New York Journal of Mathematics

New York J. Math. **24** (2018) 1056–1067.

Genus theory and governing fields

Christian Maire

Abstract. In this note we develop an approach to genus theory for a Galois extension L/K of number fields by introducing some governing field. When the restriction of each inertia group to the (local) abelianization is annihilated by a fixed prime number p, this point of view allows us to estimate the genus number of L/K with the aid of a subspace of the governing extension generated by some Frobenius elements. Then given a number field K and a possible genus number g, we derive information about the smallest prime ideals of K for which there exists a degree p cyclic extension L/K ramified only at these primes and having g as genus number.

Contents

1. Introduction

1.1. Let us start to recall a vague principle of genus theory in abelian extensions L/K of number fields: "the more L/K is ramified, the larger the class group of L must be". The reason is the following one: as we shall see, the genus field of L/K is related to the ray class field $K_{\mathfrak{m}}$ of K for a certain modulus $\mathfrak{m}$ built over the set of ramification of L/K; usually the ramification of $LK_{\mathfrak{m}}/K$ is absorbed in L/K, thus by class field theory the class group Cl(L) of L maps onto $\mathrm{Gal}(LK_{\mathfrak{m}}/L)$, and this last one "grows with $\mathfrak{m}$".

Let us introduce the objects more precisely. Let L/K be a Galois extension of number fields. Denote by K^H (resp. L^H) the Hilbert class field of K

Received September 7, 2018.

1991 *Mathematics Subject Classification.* 11R37, 11R29, 11R45.

Key words and phrases. Genus theory, governing field, Chebotarev density theorem.

The author was partially supported by the ANR project FLAIR (ANR-17-CE40-0012). This work has been done during a visit at Harbin Institute of Technology. The author thanks the Institute for Advanced in Mathematics of HIT for providing a beautiful research atmosphere.

ISSN 1076-9803/2018

(resp. of L), and consider $\mathrm{M}_{\mathrm{L}/\mathrm{K}}/\mathrm{K}$ the maximal abelian extension of K inside L^H/K. The compositum $\mathrm{K}^* := \mathrm{L}\mathrm{M}_{\mathrm{L}/\mathrm{K}}$ is called the *genus field* of the extension L/K, and the quantity $g^* = g(\mathrm{L}/\mathrm{K})^* = [\mathrm{K}^* : \mathrm{L}]$ its *genus number*. Let $\mathrm{L}^{ab} = \mathrm{M}_{\mathrm{L}/\mathrm{K}} \cap \mathrm{L}$ be the maximal abelian subextension of L/K. Then the relation

$$g^* = \frac{|\mathrm{Cl}(\mathrm{K})|}{[\mathrm{L}^{ab} : \mathrm{K}]} \cdot [\mathrm{M}_{\mathrm{L}/\mathrm{K}} : \mathrm{K}^H]$$

shows that, when the class group of K is known, it is easy to pass from $g := g(\mathrm{L}/\mathrm{K}) = [\mathrm{M}_{\mathrm{L}/\mathrm{K}} : \mathrm{K}^H]$ to g^*.

Since the 1950's, genus theory has been studied and developed by many authors. But let us simply mention the initial works of Hasse [9], Leopoldt [13], Fröhlich [3], Furuta [4], Razar [17], etc. For a more recent development, see [5, Chapter IV, §4] for example.

The aim of this note is to develop a new point of view of genus theory in L/K by introducing some governing extension F/K thanks to Kummer duality. We then obtain that $g(\mathrm{L}/\mathrm{K})$ is related to the kernel of a morphism Θ_S involving some Frobenius elements in Gal(F/K). The quantity $g(\mathrm{L}/\mathrm{K})$ is more directly connected to Θ_S, so in what follows we consider g instead of g^*.

Our work has been inspired by the book of Gras [5, Chapter V], by [7], by [8], and by [16, §5].

1.2. To simplify the presentation of our first result, take a prime number $p > 2$ and let L/K be a tamely ramified abelian extension where all the inertia groups are annihilated by p. Denote by $S = \{\mathfrak{p}_1, \cdots, \mathfrak{p}_s\}$ the set of ramification of L/K. Put $\mathrm{K}' = \mathrm{K}(\mu_p)$ and $\mathrm{F} = \mathrm{K}'(\sqrt[p]{\mathcal{O}_\mathrm{K}^\times})$, where $\mathcal{O}_\mathrm{K}^\times$ is the group of units of the ring of integers $\mathcal{O}_\mathrm{K}$ of K: the number field F is *the governing field* of our study. For each prime ideal $\mathfrak{p} \in S$, choose a prime ideal $\mathfrak{P}$ in $\mathcal{O}_{\mathrm{K}'}$ above $\mathfrak{p}$ and put $\sigma_\mathfrak{p} := \sigma_\mathfrak{P}$, the Frobenius element at $\mathfrak{P}$ in $\mathrm{Gal}(\mathrm{F}/\mathrm{K}')$. Consider the morphism Θ_S defined as follows:

$$\begin{array}{rcl}\Theta_S : (\mathbb{F}_p)^s & \longrightarrow & \mathrm{Gal}(\mathrm{F}/\mathrm{K}') \\ (a_1, \cdots, a_s) & \mapsto & \displaystyle\prod_{i=1}^{s} \sigma_{\mathfrak{p}_i}^{a_i} .\end{array}$$

Typically, our point of view allows us to obtain the following:

Theorem 1.1. *Under the above assumptions, one has* $g(\mathrm{L}/\mathrm{K}) = \#\ker(\Theta_S)$.

In Section 3.4 we give a more general version of Theorem 1.1, but the one here shows clearly the flavor of our work: some relationship between the genus number of L/K and some Frobenius elements in a governing extension.

Before we present the next result, let us introduce more notation. If K is a number field, let $(r_{\mathrm{K},1}, r_{\mathrm{K},2})$ be its signature and put $r_\mathrm{K} = r_{\mathrm{K},1} + r_{\mathrm{K},2} - 1 + \delta_{\mathrm{K},p}$, where $\delta_{\mathrm{K},p} = 1$ or 0 according $\mu_p \subset \mathrm{K}$ or not, where μ_p is the group of pth roots of unity.

Definition 1.2. *Let p be a prime number and let S be a finite set of places of* K. *A degree p cyclic extension* L/K *is called S-totally ramified if S is exactly the set of ramification of* L/K.

One also obtains:

Theorem 1.3. *Let* K *be a number field. Let $s \geq 1$ and $k \geq 1$ be two integers such that $s - r_{\mathrm{K}} \leq k \leq s$, and let p be a prime number. Then there exist infinitely many sets S of places of* K *with $|S| = s$, such that there exists a degree p cyclic extension* L/K*, S-totally ramified, with $g(\mathrm{L}/\mathrm{K}) = p^k$. Moreover, assuming GRH,*

(i) *when p is fixed, a such set S can be chosen such that the absolute norm of each $\mathfrak{p} \in S$ is $O(s \log s)$.*
(ii) *when s is fixed, a such set S can be chosen such that the absolute norm of each $\mathfrak{p} \in S$ is $O(p^{2r_{\mathrm{K}}+2}(\log p)^2)$.*

1.3. This note contains four sections. In §2 we recall well-know results in genus theory. In §3 we present and develop the main idea of this note: to connect the genus number of a Galois extension L/K, where the restriction of each inertia group to the abelianization of the local extension is annihilated by a fixed prime number p, to the kernel of some morphism Θ_S involving some Frobenius elements; when the extension L/K is abelian and the ramification is tame, we recover Theorem 1.1. In the last section we prove Theorem 1.3.

We introduce some additional notation before proceeding to the next section. Let p be a prime number. For every finitely generated $\mathbb{Z}$-module A, we denote by $d_p A := \dim_{\mathbb{F}_p} \mathbb{F}_p \otimes A$, the p-rank of A.

We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. If K is a number field and $v|\ell$ (possibly $\ell = \infty$) a place of K, we denote by K_v the completion of K at v. We then also fix an embedding ι_v of $\mathbb{Q}$ in $\overline{\mathbb{Q}_\ell}$ such that $\iota_v(\mathrm{K})\mathbb{Q}_\ell = \mathrm{K}_v$; if L/K is an extension of number fields we put $\mathrm{L}_v := \iota_v(\mathrm{L})\mathbb{Q}_\ell$.

If K_v is a local field, we denote by v_{K_v} the normalized valuation of K_v, and by $\mathcal{U}_{\mathrm{K}_v} = \{x \in \mathrm{L}_v, v_{\mathrm{K}_v}(x) > 0\}$ the groups of units of K_v. When there is no possible confusion, we write v for the valuation and $\mathcal{U}_v$ for the units.

If $\mathrm{K}_v = \mathbb{R}$ or $\mathbb{C}$, we put $\mathcal{U}_v = \mathrm{K}_v^\times$.

Acknowledgments. The author thanks Georges Gras for encouragement and constructive observations, Philippe Lebacque for stimulating exchanges, and the anonymous referee for the careful reading of the paper.

2. Genus theory: basic results

2.1. Genus field and ray class field. Let L/K be a Galois extension of number fields of set of ramification T. For a place v of K, denote by $\mathrm{D}_v := \mathrm{Gal}(\mathrm{L}_v/\mathrm{K}_v)$ the local Galois group at v, and consider $\mathrm{D}_v^{ab} = \mathrm{Gal}(\mathrm{L}_v^{ab}/\mathrm{K}_v)$ the abelianization of D_v, where here $\mathrm{L}_v^{ab}/\mathrm{K}_v$ is the maximal abelian subextension of $\mathrm{L}_v/\mathrm{K}_v$. Let $\mathrm{I}_v := \mathrm{I}(\mathrm{L}_v/\mathrm{K}_v) \subset \mathrm{D}_v$ be the inertia subgroup, and $\mathrm{I}_v^{ab} :=$

$\mathrm{I}(\mathrm{L}_v^{ab}/\mathrm{K}_v)$ be the restriction of I_v to L_v^{ab}. If v is an archimedean place, one always has $\mathrm{I}_v = \mathrm{D}_v \simeq \mathrm{D}_v^{ab}$.

Let $\mathrm{W}_v \subset \mathcal{U}_v := \mathcal{U}_{\mathrm{K}_v}$ be the kernel of the Artin map $\mathrm{Art}_{\mathrm{L}_v/\mathrm{K}_v} : \mathcal{U}_v \longrightarrow \mathrm{I}_v^{ab}$. Of course, $\mathrm{W}_v = \mathrm{N}_{\mathrm{L}_v/\mathrm{K}_v}\mathcal{U}_{\mathrm{L}_v}$, where $\mathrm{N}_{\mathrm{L}_v/\mathrm{K}_v}$ is the norm map of $\mathrm{L}_v/\mathrm{K}_v$. Clearly, $\mathrm{W}_v = \mathcal{U}_v$ when v is unramified in L/K.

Denote by $\mathrm{K}_\mathfrak{m}$ the ray class field of K corresponding by the global Artin map to the group of idèles $\mathrm{W} := \prod_v \mathrm{W}_v$.

Let $S := \{v \in T,\ \mathrm{I}_v^{ab} \neq \{1\}\}$ be the set of places v of K for which I_v^{ab} is not trivial. Put $\mathcal{U}_S := \prod_{v\in S} \mathcal{U}_v$ and $\mathrm{W}_S = \prod_{v \in S} \mathrm{W}_v$. The following proposition may be found in [4, Proposition 1]:

Proposition 2.1. *One has* $\mathrm{M}_{\mathrm{L/K}} = \mathrm{K}_\mathfrak{m}$. *Moreover,*

$$\mathrm{Gal}(\mathrm{K}_\mathfrak{m}/\mathrm{K}^H) \simeq \mathcal{U}_S/\iota_S(\mathcal{O}_\mathrm{K}^\times)\mathrm{W}_S,$$

where ι_S *is the natural embedding.*

Proof. One has $\mathrm{M}_{\mathrm{L/K}} \subset \mathrm{K}_\mathfrak{m}$. Indeed, take a place v of K and $\varepsilon \in \mathrm{W}_v$. Then ε is a norm in $\mathrm{L}_v/\mathrm{K}_v$ of some unit ε_0 in L_v. As $\mathrm{M}_{\mathrm{L/K}}\mathrm{L}/\mathrm{L}$ is unramified at v, the unit ε_0 is a norm in the local extension $(\mathrm{M}_{\mathrm{L/K}})_v\mathrm{L}_v/\mathrm{L}_v$, and then ε is a norm in $(\mathrm{M}_{\mathrm{L/K}})_v\mathrm{L}_v/\mathrm{K}_v$, which implies that $\mathrm{Art}_{(\mathrm{M}_{\mathrm{L/K}})_v/\mathrm{K}_v}(\varepsilon)$ is trivial. Then the global Artin map of the extension $\mathrm{M}_{\mathrm{L/K}}/\mathrm{K}$ vanishes on W, and thus $\mathrm{M}_{\mathrm{L/K}} \subset \mathrm{K}_\mathfrak{m}$ by maximality of $\mathrm{K}_\mathfrak{m}$.

Moreover $\mathrm{K}_\mathfrak{m}\mathrm{L}/\mathrm{L}$ is an unramified abelian extension. Indeed, for every place v of K, the local Artin symbol indicates that $\mathcal{U}_v/\mathrm{W}_v \twoheadrightarrow \mathrm{I}((\mathrm{K}_\mathfrak{m})_v/\mathrm{K}_v)$ and that $\mathrm{I}_v^{ab} = \mathrm{I}(\mathrm{L}_v/\mathrm{K}_v)^{ab} \simeq \mathcal{U}_v/\mathrm{W}_v$. By the property of the Artin symbol, one then has $\mathrm{I}(\mathrm{L}_v^{ab}(\mathrm{K}_\mathfrak{m})_v/\mathrm{K}_v) \simeq \mathcal{U}_v/\mathrm{W}_v$, thus $\mathrm{I}(\mathrm{L}_v^{ab}(\mathrm{K}_\mathfrak{m})_v/\mathrm{L}_v^{ab}) = \{1\}$ and $(\mathrm{K}_\mathfrak{m})_v\mathrm{L}_v/\mathrm{L}_v$ is unramified. By maximality of $\mathrm{M}_{\mathrm{L/K}}$ one deduces that $\mathrm{K}_\mathfrak{m} \subset \mathrm{M}_{\mathrm{L/K}}$, and finally that $\mathrm{M}_{\mathrm{L/K}} = \mathrm{K}_\mathfrak{m}$.

By class field theory one has

$$\mathrm{Gal}(\mathrm{K}_\mathfrak{m}/\mathrm{K}^H) \simeq \prod_v \mathcal{U}_v/\iota(\mathcal{O}_\mathrm{K}^\times)\mathrm{W} \simeq \mathcal{U}_T/\iota_T(\mathcal{O}_\mathrm{K}^\times)\mathrm{W}_T,$$

where $\iota : \mathcal{O}_\mathrm{K}^\times \to \prod_v \mathcal{U}_v$ is the natural embedding. To conclude, observe that for $v \in T\backslash S$, $\mathcal{U}_v = \mathrm{W}_v$, and then $\mathcal{U}_T/\mathrm{W}_T \simeq \mathcal{U}_S/\mathrm{W}_S$. □

2.2. Formula and exact sequence in genus theory. If L/K is a Galois extension, denote by $\mathcal{O}_\mathrm{K}^\times \cap \mathrm{N}_{\mathrm{L/K}}$ the units $\mathcal{O}_\mathrm{K}^\times$ of $\mathcal{O}_\mathrm{K}$ that are local norms in L/K.

Theorem 2.2. *Let* L/K *be a Galois extension of number fields of set of ramification* T. *One has*

(i) *the genus formula:*

$$g(\mathrm{L/K}) = \frac{\displaystyle\prod_{v\in T} \#\mathrm{I}_v^{ab}}{(\mathcal{O}_\mathrm{K}^\times : \mathcal{O}_\mathrm{K}^\times \cap \mathrm{N}_{\mathrm{L/K}})},$$

(ii) *the genus exact sequence:*

$$1 \longrightarrow \mathcal{O}_{\mathrm{K}}^{\times}/\mathcal{O}_{\mathrm{K}}^{\times} \cap \mathrm{N}_{\mathrm{L}/\mathrm{K}} \longrightarrow \prod_{v\in T} \mathrm{I}_v^{ab} \longrightarrow \mathrm{Gal}(\mathrm{M}_{\mathrm{L}/\mathrm{K}}/\mathrm{K}^H) \longrightarrow 1.$$

For the proof of Theorem 2.2, see for example [5, Chapter IV, §4]. See also [14].

Corollary 2.3. *Let* L/K *be a Galois extension where all the* I_v^{ab} *are annihilated by a fixed prime number* p*. Then* $\mathrm{Gal}(\mathrm{M}_{\mathrm{L}/\mathrm{K}}/\mathrm{K}^H)$ *is of exponent* p*.*

Remark 2.4. *Let us recall at least two applications of the genus exact sequence:*

(i) *the construction of number fields having an infinite Hilbert* p*-class field tower (see for example* [18]*);*
(ii) *the study of Greenberg's conjecture for totally real number fields (see for example the recent work of Gras* [6]*).*

Remark 2.5. *For genus theory in more general contexts see for example* [5, Chapter IV, §4]*,* [11, Chapter III, §2] *or* [14]*.*

3. Kummer theory and governing field

Let L/K be a Galois extension of set of ramification T. We keep the notations of §2 (see also the last few paragraphs of Section 1).

From now on, we assume that all the inertia groups I_v^{ab} *are annihilated by a fixed prime number* p*.*

Put $S := \{v \in T,\ \mathrm{I}_v^{ab} \neq \{1\}\}$ and let us write $S = S_0^{ta} \cup S_0^{wi} \cup S_\infty$, where S_0^{ta} is the set of finite places of S coprime to p (called tame places), S_0^{wi} is the set of places S dividing p (called wild places), and S_∞ contains the ramified archimedean places. In particular $S_\infty = \emptyset$ when $[\mathrm{L} : \mathrm{K}]$ is odd. Observe that by hypothesis, for $v \in S_0^{ta}$, the local field K_v contains the p-roots of the unity. Put

$$s = \#S_\infty + \#S_0^{ta} + \sum_{v\in S_0^{wi}} d_p \mathrm{I}_v^{ab}.$$

Remark 3.1. *Following Section 2.1, for each place* v *of* K *one has* $\mathcal{U}_v^p \subset \mathrm{W}_v$*; for* $v \in S_0^{ta} \cup S_\infty$ *one even has* $\mathrm{W}_v = \mathcal{U}_v^p$*.*

3.1. Governing field. Fix now $\zeta \in \overline{\mathbb{Q}}$, a primitive pth root of the unity, and put $\mu_p = \langle \zeta \rangle$.

Let us consider the number fields $\mathrm{K}' = \mathrm{K}(\zeta)$ and $\mathrm{F} = \mathrm{K}'(\sqrt[p]{\mathcal{O}_{\mathrm{K}}^{\times}})$: the field F is the *governing field* of our study. First, we give an upper bound for the absolute value of the discriminant d_{F} of F.

Proposition 3.2. *One has*

$$|\mathrm{d}_{\mathrm{F}}| \leq |\mathrm{d}_{\mathrm{K}}|^{(p-1)p^{r_{\mathrm{K}}}} \cdot p^{[\mathrm{K}:\mathbb{Q}](p-1)(4p^{r_{\mathrm{K}}}-3)}.$$

Proof. Observe that F/K is unramified outside p. For a better readability of the proof, we change a little bit the principle of notations for local extensions followed since the beginning. Let $v|p$ be a wild place of K, and let $w|v$ be a place of K' above v. Denote by w the normalized valuation of K'_w, and by e_w (respectively f_w) the absolute ramification index (resp. inertia degree) of w.

Let us start to recall that the w-valuation of the conductor of a local degree p cyclic extension $\mathrm{L}_w/\mathrm{K}'_w$ is less than $1+2e_w$ (indeed, every unit $\varepsilon \in \mathrm{K}'_w$ such that $w(\varepsilon-1) \geq 1+2e_w$ is a pth power). By the conductor-discriminant formula (see for example [15, Chapter VII, §12, Theorem 11.9]) we get

$$w(\mathrm{disc}(\mathrm{F}_w/\mathrm{K}'_w)) \leq (1+2e_w)(p^{r_\mathrm{K}}-1).$$

Hence by the discriminants formula in a tower of number fields (see for example [15, hapter III, §2, Corollary 2.10]), we finally obtain

$$(1)\quad |\mathrm{d_F}| \leq |\mathrm{d_{K'}}|^{[\mathrm{F}:\mathrm{K}']} \cdot p^{\sum_{w|p}(1+2e_w)f_w(p^{r_\mathrm{K}}-1)} \leq |\mathrm{d_{K'}}|^{p^{r_\mathrm{K}}} \cdot p^{3(p-1)(p^{r_\mathrm{K}}-1)[\mathrm{K}:\mathbb{Q}]},$$

where here the sum is taken over the places w of K' above p.

The extension K'/K is tamely ramified (the v-valuation of the conductor is ≤ 1) and then

$$(2)\qquad |\mathrm{d_{K'}}| = |\mathrm{d_K}|^{[\mathrm{K}':\mathrm{K}]} \cdot p^{\sum_{v|p} f_v \sum_{w|v} f(w/v)(e(w|v)-1)} \leq \left(|\mathrm{d_K}| \cdot p^{[\mathrm{K}:\mathbb{Q}]}\right)^{p-1},$$

where the sum is taken over the wild places v of K, and $e(w|v) = e_w/e_v$ (resp. $f(w|v) = f_w/f_v$) is the ramification index (resp. inertia degree) of v in K'/K.

Inequalities (1) and (2) then allow us to conclude. □

If M is a $\mathbb{F}_p$-module, put $\mathrm{M}^\vee := \hom(\mathrm{M}, \mu_p)$. Let

$$\psi : (\mathcal{O}_\mathrm{K}^\times/(\mathcal{O}_\mathrm{K}^\times)^p)^\vee \to \mathrm{Gal}(\mathrm{F}/\mathrm{K}')$$

be the isomorphism issue from Kummer duality. Let us recall how this isomorphism works: for $\chi \in (\mathcal{O}_\mathrm{K}^\times/(\mathcal{O}_\mathrm{K}^\times)^p)^\vee$ one associates the element $\sigma_\chi := \psi(\chi) \in \mathrm{Gal}(\mathrm{F}/\mathrm{K}')$ defined as follows:

$$\sigma_\chi(\sqrt[p]{\varepsilon}) = \chi(\varepsilon) \cdot \sqrt[p]{\varepsilon}.$$

For more details see for example [5, Chapter I, §6, exercice 6.2.2].

3.2. Tame places and Frobenius elements. Let us take $v \in S_0^{ta}$. As before (see the last few paragraphs of Section 1), we fix an embedding $\iota_v : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ such that $\iota_v(\mathrm{K})\mathbb{Q}_p = \mathrm{K}_v$. Observe that $\mathrm{K}_v = \mathrm{K}'_v$. Let us denote by σ_v $(= \sigma_{v_{\mathrm{K}'}})$ the Frobenius of $v_{\mathrm{K}'}$ in $\mathrm{Gal}(\mathrm{F}/\mathrm{K}')$.

Let $\mathrm{N}(v_{\mathrm{K}'})$ be the order of the residue field of K'_v. Take now $\zeta_v \in \mathcal{U}_v$ such that $\zeta_v^{(\mathrm{N}(v_{\mathrm{K}'})-1)/p} = \iota_v(\zeta)$ and consider the generator χ_v of $(\mathcal{U}_v/\mathcal{U}_v^p)^\vee$ defined by $\chi_v(\zeta_v) = \zeta$. Thanks to ι_v, the character χ_v can be viewed as an element of $(\mathcal{O}_\mathrm{K}^\times/(\mathcal{O}_\mathrm{K}^\times)^p)^\vee$.

Proposition 3.3. *One has* $\psi(\chi_v \circ \iota_v) = \sigma_v$.

Proof. Put $\sigma = \psi(\chi_v \circ \iota_v)$ and take $\varepsilon \in \mathcal{O}_{\mathrm{K}}^{\times}$. Let $a_v(\varepsilon) \in \mathbb{F}_p$ such that $\iota_v(\varepsilon)\mathcal{U}_v^p = \zeta_v^{a_v(\varepsilon)}\mathcal{U}_v^p$. Then by Kummer theory,

$$\sigma(\sqrt[p]{\varepsilon})/\sqrt[p]{\varepsilon} = \chi_v(\iota_v(\varepsilon)) = \zeta^{a_v(\varepsilon)}.$$

But by definition, the Frobenius element σ_v satisfies the property:

$$\sigma_v(\sqrt[p]{\varepsilon})/\sqrt[p]{\varepsilon} \equiv \varepsilon^{(\mathrm{N}(v_{\mathrm{K}'}))-1)/p} \pmod{v_{\mathrm{K}'}}.$$

Here $a \equiv b \pmod{v_{\mathrm{K}'}}$ means that $v_{\mathrm{K}'}(a-b) > 0$. Hence

$$\iota_v\Big(\sigma_v(\sqrt[p]{\varepsilon})/\sqrt[p]{\varepsilon}\Big) \equiv \iota_v(\zeta^{a_v(\varepsilon)}) \pmod{v_{\mathrm{K}'}},$$

which shows that $\sigma(\sqrt[p]{\varepsilon}) = \sigma_v(\sqrt[p]{\varepsilon})$. □

Remark 3.4. *If we choose another embedding $\iota_{v'} : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_\ell}$ (instead of ι_v), then by Kummer duality and by the property of the Artin symbol, one has $\sigma_{v'} = \sigma_v^a$ for some $a \in \mathbb{F}_p^{\times}$.*

3.3. The other places.

3.3.1. Wild places. Here now take $v|p$. Recall that $\mathrm{I}_v \simeq (\mathbb{Z}/p\mathbb{Z})^{a_v}$. By the Artin map and by Kummer duality, one has

$$\mathrm{I}_v^{\vee} \simeq (\mathcal{U}_v/\mathrm{W}_v)^{\vee} \hookrightarrow (\mathcal{U}_v/\mathcal{U}_v^p)^{\vee}.$$

Then take an $\mathbb{F}_p$-basis $\{\chi_v^{(i)}, i = 1, \cdots, a_v\}$ of $(\mathcal{U}_v/\mathrm{W}_v)^{\vee}$. For $i = 1, \cdots, a_v$, consider $\sigma_v^{(i)} \in \mathrm{Gal}(\mathrm{F}/\mathrm{K}')$ defined as follows: for $\varepsilon \in \mathcal{O}_{\mathrm{K}}^{\times}$ put

$$\sigma_v^{(i)}(\sqrt[p]{\varepsilon}) = \chi_v^{(i)}(\iota_v(\varepsilon)) \cdot \sqrt[p]{\varepsilon}.$$

3.3.2. Infinite places. Take $p = 2$ and let v be a real place of K. Here $\mathcal{U}_v/\mathcal{U}_v^2 \simeq \mathbb{R}^{\times}/\mathbb{R}^{\times,+}$. Then for $\varepsilon \in \mathcal{O}_{\mathrm{K}}^{\times}$ put

$$\sigma_v(\sqrt{\varepsilon}) = \mathrm{sign}(\iota_v(\varepsilon))\sqrt{\varepsilon},$$

where $\mathrm{sign}(\iota_v(\varepsilon))$ is the sign of the embedding $\iota_v(\varepsilon)$ of ε in K_v. Of course $\sigma_v = \sigma_{\chi_v}$, where χ_v is the non trivial character of $\mathcal{U}_v/\mathcal{U}_v^2$.

3.4. Key map and main result.

Let Θ_S be the linear map

$$\Theta_S : (\mathcal{U}_S/\mathrm{W}_S)^{\vee} \to \mathrm{Gal}(\mathrm{F}/\mathrm{K}')$$

defined as follows:

(*i*) for $v \in S_0^{ta} \cup S_\infty$, put $\Theta_S(\chi_v) = \sigma_v$,

(*ii*) for $v \in S_0^{wi}$, put $\Theta_S(\chi_v^{(i)}) = \sigma_v^{(i)}$.

While fixing an isomorphism $\mathrm{Gal}(\mathrm{F}/\mathrm{K}') \simeq \mathbb{F}_p^{r_{\mathrm{K}}}$ we see that Θ_S is a linear map from $\mathbb{F}_p^s$ to $\mathbb{F}_p^{r_{\mathrm{K}}}$.

Theorem 3.5. *Under the assumptions of section 3, the Artin map induces the isomorphism* $\ker(\Theta_S) \simeq \mathrm{Gal}(\mathrm{K}_{\mathfrak{m}}/\mathrm{K}^H)^{\vee}$.

Proof. Let us start with the exact sequence (see Proposition 2.1)

$$1 \longrightarrow \iota_S(\mathcal{O}_{\mathrm{K}}^\times/(\mathcal{O}_{\mathrm{K}}^\times)^p) \longrightarrow \mathcal{U}_S/\mathrm{W}_S \longrightarrow \mathrm{Gal}(\mathrm{K}_\mathfrak{m}/\mathrm{K}^H) \longrightarrow 1$$

and take its Kummer dual to obtain

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(\mathrm{K}_\mathfrak{m}/\mathrm{K}^H)^\vee & \longrightarrow & (\mathcal{U}_S/\mathrm{W}_S)^\vee & \longrightarrow & (\iota_S(\mathcal{O}_{\mathrm{K}}^\times/(\mathcal{O}_{\mathrm{K}}^\times)^p)^\vee & \longrightarrow & 1 \\ & & & & \downarrow & & \downarrow & & \\ & & & & \mathrm{Gal}(\mathrm{F}/\mathrm{K}') & \xleftarrow[\psi]{\simeq} & (\mathcal{O}_{\mathrm{K}}^\times/(\mathcal{O}_{\mathrm{K}}^\times)^p)^\vee. & & \end{array}$$

Observe that

$$(\mathcal{U}_S/\mathrm{W}_S)^\vee \simeq \prod_{v\in S_0^{ta}\cup S_\infty} (\mathcal{U}_v/\mathcal{U}_v^p)^\vee \prod_{v\in S_0^{wi}} (\mathcal{U}_v/\mathrm{W}_v)^\vee .$$

Thus, by Proposition 3.3 and sections 3.3.1 and 3.3.2, the induced map from $(\mathcal{U}_S/\mathrm{W}_S)^\vee$ to $\mathrm{Gal}(\mathrm{F}/\mathrm{K}')$ is exactly Θ_S. Hence we get:

$$\mathrm{Gal}(\mathrm{K}_\mathfrak{m}/\mathrm{K}^H)^\vee \simeq \ker\left((\mathcal{U}_S/\mathrm{W}_S)^\vee \xrightarrow{\Theta_S} \mathrm{Gal}(\mathrm{F}/\mathrm{K}')\right).$$

The proof is complete. □

Corollary 3.6. *One has* $g(\mathrm{L}/\mathrm{K}) = \#\ker(\Theta_S)$. *In particular,*

$$s - r_{\mathrm{K}} \leq d_p\mathrm{Gal}(\mathrm{M}_{\mathrm{L}/\mathrm{K}}/\mathrm{K}^H) \leq s.$$

Proof. This is a consequence of Theorem 3.5 and Proposition 2.1. □

Observe that Theorem 1.1 is a consequence of Corollary 3.6.

3.5. Examples.

3.5.1. Imaginary quadratic fields. Take $p=2$ and let $\mathrm{L}/\mathbb{Q}$ be an imaginary quadratic extension of discriminant d. The field $\mathrm{F} = \mathbb{Q}(\sqrt{-1})$ is the governing field and, thanks to $S_\infty = \{v_\infty\}$, the map Θ_S is onto. Then $g(\mathrm{L}/\mathbb{Q}) = 2^s$ and $g^* = 2^{s-1}$, where s is the number of primes dividing d.

3.5.2. Real quadratic fields. Take $p=2$ and let $\mathrm{L}/\mathbb{Q}$ be a real quadratic extension of discriminant d. Here $S_\infty = \emptyset$ and $\mathrm{F} = \mathbb{Q}(\sqrt{-1})$ is the governing field. Then Θ_S is the zero map if and only if every odd prime ℓ dividing d is congruent to $1 (\mathrm{mod}\ 4)$; in this case $g = 2^s$. Otherwise Θ_S is onto and $g = 2^{s-1}$, where s is the number of primes dividing d.

3.5.3. Cubic fields. As studied in [1] and [2], the situation where $p=3$, $\mathrm{K} = \mathbb{Q}(\mu_3)$ and $\mathrm{L} = \mathrm{K}(\sqrt[3]{d})$, $d \in \mathbb{Z}_{\geq 1}$, is also interesting to describe. Indeed in this case the governing extension is the extension $\mathbb{Q}(\mu_9)/\mathbb{Q}(\mu_3)$. Here $s-2 \leq d_3\mathrm{Gal}(\mathrm{K}^*/\mathrm{L}) \leq s-1$, and to have the exact value of $d_3\mathrm{Gal}(\mathrm{K}^*/\mathrm{L})$, one needs to determine: (i) the number s of prime ideals $\mathfrak{p}$ in $\mathcal{O}_{\mathrm{K}}$ ramified in L/K, and (ii) if the map Θ_S is trivial or not (here $d_3\mathrm{Im}(\Theta_S) \leq 1$). And these two conditions are characterized by the congruences in $\mathbb{Z}/9\mathbb{Z}$ of the prime numbers ℓ that divide d. Typically, if there exists a prime number $\ell|d$, $\ell \neq 3$, such that 3 divides the order of ℓ in $(\mathbb{Z}/9\mathbb{Z})^\times$, then $\mathrm{Im}(\Theta_S) \simeq \mathbb{F}_3$.

4. Proof of Theorem 1.3

Let $s, k \in \mathbb{Z}_{>0}$ such that $s - r_\mathrm{K} \leq k \leq s$. Put $n = s - k$.

First, one has to enlarge the governing field $\mathrm{F} = \mathrm{K}'(\sqrt[p]{\mathcal{O}_\mathrm{K}^\times})$ by considering the number field

$$\widetilde{\mathrm{F}} := \mathrm{F}(\sqrt[p]{a_1}, \cdots, \sqrt[p]{a_h}),$$

where the a_i's are such that $a_i\mathcal{O}_\mathrm{K} = \mathfrak{a}_i^p \in \mathrm{Cl}(\mathrm{K})$ and the family $\{\mathfrak{a}_1, \cdots, \mathfrak{a}_h\}$ forms an $\mathbb{F}_p$-basis of $\mathrm{Cl}(\mathrm{K})[p]$ (the classes annihilated by p). One has $[\widetilde{\mathrm{F}} : \mathrm{K}'] = p^{r_\mathrm{K}+h}$. Let us fix an $\mathbb{F}_p$-basis $(e_i)_{i=1,\cdots,r_\mathrm{K}}$ of

$$\mathrm{Gal}(\widetilde{\mathrm{F}}/\mathrm{K}'(\sqrt[p]{a_1}, \cdots, \sqrt[p]{a_h})) \simeq (\mathbb{F}_p)^{r_\mathrm{K}}$$

and complete this basis to an $\mathbb{F}_p$-basis $(e_i)_{i=1,\cdots,r_\mathrm{K}+h}$ of $\mathrm{Gal}(\widetilde{\mathrm{F}}/\mathrm{K}') \simeq (\mathbb{F}_p)^{r_\mathrm{K}+h}$. By the Chebotarev density theorem, let $S = \{v_1, \cdots, v_s\}$ be a set of s different tame places of K such that the Frobenius elements $\sigma_{v_i} \in \mathrm{Gal}(\widetilde{\mathrm{F}}/\mathrm{K}') \subset \mathrm{Gal}(\widetilde{\mathrm{F}}/\mathrm{K})$ of v_i satisfy:

(a) $\sigma_{v_1} = -(e_1 + \cdots + e_n)$;
(b) for $i = 2, \cdots, n+1$, $\sigma_{v_i} = e_{i-1}$;
(c) for $i = n+2, \cdots, s$, $\sigma_{v_i} = 0$,

when $n \geq 1$. When $n = 0$, choose the v_i's such that $\sigma_{v_i} = 0$, $i = 1, \cdots, s$.

Observe that $\displaystyle\sum_{i=1}^{s} \sigma_{v_i} = 0$. Then by a result of Gras-Munnier [7, Theorem 1.1] (see also [5, Chapter V, §2, Corollary 2.4.2]), there exists a degree p cyclic extension L/K, S-totally ramified. Moreover, by the choice of the e_i's and the v_i's the morphism Θ_S, with value in $\mathrm{Gal}(\mathrm{F}/\mathrm{K}')$, is of rank n. Then $\mathrm{Gal}(\mathrm{M}_{\mathrm{L}/\mathrm{K}}/\mathrm{K}) \simeq (\mathbb{F}_p)^{s-n} = (\mathbb{F}_p)^k$ by Corollary 3.6, which proves (i) of Theorem 1.3.

Before we prove (ii) of Theorem 1.3, let us make the following observation:

Lemma 4.1. *One has* $\log|\mathrm{d}_{\widetilde{\mathrm{F}}}| \leq 2|\mathrm{Cl}(\mathrm{K})|\log|\mathrm{d}_\mathrm{F}|$.

Proof. Adapt Proposition 3.2. □

Remark 4.2. *Obviously one has* $\widetilde{\mathrm{F}} = \mathrm{F}$ *for* $p \gg 0$.

The second point (ii) is a consequence of an effective version of the Chebotarev density theorem under GRH (see for example [12, Theorem 1.1] or [19, §2.5, Theorem 4]). Observe first that when $n > 1$ or when $p > 2$, all the Frobenius elements of (a) and (b) are in different conjugacy classes. (When $n = 1$ and $p = 2$, the Frobenius of v_1 and of v_2 are in the same conjugacy class, see the next to solve the problem). We can be certain that there exist such primes (associated to places v_i) with norm of order $O\left((\log|\mathrm{d}_{\widetilde{\mathrm{F}}}|)^2\right) = O\left((\log|\mathrm{d}_\mathrm{F}|)^2\right)$.

For the places $v_{n+2}, \cdots, v_s$, we need the following two lemmas.

Lemma 4.3. *Given $m \in \mathbb{Z}_{\geq 1}$, there exist m prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_m$ in $\mathcal{O}_{\mathrm{K}}$ that split totally in $\widetilde{\mathrm{F}}/\mathrm{K}$, all having absolute norm less than $C_{\mathrm{K},p}m(\log m)$, where $C_{\mathrm{K},p}$ is some constant depending on* K *and on* p.

Proof. For $x \geq 2$ let

$$\pi(x) = \left|\{\text{prime ideals } \mathfrak{p} \subset \mathcal{O}_{\mathrm{K}}, |\mathcal{O}_{\mathrm{K}}/\mathfrak{p}| \leq x, \mathfrak{p} \text{ splits totally in } \widetilde{\mathrm{F}}/\mathrm{K}\}\right|.$$

Then the effective Chebotarev density theorem under GRH indicates that $\pi(x) \geq A(x)$, where

$$A(x) = \frac{1}{[\widetilde{\mathrm{F}}:\mathrm{K}]}\left(\frac{x}{\log(x)} - Cx^{1/2}(\log|\mathrm{d}_{\widetilde{\mathrm{F}}}| + [\widetilde{\mathrm{F}}:\mathbb{Q}]\log x)\right),$$

C being some absolute constant. Then, by Lemma 4.1 and Proposition 3.2, taking

$$x_0 = C_{\mathrm{K},p}m(\log m),$$

for some constant $C_{\mathrm{K},p}$ depending on K and on p we are certain that $A(x_0) \geq m$ and we are done. □

Lemma 4.4. *Given $m \in \mathbb{Z}_{\geq 1}$, there exist m prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_m$ in $\mathcal{O}_{\mathrm{K}}$ that split totally in $\widetilde{\mathrm{F}}/\mathrm{K}$, all having absolute norm less than*

$$C_{\mathrm{K},m}p^{2r_{\mathrm{K}}+2}(\log p)^2,$$

where $C_{\mathrm{K},m}$ is some constant depending on K *and on* m.

Proof. Observe that $\widetilde{\mathrm{F}}/\mathrm{K}$ is unramified outside p. Let ℓ be a prime number coprime to the set of ramification of $\widetilde{\mathrm{F}}/\mathbb{Q}$ and such that $\ell \geq m$. By Bertrand's postulate, this ℓ can be taken less than $C_{\mathrm{K}} \cdot m$, where C_{K} is some constant depending on K. Put $\mathrm{N} = \mathbb{Q}(\mu_\ell)$ and $\mathrm{N}_0 = \mathrm{N}\widetilde{\mathrm{F}}$. The extension $\mathrm{N}_0/\widetilde{\mathrm{F}}$ is of degree $\ell - 1$, and $|\mathrm{d}_{\mathrm{N}_0}| \leq |\mathrm{d}_{\widetilde{\mathrm{F}}}|^{\ell-1}|\mathrm{d}_{\mathrm{N}}|^{[\widetilde{\mathrm{F}}:\mathbb{Q}]}$. Let us choose now m prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_m$ in $\mathcal{O}_{\mathrm{K}}$, all unramified in N_0/K, such that their Frobenius in $\mathrm{Gal}(\mathrm{N}_0/\widetilde{\mathrm{F}}) \subset \mathrm{Gal}(\mathrm{N}_0/\mathrm{K})$ are in some different conjugacy classes: by the Chebotarev density theorem (under GRH), the $\mathfrak{p}_i$'s can be choosen of norm smaller than $C(\log|\mathrm{d}_{N_0}|)^2$, where C is some absolute constant. Hence by Lemma 4.1, for $i = 1, \cdots, m$, we obtain that the $\mathrm{N}(\mathfrak{p}_i)$'s are smaller than

$$C\left(\ell p^{r_{\mathrm{K}}+1}|\mathrm{Cl}(\mathrm{K})|[\mathrm{K}:\mathbb{Q}]\log(p^4\ell|\mathrm{d}_{\mathrm{K}}|^{2/[\mathrm{K}:\mathbb{Q}]})\right)^2 \leq C_{\mathrm{K},m}p^{2r_{\mathrm{K}}+2}(\log p)^2.$$

Finally to conclude, observe that each $\mathfrak{p}_i$ splits totally in F/K. □

References

[1] Aouissi, Siham; Mayer, Daniel C.; Ismaili, Moulay Chrif. Structure of relative genus fields of cubic Kummer extensions. Preprint, 2018. arXiv:1808.04678. 1063

[2] Aouissi, Siham; Mayer, Daniel C.; Ismaili, Moulay Chrif; Talbi, Mohamed; Azizi, Adbelmalek. 3-rank of ambiguous class groups in cubic Kummer extensions. Preprint, 2018. arXiv:1804.00767. 1063

[3] Fröhlich, A. The genus field and genus group in finite number fields I. *Mathematika* **6** (1959), 40–46. MR0113868, Zbl 0202.33005, doi: 10.1112/S0025579300001911. 1057

[4] Furuta, Yoshiomi. The genus field and genus number in algebraic number fields. *Nagoya Math. J.* **29** (1967), 281–285. MR0209260, Zbl 0166.05901, doi: 10.1017/S0027763000024387. 1057, 1059

[5] Gras, Georges. Class field theory. From theory to practice. Springer Monographs in Mathematics. *Springer-Verlag, Berlin*, 2003. xiv+491 pp. ISBN: 3-540-44133-6. MR1941965, Zbl 1019.11032, doi: 10.1007/978-3-662-11323-3. 1057, 1060, 1061, 1064

[6] Gras, Georges. Approche p-adique de la conjecture de Greenberg pour les corps totalement réels. *Ann. Math. Blaise Pascal* **24** (2017), no 2, 235–291. MR3734135, Zbl 06833072, doi: 10.5802/ambp.370. 1060

[7] Gras, Georges; Munnier, Adeline. Extensions cycliques T-totalement ramifiées. *Théorie des nombres, Années 1996/97–1997/98*, 16 pp., Publ. Math. UFR Sci. Tech. Besançon. *Univ. Franche-Comté, Besançon*, 1999. MR1735371. 1057, 1064

[8] Hajir, Farshid; Maire, Christian. Unramified subextensions of ray class field towers. *J. Algebra* **249** (2002), no. 2, 528–543. MR1901171, Zbl 1018.11058, doi: 10.1006/jabr.2001.9079. 1057

[9] Hasse, Helmut. Zur Geschlechtertheorie in quadratischen Zahlkörpern. *J. Math. Soc. Japan* **3** (1951), 45–51. MR0043828, Zbl 0043.04002, doi: 10.2969/jmsj/00310045. 1057

[10] Iyanaga, Shokichi; Tamagawa, Tsuneo. Sur la théorie du corps de classes sur le corps des nombres rationnels. *J. Math. Soc. Japan* **3** (1951), 220–227. MR0044575, Zbl 0043.04103, doi: 10.2969/jmsj/00310220.

[11] Jaulent, Jean-Franqis. L'arithmétique des ℓ-extensions. Dissertation, Université de Franche-Comté, Besanǫn, 1986. Théorie des nombres. Fasc. 1. 1984–1986. Publications Mathématiques de la Faculté des Sciences de Besançon. *Université de Franche-Comté, Faculté des Sciences, Besançon*, 1986. viii+349 pp. MR0859709, Zbl 0601.12002. 1060

[12] Lagarias, Jeffrey C.; Odlyzko, Andrew M. Effective versions of the Chebotarev density theorem. *Algebraic number fields: L-functions and Galois properties* (Proc. Sympos., Univ Durham, Durham 1975), 409–464. *Academic Press, London*, 1977. MR0447191, Zbl 0362.12011. 1064

[13] Leopoldt, Heinrich W. Zur Geschlechtertheorie in abelschen Zahlkörpern. *Math. Nachr.* **9** (1953), 351–362. MR0056032, Zbl 0053.35502, doi: 10.1002/mana.19530090604. 1057

[14] Maire, Christian. Finitude de tours et p-tours T-ramifiées modérées, S-décomposées. *J. Théor. Nombres Bordeaux* **8** (1996), no. 1, 47–73. MR1399946, Zbl 0877.11060, doi: 10.5802/jtnb.156. 1060

[15] Neukirch, Jürgen. Algebraic number theory. Grundlehren der Mathematischen Wissenschaften, 322. *Springer-Verlag, Berlin*, 1999. xviii+571 pp. ISBN: 3-540-65399-6. MR1697859, Zbl 0956.11021, doi: 10.1007/978-3-662-03983-0. 1061

[16] Ozaki, Manabu. Construction of maximal unramified p-extensions with prescribed Galois groups. *Invent. Math.* **183** (2011), no. 3, 649–680. MR2772089, Zbl 1232.11118, arXiv:0705.2293, doi: 10.1007/s00222-010-0289-0. 1057

[17] Razar, Michael J. Central and genus class fields and the Hasse norm theorem. *Compositio Math.* **35** (1977), no. 3, 281–298. MR0466073, Zbl 0376.12006, http://www.numdam.org/item?id=CM_1977__35_3_281_0. 1057

[18] Roquette, Peter. On class field towers. *Algebraic Number Theory* (Proc. Instructional Conf., Brighton, 1965), 231–249. *Thompson, Washington, D.C.*, 1967. MR0218331. 1060

[19] Serre, Jean-Pierre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401. MR0644559, Zbl 0496.12011, doi: 10.1007/BF02698692. 1064

(Christian Maire) FEMTO-ST Institute, Univ. Bourgogne Franche-Comté, CNRS, 15B avenue des Montboucons, 25030 Besançon cedex, France.
christian.maire@univ-fcomte.fr

This paper is available via http://nyjm.albany.edu/j/2018/24-50.html.