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 1056
2. Genus theory: basic results 1058
3. Kummer theory and governing field 1060
4. Proof of Theorem 1.3 1064
References 1065

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 \( K_m \) of \( K \) for a certain modulus \( m \) built over the set of ramification of \( L/K \); usually the ramification of \( LK_m/K \) is absorbed in \( L/K \), thus by class field theory the class group \( Cl(L) \) of \( L \) maps onto \( Gal(LK_m/L) \), and this last one “grows with \( 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 \( K \)
(resp. of L), and consider $M_{L/K}/K$ the maximal abelian extension of K inside $L^H/K$. The compositum $K^* := LM_{L/K}$ is called the genus field of the extension $L/K$, and the quantity $g^* := g(L/K)^* = [K^* : L]$ its genus number. Let $L^{ab} = M_{L/K} \cap L$ be the maximal abelian subextension of L/K. Then the relation

$$g^* = \frac{|\text{Cl}(K)|}{[L^{ab} : K]} \cdot [M_{L/K} : KH]$$

shows that, when the class group of K is known, it is easy to pass from $g := g(L/K) = [M_{L/K} : KH]$ 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 $g(L/K)$ is related to the kernel of a morphism $\Theta_S$ involving some Frobenius elements in $\text{Gal}(F/K)$. The quantity $g(L/K)$ is more directly connected to $\Theta_S$, 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 $S = \{p_1, \ldots, p_s\}$ the set of ramification of $L/K$. Put $K' = K(\mu_p)$ and $F = K'(\sqrt[p]{\mathcal{O}_K^x})$, where $\mathcal{O}_K^x$ is the group of units of the ring of integers $\mathcal{O}_K$ of K: the number field F is the governing field of our study. For each prime ideal $p \in S$, choose a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ above $p$ and put $\sigma_p := \sigma_{\mathfrak{p}}$, the Frobenius element at $\mathfrak{p}$ in $\text{Gal}(F/K')$. Consider the morphism $\Theta_S$ defined as follows:

$$\Theta_S : (\mathfrak{p}_p)^s \rightarrow \text{Gal}(F/K')$$

$$(a_1, \ldots, a_s) \mapsto \prod_{i=1}^s \sigma_{a_i}^{a_i}.$$  

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

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

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 $(r_{K,1}, r_{K,2})$ be its signature and put $r_K = r_{K,1} + r_{K,2} = 1 + \delta_{K,p}$, where $\delta_{K,p} = 1$ or 0 according $\mu_p \subset K$ or not, where $\mu_p$ is the group of $p$th 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 $s - \tau_K \leq k \leq s$, 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 $g(L/K) = p^k$. 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 $O(p^{2\tau_K+2}(\log p)^2)$.

1.3. This note contains four sections. In §2 we recall well-known 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 $\Theta_S$ 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 $\iota_v$ of $\mathbb{Q}$ in $\overline{\mathbb{Q}}_\ell$ such that $\iota_v(K)\overline{\mathbb{Q}}_\ell = K_v$; if $L/K$ is an extension of number fields we put $L_v := \iota_v(L)\overline{\mathbb{Q}}_\ell$. If $K_v$ is a local field, we denote by $v_{K_v}$ the normalized valuation of $K_v$, and by $\mathcal{U}_{K_v} = \{x \in L_v, v_{K_v}(x) > 0\}$ 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 $K_v = \mathbb{R}$ or $\mathbb{C}$, we put $\mathcal{U}_v = K_v^\times$.

**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 $D_v := \text{Gal}(L_v/K_v)$ the local Galois group at $v$, and consider $D_v^{ab} = \text{Gal}(L_v^{ab}/K_v)$ the abelianization of $D_v$, where here $L_v^{ab}/K_v$ is the maximal abelian subextension of $L_v/K_v$. Let $I_v := I(L_v/K_v) \subset D_v$ be the inertia subgroup, and $I_v^{ab} :=$
\( I(L^{ab}_v/K_v) \) be the restriction of \( I_v \) to \( L^{ab}_v \). If \( v \) is an archimedean place, one always has \( I_v = D_v \cong D^{ab}_v \).

Let \( W_v \subset \mathcal{U}_v := \mathcal{U}_{K_v} \) be the kernel of the Artin map \( Art_{L_v/K_v} : \mathcal{U}_v \rightarrow \mathfrak{i}^{ab}_v \). Of course, \( W_v = N_{L_v/K_v} \mathcal{U}_v \), where \( N_{L_v/K_v} \) is the norm map of \( L_v/K_v \).

Clearly, \( W_v = \mathcal{U}_v \) when \( v \) is unramified in \( L/K \).

Denote by \( K_m \) the ray class field of \( K \) corresponding by the global Artin map to the group of idèles \( W := \prod_v W_v \).

Let \( S := \{ v \in T, \mathfrak{i}^{ab}_v \neq \{1\} \} \) 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 \( W_S = \prod_{v \in S} W_v \). The following proposition may be found in [4, Proposition 1]:

**Proposition 2.1.** One has \( M_{L/K} = K_m \). Moreover,

\[
\text{Gal}(K_m/K^H) \simeq \mathcal{U}_S/\mathfrak{i}_S(\mathcal{O}_K^\times)W_S,
\]

where \( \mathfrak{i}_S \) is the natural embedding.

**Proof.** One has \( M_{L/K} \subset K_m \). Indeed, take a place \( v \) of \( K \) and \( \varepsilon \in W_v \). Then \( \varepsilon \) is a norm in \( L_v/K_v \) of some unit \( \varepsilon_0 \) in \( L_v \). As \( M_{L/K}L/L \) is unramified at \( v \), the unit \( \varepsilon_0 \) is a norm in the local extension \( (M_{L/K})_vL_v/L_v \), and then \( \varepsilon \) is a norm in \( (M_{L/K})_vL_v/K_v \), which implies that \( Art_{(M_{L/K})_v/K_v}(\varepsilon) \) is trivial. Then the global Artin map of the extension \( M_{L/K}/K \) vanishes on \( W \), and thus \( M_{L/K} \subset K_m \) by maximality of \( K_m \).

Moreover \( K_mL/L \) is an unramified abelian extension. Indeed, for every place \( v \) of \( K \), the local Artin symbol indicates that \( \mathcal{U}_v/W_v \rightarrow I((K_m)_v/K_v) \) and that \( I_v^{ab} = I(L_v/K_v)^{ab} \simeq \mathcal{U}_v/W_v \). By the property of the Artin symbol, one then has \( I(L_v^{ab}(K_m)_v/K_v) \simeq \mathcal{U}_v/W_v \), thus \( I(L_v^{ab}(K_m)_v/L_v) = \{1\} \) and \( (K_m)_vL_v/L_v \) is unramified. By maximality of \( M_{L/K} \) one deduces that \( K_m \subset M_{L/K} \), and finally that \( M_{L/K} = K_m \).

By class field theory one has

\[
\text{Gal}(K_m/K^H) \simeq \prod_v \mathcal{U}_v/\mathfrak{i}(\mathcal{O}_K^\times)W \simeq \mathcal{U}_T/\mathfrak{i}_T(\mathcal{O}_K^\times)W_T,
\]

where \( \mathfrak{i} : \mathcal{O}_K^\times \rightarrow \prod_v \mathcal{U}_v \) is the natural embedding. To conclude, observe that for \( v \in T \setminus S \), \( \mathcal{U}_v = W_v \), and then \( \mathcal{U}_T/W_T \simeq \mathcal{U}_S/W_S \). \( \square \)

### 2.2. Formula and exact sequence in genus theory.

If \( L/K \) is a Galois extension, denote by \( \mathcal{O}_K^\times \cap N_{L/K} \) the units \( \mathcal{O}_K^\times \) of \( \mathcal{O}_K \) 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:

\[
g(L/K) = \frac{\prod_{v \in T} \# I_v^{ab}}{O_K^\times : O_K^\times \cap N_{L/K}},
\]
(ii) the genus exact sequence:

\[ 1 \rightarrow \mathcal{O}_K^\times / \mathcal{O}_K^\times \cap N_{L/K} \rightarrow \prod_{v \in T} I_v^{ab} \rightarrow \text{Gal}(M_{L/K}/K^H) \rightarrow 1. \]

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

\[ s = \#S_\infty + \#S_0^{t} + \sum_{v \in S_0^{w}} d_v I_v^{ab}. \]

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

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

Let us consider the number fields $K' = K(\zeta)$ and $F = K'(\sqrt[p]{\mathcal{O}_K^\times})$: 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

\[ |d_F| \leq |d_K|^{(p-1)p^r_K} \cdot p^{[K:\mathbb{Q}](p-1)(4p^r_K-3)}. \]
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 $L_w/K''_w$ is less than $1+2e_w$ (indeed, every unit $\varepsilon \in K''_w$ such that $w(\varepsilon - 1) \geq 1 + 2e_w$ is a $p$th power). By the conductor-discriminant formula (see for example [15, Chapter VII, \$12, Theorem 11.9]) we get

$$w(\text{disc}(F_w/K''_w)) \leq (1+2e_w)(p^r - 1).$$

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

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

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 $\leq 1$) and then

$$|d_{K'}| = |d_{K''_w}|^{[K':K]} \cdot p^{\sum_{w|p} f_w \sum_{w|v} f(w/v)(e(w/v) - 1)} \leq \left(|d_{K''_w}| \cdot p^{[K:Q]}\right)^{p-1},$$

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 $M^\vee := \text{hom}(M, \mu_p)$. Let

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

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

$$\sigma_\chi(\psi(\varepsilon)) = \chi(\varepsilon) \cdot \psi(\varepsilon).$$

For more details see for example [5, Chapter I, \$6, exercise 6.2.2].

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

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

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

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

\sigma(\sqrt{\varepsilon})/\sqrt{\varepsilon} = \chi_v(\iota_v(\varepsilon)) = \zeta_v^{a_v(\varepsilon)}.

But by definition, the Frobenius element } \sigma_v \text{ satisfies the property:

\sigma_v(\sqrt{\varepsilon})/\sqrt{\varepsilon} \equiv \varepsilon^{(N(\nu_{K'}) - 1)/p} \mod \nu_{K'}.

Here } a \equiv b \mod \nu_{K'} \text{ means that } \nu_{K'}(a - b) > 0. \text{ Hence}

\iota_v(\sigma_v(\sqrt{\varepsilon})/\sqrt{\varepsilon}) \equiv \iota_v(\zeta_v^{a_v(\varepsilon)}) \mod \nu_{K'},

\text{which shows that } \sigma(\sqrt{\varepsilon}) = \sigma_v(\sqrt{\varepsilon}). \qed

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

\section{The other places.}

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

I_v^\prime \simeq (\mathcal{U}_v/\mathcal{W}_v)^\prime \hookrightarrow (\mathcal{U}_v/\mathcal{U}_v^p)^\prime.

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

\sigma_v^{(i)}(\sqrt{\varepsilon}) = \chi_v^{(i)}(\iota_v(\varepsilon)) \cdot \sqrt{\varepsilon}.

\subsection{Infinite places.} \text{Take } p = 2 \text{ and let } v \text{ be a real place of } K. \text{ Here } \mathcal{U}_v/\mathcal{U}_v^2 \simeq \mathbb{R}^\times/\mathbb{R}^\times. \text{ Then for } \varepsilon \in \mathcal{O}_K^\times \text{ put}

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

\text{where sign}(\iota_v(\varepsilon)) \text{ is the sign of the embedding } \iota_v(\varepsilon) \text{ of } \varepsilon \text{ in } \mathbb{K}. \text{ Of course } \sigma_v = \sigma_{\chi_v}, \text{ where } \chi_v \text{ is the non trivial character of } \mathcal{U}_v/\mathcal{U}_v^2.

\section{Key map and main result.} \text{Let } \Theta_S \text{ be the linear map}

\Theta_S : (\mathcal{U}_S/\mathcal{W}_S)^\prime \rightarrow \text{Gal}(\mathbb{F}/K')

defined as follows:

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

(ii) for } v \in S_0^{\text{ra}}, \text{ put } \Theta_S(\chi_v^{(i)}) = \sigma_v^{(i)}.

\text{While fixing an isomorphism } \text{Gal}(\mathbb{F}/K') \simeq \mathbb{F}_p^\times \text{ we see that } \Theta_S \text{ is a linear map from } \mathbb{F}_p^\times \text{ to } \mathbb{F}_p^\times.

\textbf{Theorem 3.5.} Under the assumptions of section 3, the Artin map induces the isomorphism } \ker(\Theta_S) \simeq \text{Gal}(\mathbb{K}_m/\mathbb{K}^H)^\prime.
**Proof.** Let us start with the exact sequence (see Proposition 2.1)

\[ 1 \longrightarrow \iota_\mathcal{S}(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p) \longrightarrow U_{\mathcal{S}/W} \longrightarrow \text{Gal}(K_m/K_H) \longrightarrow 1 \]

and take its Kummer dual to obtain

\[ 1 \longrightarrow \text{Gal}(K_m/K_H)^\vee \longrightarrow (U_{\mathcal{S}/W})^\vee \longrightarrow (\iota_\mathcal{S}(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p))^\vee \longrightarrow 1 \]

Observe that

\[ (U_{\mathcal{S}/W})^\vee \simeq \prod_{v \in S_0 \cup S_{\infty}} (U_v/U_v^p)^\vee \prod_{v \in S_{\infty}} (U_v/W_v)^\vee. \]

Thus, by Proposition 3.3 and sections 3.3.1 and 3.3.2, the induced map from \((U_{\mathcal{S}/W})^\vee\) to \(\text{Gal}(F/K')\) is exactly \(\Theta_\mathcal{S}\). Hence we get:

\[ \text{Gal}(K_m/K_H)^\vee \simeq \ker \left( (U_{\mathcal{S}/W})^\vee \xrightarrow{\Theta_\mathcal{S}} \text{Gal}(F/K') \right). \]

The proof is complete.

**Corollary 3.6.** One has \(g(L/K) = \# \ker(\Theta_\mathcal{S})\). In particular,

\[ s - r_K \leq d \text{Gal}(M_{L/K}/K_H) \leq s. \]

**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 \(L/Q\) be an imaginary quadratic extension of discriminant \(d\). The field \(F = Q(\sqrt{-1})\) is the governing field and, thanks to \(S_{\infty} = \{v_{\infty}\}\), the map \(\Theta_\mathcal{S}\) is onto. Then \(g(L/Q) = 2^s\) 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 \(L/Q\) be a real quadratic extension of discriminant \(d\). Here \(S_{\infty} = \emptyset\) and \(F = Q(\sqrt{-1})\) is the governing field. Then \(\Theta_\mathcal{S}\) is the zero map if and only if every odd prime \(\ell\) dividing \(d\) is congruent to 1 modulo 4; in this case \(g = 2^s\). Otherwise \(\Theta_\mathcal{S}\) 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 \(p = 3\), \(K = Q(\mu_3)\) and \(L = K(\sqrt[3]{d})\), \(d \in \mathbb{Z}_{>1}\), is also interesting to describe. Indeed in this case the governing extension is the extension \(Q(\mu_9)/Q(\mu_3)\). Here \(s - 2 \leq d_3 \text{Gal}(K^*/L) \leq s - 1\), and to have the exact value of \(d_3 \text{Gal}(K^*/L)\), one needs to determine: (i) the number \(s\) of prime ideals \(p\) in \(\mathcal{O}_K\) ramified in \(L/K\), and (ii) if the map \(\Theta_\mathcal{S}\) is trivial or not (here \(d_3 \text{Im}(\Theta_\mathcal{S}) \leq 1\)). And these two conditions are characterized by the congruences in \(\mathbb{Z}/9\mathbb{Z}\) of the
prime numbers \( \ell \) that divide \( d \). Typically, if there exists a prime number \( \ell | d \), \( \ell \neq 3 \), such that 3 divides the order of \( \ell \) in \((\mathbb{Z}/9\mathbb{Z})^\times \), then \( \text{Im}(\Theta_S) \simeq \mathbb{F}_3 \).

4. Proof of Theorem 1.3

Let \( s, k \in \mathbb{Z}_{>0} \) such that \( s - r_K \leq k \leq s \). Put \( n = s - k \).

First, one has to enlarge the governing field \( F = K'((\sqrt[3]{\mathcal{O}_K^h}) \) by considering the number field

\[
\tilde{F} := F((\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_h}),
\]

where the \( a_i \)'s are such that \( a_i \mathcal{O}_K = a_i^h \in \text{Cl}(K) \) and the family \( \{a_1, \ldots, a_h\} \) forms an \( \mathbb{F}_p \)-basis of \( \text{Cl}(K)[p] \) (the classes annihilated by \( p \)). One has \( [\tilde{F} : K'] = p^{r_K + h} \). Let us fix an \( \mathbb{F}_p \)-basis \( (e_i)_{i=1}^{r_K} \) of

\[
\text{Gal}(\tilde{F}/K'((\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_h}))) \simeq (\mathbb{F}_p)^{r_K}
\]

and complete this basis to an \( \mathbb{F}_p \)-basis \( (e_i)_{i=1}^{r_K + h} \) of \( \text{Gal}(\tilde{F}/K') \simeq (\mathbb{F}_p)^{r_K + h} \).

By the Chebotarev density theorem, let \( S = \{v_1, \ldots, v_s\} \) be a set of \( s \) different tame places of \( K \) such that the Frobenius elements \( \sigma_{v_i} \in \text{Gal}(\tilde{F}/K') \subseteq \text{Gal}(\tilde{F}/K) \) of \( v_i \) satisfy:

\[\begin{align*}
(a) \quad & \sigma_{v_i} = -(e_1 + \cdots + e_n); \\
(b) \quad & \text{for } i = 2, \ldots, n+1, \sigma_{v_i} = e_{i-1}; \\
(c) \quad & \text{for } i = n+2, \ldots, s, \sigma_{v_i} = 0,
\end{align*}\]

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

Observe that \( \sum_{i=1}^{s} \sigma_{v_i} = 0 \). 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 \( \Theta_S \), with value in \( \text{Gal}(F/K') \), is of rank \( n \). Then \( \text{Gal}(M_{L/K}[K]) \simeq (\mathbb{F}_p)^{s-n} = (\mathbb{F}_p)^k \) 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 \( \log |d_{F'}| \leq 2|\text{Cl}(K)| \log |d_F| \).

**Proof.** Adapt Proposition 3.2. \( \square \)

**Remark 4.2.** Obviously one has \( \tilde{F} = F \) 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 \( O \left( (\log |d_{F'}|)^2 \right) = O \left( (\log |d_F|)^2 \right) \).
For the places \( v_{n+2}, \ldots, v_s \), we need the following two lemmas.

**Lemma 4.3.** Given \( m \in \mathbb{Z}_{\geq 1} \), there exist \( m \) prime ideals \( p_1, \ldots, p_m \) in \( \mathcal{O}_K \) that split totally in \( \widetilde{F}/K \), all having absolute norm less than \( C_{K,p}m(\log m) \), where \( C_{K,p} \) is some constant depending on \( K \) and on \( p \).

**Proof.** For \( x \geq 2 \) let
\[
\pi(x) = \left| \{ \text{prime ideals } p \subset \mathcal{O}_K, |\mathcal{O}_K/p| \leq x, \text{p splits totally in } \widetilde{F}/K \} \right|.
\]
Then the effective Chebotarev density theorem under GRH indicates that
\[
\pi(x) \geq A(x) \log x,
\]
where \( \pi(x) \geq A(x) \log x \) for some constant \( C_{K,m} \) depending on \( K \) and on \( m \). Then, by Lemma 4.1 and Proposition 3.2, taking
\[
x_0 = C_{K,m}m(\log m),
\]
for some constant \( C_{K,m} \) depending on \( K \) and on \( m \) we are certain that \( A(x_0) \geq m \) and we are done. \( \square \)

**Lemma 4.4.** Given \( m \in \mathbb{Z}_{\geq 1} \), there exist \( m \) prime ideals \( p_1, \ldots, p_m \) in \( \mathcal{O}_K \) that split totally in \( \widetilde{F}/K \), all having absolute norm less than
\[
C_{K,m}p^{2r_K+2}(\log p)^2,
\]
where \( C_{K,m} \) is some constant depending on \( K \) and on \( m \).

**Proof.** Observe that \( \widetilde{F}/K \) is unramified outside \( p \). Let \( \ell \) be a prime number coprime to the set of ramification of \( \widetilde{F}/\mathbb{Q} \) and such that \( \ell \geq m \). By Bertrand’s postulate, this \( \ell \) can be taken less than \( C_K \cdot m \), where \( C_K \) is some constant depending on \( K \). Put \( N = \mathbb{Q}(\mu_\ell) \) and \( N_0 = \mathbb{N} \). The extension \( N_0/\widetilde{F} \) is of degree \( \ell-1 \), and \( |d_{N_0}| \leq |\mathbb{F}^{\ell-1}|d_N|\mathbb{F}:\mathbb{Q}| \). Let us choose now \( m \) prime ideals \( p_1, \ldots, p_m \) in \( \mathcal{O}_K \), all unramified in \( N_0/K \), such that their Frobenius in \( \text{Gal}(N_0/\widetilde{F}) \subset \text{Gal}(N_0/K) \) are in some different conjugacy classes: by the Chebotarev density theorem (under GRH), the \( p_i \)'s can be chosen of norm smaller than \( C(\log |d_{N_0}|)^2 \), where \( C \) is some absolute constant. Hence by Lemma 4.1, for \( i = 1, \ldots, m \), we obtain that the \( N(p_i) \)'s are smaller than
\[
C \left( \ell p^{r_K+1}|\text{Cl}(K)||K:\mathbb{Q}| \log(p^4\ell|d_K|^{2/[K:\mathbb{Q}]}) \right)^2 \leq C_{K,m}p^{2r_K+2}(\log p)^2.
\]
Finally to conclude, observe that each \( p_i \) splits totally in \( F/K \). \( \square \)

**References**


(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](http://nyjm.albany.edu/j/2018/24-50.html).