction and history

The notions of ℓ-rational field and ℓ-regular field (for a prime number ℓ and a number field K), independently introduced by A. Movahhedi and T. Nguyen Quang Do in [MN], and by G. Gras and J.-F. Jaulent in [GJ], coincide as soon as K contains the maximal real subfield of the field of ℓth roots of unity, thus especially for $\ell = 2$.

- The ℓ-regularity expresses the triviality of the regular ℓ-kernel of K (i.e. the kernel, in the ℓ-part of the universal group $K_2(K)$, of Hilbert symbols attached to the non-complex places not dividing ℓ).

* Corresponding author.
E-mail addresses: g.mn.gras@wanadoo.fr (G. Gras), jean-francois.jaulent@math.u-bordeaux1.fr (J.-F. Jaulent).
URL: http://monsite.orange.fr/maths.g.mn.gras/ (G. Gras).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.06.012

- The ℓ-rationality traduces the pro-ℓ-freeness of the Galois group $\mathcal{G}_K := \mathrm{Gal}(M_K/K)$ of the maximal pro-ℓ-extension ℓ-ramified ∞-split M_K of K (i.e. unramified at the finite places[1] not dividing ℓ and totally split at the infinite places).

More precisely, let c_K be the number of complex places of K; let $\boldsymbol{\mu}_K$ (resp. $\boldsymbol{\mu}_{K_\mathfrak{l}}$) be the ℓ-group of roots of unity in K (resp. in the localization $K_\mathfrak{l}$); and let

$$V_K := \{x \in K^\times \mid x \in K_\mathfrak{l}^{\times\ell}\ \forall\mathfrak{l} \mid \ell \text{ and } v_\mathfrak{p}(x) \equiv 0 \bmod \ell\ \forall\mathfrak{p} \nmid \ell\infty\}$$

be the group of ℓ-hyperprimary elements in $K^\times$. Then, with these notations, from [JN, Th. 1.2] or [G$_3$, IV.3.5, III.4.2.3], the ℓ-rationality of K may be expressed as follows:

Theorem and definition 0. *The following conditions are equivalent*:

(i) *The Galois group $\mathcal{G}_K$ is a free pro-ℓ-group on $1 + c_K$ generators.*
(ii) *The abelianization $\mathcal{G}_K^{ab}$ of $\mathcal{G}_K$ is a free $\mathbb{Z}_\ell$-module of dimension $1 + c_K$.*
(iii) *The field K satisfies the Leopoldt conjecture (for the prime ℓ) and the torsion submodule $\mathcal{T}_K$ of $\mathcal{G}_K^{ab}$ is trivial.*
(iv) *One has the equalities*:

$$V_K = K^{\times\ell} \quad \textit{and} \quad \mathrm{rk}_\ell(\boldsymbol{\mu}_K) = \sum_{\mathfrak{l}|\ell} \mathrm{rk}_\ell(\boldsymbol{\mu}_{K_\mathfrak{l}}).$$

When any of these conditions is realized, the number field K is said to be *ℓ-rational.*

The premises of the notion of ℓ-regularity go back to the works of G. Gras, mainly to his note on the K_2 of number fields [G$_2$, II, §2; III, §§1, 2], whereas the notion of ℓ-rationality appears (in a hidden form) in the work of H. Miki [Mi] concerning the study of a sufficient condition for the Leopoldt conjecture, as well as those of K. Wingberg [W$_1$,W$_2$], concerning the same condition.

Movahhedi's thesis and the above papers [GJ,MN] characterised the going up for ℓ-rationality in any ℓ-extension in terms of ℓ-primitivity of the ramification (a definition given in [G$_2$, III, §1] from the use of the Log function defined in [G$_1$]), a property which was unknown in the preceding approaches.

For instance, this gives immediately that if K is an ℓ-extension of $\mathbb{Q}$, an N.S.C. for K to be ℓ-rational is that $K/\mathbb{Q}$ be ℓ-ramified, or that $K/\mathbb{Q}$ be $\{p, \ell\}$-ramified, where $p \neq \ell$ is a prime $\equiv 1 \bmod (\ell)$ such that $p \not\equiv \pm 1 \bmod (8)$ if $\ell = 2$ and $p \not\equiv 1 \bmod (\ell^2)$ if $\ell \neq 2$ (cf. [G$_3$, IV.3.5.1] giving Jossey's examples without any class groups considerations, which is the philosophy of ℓ-ramification theory). We must also quote another approach of ℓ-rationality, by R.I. Berger, using a normic criterion via genera theory (see [G$_3$, IV.4.8]).

A synthesis of these results is given in [JN] and a systematic exposition is developed in the book of G. Gras [G$_3$, III, §4, (b); IV, §3, (b); App., §2]; see also [NSW, Ch. X, §7] for cohomological proofs and the descriptions of the Galois groups.

Last, various generalizations of these notions have been studied by O. Sauzet and J.-F. Jaulent (cf. [JS$_1$,JS$_2$]), especially in the case $\ell = 2$ which is, as usual, the most tricky; in particular, they introduce the notion of 2-birational fields.

Very recently, J. Jossey [Jo] has given a notion of ℓ-rationality which is incompatible with the classical one (for $\ell = 2$, as soon as K contains real embeddings) and is unlucky since it does not apply to the field of rationals $\mathbb{Q}$.

For these reasons, to avoid any confusion, we propose to speak, in his context, of 2-*superrational* fields. More precisely:

[1] According to the conventions of the ℓ-adic class field theory (cf. [G$_3$,Ja]), we never speak of ramification at infinity but of *complexification* of real places.

Definition 1. Let K be a number field with r_K real places and c_K complex places; let M'_K be the maximal 2-ramified pro-2-extension of K, and M_K be the maximal subextension of M'_K totally split at the infinite places. We say that K is:

(i) 2-*superrational*, if $\mathcal{G}'_K := \mathrm{Gal}(M'_K/K)$ is pro-2-free;
(ii) 2-*rational*, if its quotient $\mathcal{G}_K := \mathrm{Gal}(M_K/K)$ is pro-2-free.

The purpose of the next section is to focus on the structure of the Galois group $\mathcal{G}'_K$ when the number field K is 2-rational.

2. Description of the Galois group $\mathcal{G}'_K = \mathrm{Gal}(M'_K/K)$

As a matter of fact, the structure of $\mathcal{G}'_K = \mathrm{Gal}(M'_K/K)$, in case the number field K is 2-rational, is given by the following special case of [MN, Th. 2.8]:

Theorem 2. *Let K be a 2-rational number field having r_K real places and c_K complex places. The Galois group $\mathcal{G}'_K := \mathrm{Gal}(M'_K/K)$ of the maximal 2-ramified pro-2-extension M'_K of K is the pro-2-free product*

$$\mathcal{G}'_K \simeq \mathbb{Z}_2^{\circledast(1+c_K)} \circledast (\mathbb{Z}/2\mathbb{Z})^{\circledast r_K}$$

of $1 + c_K$ copies of the procyclic group $\mathbb{Z}_2$ and of r_K copies of $\mathbb{Z}/2\mathbb{Z}$.

In fact, the article of A. Movahhedi and T. Nguyen Quang Do [MN] deals with S-ramified pro-extensions, so the theorem above is obtained in case the finite set S contains only the infinite places and those dividing ℓ. Unfortunately it seems that some of these results of [MN], which do contains [Jo, Theorem 2], are largely ignored and we thank the referee for his pertinent remark. Moreover, the similar reference [JN] does not include all these results on the role of the real infinite places.

So, in order to complete [JN], we give here an alternative proof of this result, which relies on the functorial properties of ℓ-ramification theory, in the spirit of Jossey's approach (based on Herfort–Zalesskii description of virtually free groups) and does not involve the notion of primitive set of places.

As a consequence, this gives:

Corollary 3. *The 2-rational number fields which are 2-superrational are the totally imaginary ones.*

Proof. Consider the quadratic extension $L = K[i]$ generated by the 4th roots of unity. It is 2-ramified over K, thus thanks to the going up theorem of [GJ,MN] (cf. e.g. [JN, Th. 3.5] or [G_3, IV.3.4.3, (iii)]), it is 2-rational, then 2-superrational since it is totally imaginary. In other words, the Galois group $\mathcal{G}_L = \mathcal{G}'_L$ of the maximal 2-ramified pro-2-extension M_L of L is pro-2-free.

Since the quadratic extension L/K is 2-ramified, M_L is also the maximal 2-ramified pro-2-extension M'_K of K; the Galois group $\mathcal{G}'_K$ is *potentially free* since it contains the pro-2-free open subgroup $\mathcal{G}_L$ of index 2 in $\mathcal{G}'_K$.

As in [Jo], the results of W. Herfort and P. Zalesskii (cf. [HZ, Th. 0.2]) give the existence of a finite family $(\mathcal{F}_i)_{i=0,\dots,k}$ of free pro-2-groups on respectively $d_0, \dots, d_k$ generators (where k is the number of conjugacy classes of subgroups of order 2 in $\mathcal{G}'_K$), such that:

$$\mathcal{G}'_K \simeq \mathcal{F}_0 \circledast \Big(\mathop{\circledast}_{i=1}^{k} (\mathcal{F}_i \times \mathbb{Z}/2\mathbb{Z}) \Big).$$

In particular, the abelianisation $\mathcal{G}_K'^{ab}$ of $\mathcal{G}_K'$ admits the direct decomposition:

$$\mathcal{G}_K'^{ab} \simeq \mathbb{Z}_2^{d_0} \oplus \Big(\bigoplus_{i=1}^{k} \big(\mathbb{Z}_2^{d_i} \oplus \mathbb{Z}/2\mathbb{Z}\big)\Big) \simeq \mathbb{Z}_2^{d_0+d_1+\cdots+d_k} \oplus (\mathbb{Z}/2\mathbb{Z})^k.$$

Since the 2-rational field K satisfies the Leopoldt conjecture, we get $\sum_{i=0}^{k} d_i = 1 + c_K$ as well as the isomorphism $\mathcal{T}_K' := \mathrm{tor}_{\mathbb{Z}_2}(\mathcal{G}_K'^{ab}) \simeq (\mathbb{Z}/2\mathbb{Z})^k$. Moreover $\mathcal{T}_K := \mathrm{tor}_{\mathbb{Z}_2}(\mathcal{G}_K^{ab}) = 1$, so that $\mathcal{T}_K'$ is generated by the decomposition groups of the real places of K which are deployed, a key argument of class field theory (cf. [Ja], [G_3, III.4.1.5], or [MN, 2.5] in the ℓ-rational case) giving $k = r_K$.

Now the pro-2-decomposition of $\mathcal{G}_K'$ clearly shows that the minimal number of generators $d(\mathcal{G}_K')$ and of relations $r(\mathcal{G}_K')$, defining $\mathcal{G}_K'$ as a pro-2-group, are:

$$d(\mathcal{G}_K') = k + \sum_{i=0}^{k} d_i = r_K + 1 + c_K \quad \text{and} \quad r(\mathcal{G}_K') = \sum_{i=1}^{k} (1 + d_i) = d(\mathcal{G}_K') - d_0.$$

It is well known by many authors (cf. e.g. [G_3, App., Th. 2.2, (i)]) that one has[2]:

$$d(\mathcal{G}_K') - r(\mathcal{G}_K') = \dim_{\mathbb{F}_2}\big(H^1(\mathcal{G}_K', \mathbb{F}_2)\big) - \dim_{\mathbb{F}_2}\big(H^2(\mathcal{G}_K', \mathbb{F}_2)\big) = 1 + c_K.$$

Thus we obtain $d_0 = 1 + c_K$, giving $d_i = 0$ for $1 \leqslant i \leqslant k$, then the expected result. □

References

[G_1] G. Gras, Logarithme p-adique et groupes de Galois, J. Reine Angew. Math. 343 (1983) 64–80.
[G_2] G. Gras, Remarks on K_2 of number fields, J. Number Theory 23 (1986) 64–80.
[G_3] G. Gras, Class Field Theory: From Theory to Practice, Springer Monogr. Math., Springer, 2003; second corrected printing 2005.
[GJ] G. Gras, J.-F. Jaulent, Sur les corps de nombres réguliers, Math. Z. 202 (1989) 343–365.
[HZ] W. Herfort, P. Zalesskii, Finitely generated pro-2-groups with a free subgroup of index 2, Manuscripta Math. 93 (1997) 457–464.
[Ja] J.-F. Jaulent, Théorie ℓ-adique globale du corps de classes, J. Théor. Nombres Bordeaux 10 (1998) 355–397.
[JN] J.-F. Jaulent, T. Nguyen Quang Do, Corps p-rationnels, corps p-réguliers et ramification restreinte, J. Théor. Nombres Bordeaux 5 (1993) 343–365.
[JS_1] J.-F. Jaulent, O. Sauzet, Pro-ℓ-extensions de corps de nombres $\mathfrak{l}$-rationnels, J. Number Theory 65 (1997) 240–267, J. Number Theory 80 (2000) 318–319.
[JS_2] J.-F. Jaulent, O. Sauzet, Extensions quadratiques 2-birationnelles de corps totalement réels, Publ. Mat. 44 (2000) 343–351.
[Jo] J. Jossey, Galois 2-extensions unramified outside 2, J. Number Theory 124 (2007) 42–76.
[Mi] H. Miki, On the Leopoldt conjecture on the p-adic regulators, J. Number Theory 26 (1987) 117–128.
[MN] A. Movahhedi, T. Nguyen Quang Do, Sur l'arithmétique des corps de nombres p-rationnels, in: Sém. Théor. Nombres Paris (1987/1988), in: Progr. Math., vol. 89, 1990, pp. 155–200.
[NSW] J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of Number Fields, Grundlehren Math. Wiss., vol. 323, Springer-Verlag, 2000; second ed. 2008.
[Sa] I.R. Šafarevič, Extensions with prescribed ramification points, Publ. Math. Inst. Hautes Etudes Sci. 36 (1986) 71–95.
[W_1] K. Wingberg, On Galois groups of p-closed algebraic number fields with restricted ramification, J. Reine Angew. Math. 400 (1989) 185–202.
[W_2] K. Wingberg, On Galois groups of p-closed algebraic number fields with restricted ramification II, J. Reine Angew. Math. 416 (1991) 187–194.

[2] This argument is equivalent to the use of the formulas of Šafarevič (cf. [Sa] or [NSW, Th. 8.7.3]).