GENUS THEORY, GOVERNING FIELD, RAMIFICATION AND FROBENIUS

by

Roslan Ibara Ngiza Mfumu & Christian Maire

Abstract. — In this work we develop, through a governing field, genus theory for a number field K with tame ramification in T and splitting in S, where T and S are finite disjoint sets of primes of K. This approach extends that initiated by the second author in the case of the class group. We are able to express the S-T genus number of a cyclic extension L/K of degree p in terms of the rank of a matrix constructed from the Frobenius elements of the primes ramified in L/K, in the Galois group of the underlying governing extension. For quadratic extensions $\mathrm{L}/\mathbb{Q}$, the matrices in question are constructed from the Legendre symbols of the primes ramified in $\mathrm{L}/\mathbb{Q}$ and the primes of S.

1. Introduction

Let K be a number field, and let S and T be two finite and disjoint sets of places of K. We assume that T contains only non-archimedean places. Let K_T^S denote the maximal abelian extension of K, totally decomposed at all places in S (or S-split), unramified outside of T, and with at most tame ramification at the places $v \in T$ (or T-tamely ramified). This is a finite extension, and the Artin map allows us to identify the Galois group $\mathrm{Gal}(\mathrm{K}_T^S/\mathrm{K})$ with the S-ray class group of K modulo $\mathfrak{m} := \prod_{v\in T} v$, which we denote by $\mathrm{Cl}_{\mathrm{K},\mathfrak{m}}^S$. For more details, see Section §1.1.1.

Now let L/K be an extension of number fields with ramification set Σ. The genus theory provides information about the class group $\mathrm{Cl}_{\mathrm{L},\mathfrak{m}_\mathrm{L}}^{S_\mathrm{L}}$ in terms of Σ and the behavior of the S-units of K in L/K. See Theorem 2.1.

2000 ***Mathematics Subject Classification.*** — 11R37, 11R29.
Key words and phrases. — Genus theory, governing field, Frobenius.

The authors thank the International Mathematical Union - Commission for Developing Countries (IMU-CDC) and the GRAID program for their support. This work has been supported by the EIPHI Graduate School (contract "ANR-17-EURE-0002") and by the Bourgogne-Franche-Comté Region; by the AFRIMath Research Network of CNRS; by the European Mathematical Society; by the REDGATE project funded by CNRS (Dispositif de soutien aux collaborations avec l'Afrique subsaharienne); by the Agence Universitaire de la Francophonie (AUF); and by the Doctoral School SPIM from Bourgogne-Franche-Comté. The authors are grateful to the referees for thoroughly reading the paper and making a number of helpful suggestions. They also thank Ravi Ramakrishna for his interest in their work and his comments.

The first remarkable result in genus theory dates back to Gauss, concerning the 2-Sylow subgroup of the class group of quadratic extensions of $\mathbb{Q}$ (see [**8**, Chapter 1, §1] and [**4**, Chapter IV, §4, Exercise 4.2.10]). The phenomenon described by Gauss has been studied, developed, and generalized by many authors, including Hasse [**6**], Leopoldt [**9**], Furuta [**3**], and others. For more details, see [**4**, III.4].
The introduction of the sets T and S was initiated by Jaulent [**7**], Federer [**1**], and others. A very good overview of all this can be found in [**7**, Chapter II, 2.4, Chapter III, 2.1].

The work presented here is inspired by [**11**]. We develop the S-T genus theory via a governing extension denoted by $\mathrm{F}_T^S/\mathrm{K}$, where the usual ramification conditions are interpreted through relations between Frobenius elements. As a consequence, and similarly to [**11**, Theorem 1.3], questions in genus theory can be translated into questions about the behavior of Frobenius elements in a governing field, for which the Chebotarev density theorem becomes central.

When the base field K is given and the Galois group of L/K is a fixed abelian group, Frei, Loughran, and Newton [**2**] studied the asymptotic behavior of the genus number of L/K with respect to the discriminant of L. It would be interesting to revisit their results in light of our work.

Before presenting our results, let us begin by specifying the context.

1.1. The context. —

1.1.1. Ray class groups. — Let K be a number field, T a finite set of non-archimedean places of K, and S a finite set of places of K, disjoint from T. Let us denote $S = S_0 \cup S_\infty$, where S_0 contains only non-archimedean places and S_∞ contains archimedean places, which we assume to be contained in the set $Pl^{re}_{\mathrm{K},\infty}$ of real places of K.
For a place v of K, let ι_v denote the embedding of K into its completion K_v.
Set

- $I_{\mathrm{K},T}$ to be the group of nonzero fractional ideals of K prime to T,
- $\mathfrak{m} = \prod_{v \in T} v$, to be the ray modulus of K associated to T,
- $P^{S_\infty}_{\mathrm{K},\mathfrak{m}}$ to be the subgroup of principal ideals (x) of $I_{\mathrm{K},T}$, $x \equiv 1\,(\mathfrak{m})$, and $\iota_v(x) > 0$ for all $v \in pl^{re}_{\mathrm{K},\infty} \backslash S_\infty$,
- $\langle S_0 \rangle$ to be the subgroup of $I_{\mathrm{K},T}$ generated by the places in S_0,
- $R^S_{\mathrm{K},\mathfrak{m}}$ to be the subgroup $P^{S_\infty}_{\mathrm{K},\mathfrak{m}} \langle S_0 \rangle$ of $I_{\mathrm{K},T}$.

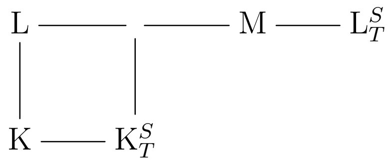
Let $\mathrm{Cl}^S_{\mathrm{K},\mathfrak{m}}$ be the S-ray-class group modulo $\mathfrak{m}$, *i.e.*

$$\mathrm{Cl}^S_{\mathrm{K},\mathfrak{m}} := I_{\mathrm{K},T}/R^S_{\mathrm{K},\mathfrak{m}}.$$

By class field theory, $\mathrm{Cl}^S_{\mathrm{K},\mathfrak{m}}$ is isomorphic to the Galois group of $\mathrm{K}^S_T/\mathrm{K}$, where K^S_T/K is the maximal abelian extension K, which is T-tamely ramified and S-split, see [**4**, Chapter II, §5].

1.1.2. Genus fields and genus numbers. — Let p be a prime number and let L/K be a cyclic extension of degree p. Denote by Σ the set of ramification of L/K. When $p = 2$, regarding the infinite places, we will refer to decomposition (one place splitting into two places) versus non-decomposition (one real place becoming one single complex place); note that in many other contexts, one says in the latter case that the real place ramifies.

Let T_{L} (respectively S_{L}) denote the places of L lying above those of T (resp. of S), and consider $\mathfrak{m}_{\mathrm{L}} := \prod_{w \in T_{\mathrm{L}}} w$. Set $L_T^S := L_{T_L}^{S_L}$, and $\mathrm{Cl}_{\mathrm{L},\mathfrak{m}}^S := \mathrm{Cl}_{\mathrm{L},\mathfrak{m}_{\mathrm{L}}}^{S_L}$.
Let M/K be the maximal abelian extension of K contained in L_T^S.



The field M is called the *S-T genus field* associated with L/K, and the quantity $(g_T^S)^* = [\mathrm{M} : \mathrm{L}]$ is the *S-T genus number.* Set $g_T^S = [\mathrm{M} : \mathrm{K}_T^S]$: this is the quantity g_T^S that we are studying. It can be observed that it is easy to pass from g_T^S to $(g_T^S)^*$ as soon as $\#\mathrm{Cl}_{\mathrm{K},\mathfrak{m}}^S$ is known, and the knowledge of g_T^S provides information about $\mathrm{Cl}_{\mathrm{L},\mathfrak{m}}^S$. Of course, genus theory makes sense when the field L is not contained in K_T^S, because otherwise $\mathrm{M} = \mathrm{K}_T^S$. The extension M/K being abelian, its Galois group can be approached through class field theory, which allows expressing $[\mathrm{M} : \mathrm{K}]$ in terms of the ramification in L/K and the S-units of K, thus leading to a non-trivial lower bound for $\#\mathrm{Cl}_{\mathrm{L},\mathfrak{m}}^S$.

Since L/K is cyclic of degree p, the Galois group $\mathrm{Gal}(\mathrm{M}/\mathrm{K}_T^S)$ is abelian of exponent p (see Theorem 2.1). Thus, when $p > 2$, the infinite places play no role. Consequently, we assume that $S_\infty = Pl_{\mathrm{K},\infty}^{re}$ in this case.

1.1.3. Governing fields. — We continue with a fixed prime number p. We then assume that for all $v \in T$, we have $N_v \equiv 1 \bmod p$, where N_v is the cardinality of the residue field of the completion K_v of K at v. Note that without this condition, the p-part contributed by the places v of T in $\mathrm{Cl}_{\mathrm{K},\mathfrak{m}}^S$, would be trivial.

Let E_T^S be the group of S-units of K congruent to $1 \pmod{\mathfrak{m}}$, that is,

$$E_T^S = \{x \in \mathrm{K}^\times \mid x \equiv 1 \pmod{\mathfrak{m}}, \, v(x) = 0 \ \forall v \notin S\}.$$

Observe that the dependence on T is in $\mathfrak{m}$. Here, we clarify the meaning of $v(x) = 0$. If $v \in S_0$, we identify the place v with its valuation; if $v \in Pl_{\mathrm{K},\infty}^{re}$, $v(x) = 0$ means $\iota_v(x) > 0$; for v archimedean, $v \notin Pl_{\mathrm{K},\infty}^{re}$, we define $v(x) = 0$.

Let $\mathrm{K}' = \mathrm{K}(\zeta_p)$, where ζ_p is a primitive pth root of unity.
The governing field F_T^S associated with the triplet (K, T, S) is defined as

$$\mathrm{F}_T^S := \mathrm{K}'(\sqrt[p]{E_T^S}).$$

We then define $\Gamma_T^S := \mathrm{Gal}(\mathrm{F}_T^S/\mathrm{K}')$: it is an abelian p-elementary group.

When $T = \emptyset$ and $S = Pl_{\mathrm{K},\infty}^{re}$, by Dirichlet's theorem the p-rank of $\Gamma^S := \Gamma_\emptyset^S$ is $r_1 + r_2 - 1 + \delta_{\mathrm{K},p} + \#S_0$, where (r_1, r_2) is the signature of K, and where $\delta_{\mathrm{K},p} = 1$ if $\zeta_p \in \mathrm{K}$, and 0 otherwise.

1.2. Our result. — We will present our main theorem (see Theorem 4.1 and Corollary 4.2) in a special case as a way of illustrating its key elements without many of the technicalities of the full result.

We assume that the set Σ does not contain any places above p; in other words, the extension L/K is tamely ramified. To further simplify the presentation, we also assume that the places in S split in L/K.

For each place $v \in \Sigma$, we choose a place w of K' above v and set $\sigma_v := \sigma_w$, the Frobenius element associated with w in $\Gamma_T^S := \mathrm{Gal}(\mathrm{F}_T^S/\mathrm{K})$; of course, this element depends on the choice of w, but we will see that the conditions involving it are independent of this choice.

Let $m = \#\Sigma\backslash\Sigma\cap(S\cup T)$, and let $\{e_{v_1},\ldots,e_{v_m}\}$ be a basis of $(\mathbb{F}_p)^m$ indexed by the places v of $\Sigma\backslash\Sigma\cap(S\cup T)$.
We then consider the linear map $\Theta_{\Sigma,T}^S$ defined by

$$\begin{array}{rrcl} \Theta_{\Sigma,T}^S : & (\mathbb{F}_p)^m & \longrightarrow & \Gamma_T^S \\ & e_v & \longmapsto & \sigma_v. \end{array}$$

We have the following result (see Corollary 4.5)

Theorem 1.1. — *Under the previous conditions, we have*

$$g_T^S = \#\ker(\Theta_{\Sigma,T}^S).$$

Remark 1.2. — Taking $T=\emptyset$ and $S = Pl_{\mathrm{K},\infty}^{re}$ we find Theorem 1.1 of [**11**].

The essence of our work is to translate the ramification conditions to dependence relations on Frobenius elements in a governing field. Therefore, if we ensure that the Frobenius elements associated with the places of T form a linearly independent set in $\Gamma^S := \mathrm{Gal}(\mathrm{F}^S/\mathrm{K}')$, then we can express quite easily the Galois group Γ_T^S.
Set $H_T := \sum_{v\in T}\mathbb{F}_p\sigma_v \subset \Gamma^S$.

Proposition 1.3. — *Suppose that the set $\{\sigma_v,\, v\in T\}$ forms a linearly independent family over $\mathbb{F}_p$ in Γ^S. Then $\Gamma_T^S \simeq \Gamma^S/H_T$.*

The condition of linear independence has an interpretation. Indeed, according to the Gras-Munnier theorem (see [**5**]) and its generalizations in Gras' book (see [**4**, Chapter V, Corollary 2.4.2]), a non-trivial relation between the Frobenius elements σ_v, $v\in T$, is equivalent to the existence of a cyclic extension of degree p of K, T-ramified and S-split, and consequently contributes "trivially" to g_T^S. Thus, the condition of linear independence forces avoidance of this situation.

Theorem 1.1 becomes interesting when we have a good understanding of the governing field F^S, especially when we know about the units of the base field. Typically, this occurs for $\mathrm{K}=\mathbb{Q}$, but also, as noted in [**11**, §3.5.3], for $p=3$ and for the base field $\mathrm{K}=\mathbb{Q}(\zeta_3)$. By introducing S-places, the role of the ordinary unit group is now played by the S-unit group, and when the field K is principal, the governing field is relatively easy to describe. A remarkable situation arises when $p=2$ and $\mathrm{L}/\mathbb{Q}$ is a quadratic extension. The quantity g_T^S corresponds to the kernel of a matrix constructed using Legendre symbols.
We explore a specific situation.
Let $\mathrm{L}/\mathbb{Q}$ be real quadratic extension with set of ramification $\Sigma=\{p_1,\cdots,p_m\}$. We take $T=\emptyset$. Let $S_0=\{\ell_1,\cdots,\ell_{s_0}\}$ be a set of primes of $\mathbb{Q}$, such that $\Sigma\cap(\{S_0\}\cup\{2\})=\emptyset$. We assume that S_∞ contains the unique infinite place v_∞, and set $\ell_0=-1$. Set $S=S_0\cup S_\infty$ and $s:=\#S$. In particular $s=s_0+1$. Observe that in this case Cl_L^S is the S_0-class group of L (in the ordinary sense).
Here, to simplify, we suppose that the places v in S_0 split in $\mathrm{L}/\mathbb{Q}$.

Let $A=(a_{i,j})$ be the matrix of size $s\times m$ defined by

$$a_{i,j}=\left(\frac{\ell_{i-1}}{p_j}\right),$$

where $\left(\frac{\ell_{i-1}}{p_j}\right)\in\mathbb{F}_2$ is the additive Legendre symbol.
Observe that $\mathrm{F}^S=\mathbb{Q}(\sqrt{-1},\sqrt{\ell_1},\cdots,\sqrt{\ell_{s_0}})$ and that $\Gamma^S:=\mathrm{Gal}(\mathrm{F}^S/\mathbb{Q})\simeq(\mathbb{F}_p)^s$. Hence the map $\Theta:(\mathbb{F}_p)^m\to(\mathbb{F}_p)^s$ of Theorem 1.1 is represented by the matrix A with the respect to obvious basis.

Corollary 1.4. — *Under the previous conditions, we have:*

$$g_\emptyset^S=\#\ker(A).$$

Example 1.5. — Take $\mathrm{K}=\mathbb{Q}$, and $\mathrm{L}=\mathbb{Q}(\sqrt{p_1p_2p_3})$, where p_1,p_2,p_3 are three distinct primes such that $p_1p_2p_3\equiv 1 \bmod 4$. Take $S=\{v_\infty\}\cup\{\ell_1,\ell_2\}$ such that the primes ℓ_i split in $\mathrm{L}/\mathbb{Q}$. One has (recall that $\ell_0=-1$)

$$A=\begin{pmatrix}\left(\frac{-1}{p_1}\right) & \left(\frac{-1}{p_2}\right) & \left(\frac{-1}{p_3}\right)\\ \left(\frac{\ell_1}{p_1}\right) & \left(\frac{\ell_1}{p_2}\right) & \left(\frac{\ell_1}{p_3}\right)\\ \left(\frac{\ell_2}{p_1}\right) & \left(\frac{\ell_2}{p_2}\right) & \left(\frac{\ell_2}{p_3}\right)\end{pmatrix},$$

where $\left(\frac{\cdot}{\cdot}\right)\in\mathbb{F}_2$ is the additive Legendre symbol, and $g_\emptyset^S=\#\ker(A)$.
As we shall see, assuming $S_\infty=\emptyset$ actually corresponds to omitting the first row of A.

The rest of our work consists of four sections. In Section 2, we introduce and develop the elements of genus theory that are useful for our results. Section 3 is dedicated to the governing field. It is also in this section that we prove Proposition 1.3. Section 4 focuses on our results and its proof. In the final section, we focus on the quadratic case.

2. Elements of genus theory

2.1. ***S*-*T* genus formula.** — For this part, we refer, for example, to [**4**, Chapter IV, §4], [**7**, Chapter III, §2], or [**10**].
We consider the framework of Section §1.1. Let T and S be two finite disjoint sets of places of K, non-archimedean for T and arbitrary for $S=S_0\cup S_\infty$.
Let L/K be a cylic extension of degree p.
We denote by $E_T^S\cap\mathscr{N}_{\mathrm{L}/\mathrm{K}}$, the elements of E_T^S that are locally norms everywhere in L/K.

The following theorem can be formulated in a more general context (see [**4**, Chapter IV]), but we will focus on the case of cyclic extension of degree p.

Theorem 2.1. — *Let* L/K *be a cylic extension of degree* p *with ramification set* Σ. *Then* $\mathrm{Gal}(\mathrm{M}/\mathrm{K}_T^S)$ *is an abelian group of exponent* p. *In particular,* g_T^S *is a power of* p, *and*

$$\log_p\left(g_T^S\right)=\#S^{ns}+\#\Sigma\backslash\Sigma\cap(S\cup T)-\log_p\left(E_T^S:E_T^S\cap\mathscr{N}_{\mathrm{L}/\mathrm{K}}\right),$$

where S^{ns} *denotes the set of places in* S *that are not split in* L/K.

Thus, the study of g_T^S is closely related to the quantity $E_T^S \cap \mathscr{N}_{\mathrm{L/K}}$. We will use the governing field F_T^S to get an explicit understanding of the size of the units in E_T^S which are locally norms everywhere. To achieve this, Proposition 2.4 below is central.

We set $\Sigma' := \Sigma \backslash \Sigma \cap (S \cup T)$.

2.2. Genus fields and ray class fields. — Let L/K be a cyclic extension of degree p. For $v \in Pl_{\mathrm{K}}$, we denote by $D_v := D_v(\mathrm{L/K})$ its decomposition group in L/K and by $I_v := I_v(\mathrm{L/K})$ its inertia group. It is worth mentioning that for an archimedean place v, we do not speak of ramification but rather of non-decomposition.
We now make the choice of a place $w|v$, and we set $\mathrm{L}_v := \mathrm{L}_w$.
Thus,

- for places $v \in \Sigma' := \Sigma \backslash \Sigma \cap (S \cup T)$, the local reciprocity map induces a surjective morphism from U_v to I_v, with kernel $W_v := \mathrm{N}_{\mathrm{L}_v/\mathrm{K}_v} U_{\mathrm{L}_v}$,
- for places $v \in S$, the local reciprocity map induces a surjective morphism from $\mathrm{K}_v^\times$ to D_v, with kernel $W_v := \mathrm{N}_{\mathrm{L}_v/\mathrm{K}_v} \mathrm{L}_v^\times$. Note that $W_v = \mathrm{K}_v^\times$ if and only if v splits in L/K.

Here, $U_v \subset \mathrm{K}_v^\times$ (respectively U_{L_v}) denotes the group of local units of K_v (resp. L_v), and $\mathrm{N}_{\mathrm{L}_v/\mathrm{K}_v}$ denotes the norm map of the local extension $\mathrm{L}_v/\mathrm{K}_v$. For a real infinite place v, we adopt the convention $U_v = (\mathbb{R}^\times)^2$, and for a complex place $U_v = \mathbb{C}^\times$.

Set

$$W = \prod_{v \in (S \cup \Sigma) \backslash (T \cap \Sigma)} W_v = \prod_{v \in \Sigma'} W_v \prod_{v \in S} W_v.$$

Remark 2.2. — Observe that for any place $v \in \Sigma' \cup S$ we have $\iota_v(E_T^S \cap (\mathrm{K}^\times)^p) \subset W_v$.

Definition 2.3. — We denote by $\mathrm{K}_{\Sigma,S,T}$ the abelian extension of K corresponding, via the global reciprocity map, to the idèle subgroup V:

$$V := W \left(\prod_{v \notin \Sigma' \cup S \cup T} U_v \right) \left(\prod_{v \in T} U_v^1 \right) = \left(\prod_{v \in \Sigma' \cup S} W_v \right) \left(\prod_{v \notin \Sigma' \cup S \cup T} U_v \right) \left(\prod_{v \in T} U_v^1 \right).$$

Here, U_v^1 is the subgroup of principal units of U_v.

The following proposition is central.

Proposition 2.4. — *Let* M/K *be the maximal abelian extension of* K *contained in* L_S^T. *Then we have* $\mathrm{M} = \mathrm{K}_{\Sigma,S,T}$. *Moreover*

$$\mathrm{Gal}(\mathrm{K}_{\Sigma,S,T}/\mathrm{K}_T^S) \simeq \frac{U_{\mathrm{K},\Sigma'}^S}{\nu(E_T^S) W},$$

where $U_{\mathrm{K},\Sigma'}^S = \prod_{v \in S} \mathrm{K}_v^\times \prod_{v \in \Sigma'} U_v$, *and where* $\nu : E_T^S \longrightarrow U_{\mathrm{K},\Sigma'}^S$ *is the diagonal embedding.*

Proof. — Let's note that:

- a *finite* place $v \notin \Sigma' \cup S \cup T$ of K is unramified in M/K,
- a place $v \in T$ is tamely ramified in M/K.

Therefore, the global reciprocity map for the extension M/K is trivial on

$$\left(\prod_{v\notin\Sigma'\cup S\cup T} U_v\right)\left(\prod_{v\in T} U_v^1\right).$$

Now we consider W.

For $v \in S$, since v splits totally in $\mathrm{L}_S^T/\mathrm{L}$ and thus in M/L, then $\mathrm{M}_v = \mathrm{L}_v$. Consequently, every element ε of W_v is also a norm in $\mathrm{M}_v/\mathrm{K}_v$. In other words, the local symbol at v in the extension M/K vanishes on W_v.

For $v \in \Sigma'$, let $\varepsilon \in W_v$. Then, by definition of W_v, there exists $z \in U_{\mathrm{L}_v}$ such that $\varepsilon = N_{\mathrm{L}_v/\mathrm{K}_v}(z)$. But since the extension $\mathrm{M}_v/\mathrm{K}_v$ is unramified at v, the element z is a norm in $\mathrm{M}_v/\mathrm{L}_v$, and thus ε is a norm in $\mathrm{M}_v/\mathrm{K}_v$. In other words, here too, the local symbol at v in the extension M/K vanishes on W_v.

In conclusion, the global reciprocity map for the extension M/K is trivial on V. Therefore, by maximality of $\mathrm{K}_{\Sigma,S,T}$, we have $\mathrm{M} \subset \mathrm{K}_{\Sigma,S,T}$.

Let's show the reverse inclusion. For that, observe that $\mathrm{K}_{\Sigma,S,T}/\mathrm{L}$ is an abelian extension such that:

- every place $v \in T$ is tamely ramified (possibly unramified);
- for every place $v \in S$, the following commutative diagram holds:

$$\begin{array}{ccc} \mathrm{K}_v^\times/W_v & \twoheadrightarrow & D_v(\mathrm{K}_{\Sigma,S,T}/\mathrm{K}) \\ & \searrow^{\simeq} & \downarrow \\ & & D_v(\mathrm{L}/\mathrm{K}) \end{array}$$

  showing that $D_v(\mathrm{K}_{\Sigma,S,T}/\mathrm{L})$ is trivial, hence $\mathrm{K}_{\Sigma,S,T}/\mathrm{L}$ is decomposed at every place $v \in S$;
- similary, every place $v \in \Sigma'$ is unramified in $\mathrm{K}_{\Sigma,S,T}/\mathrm{L}$.

Thus, $\mathrm{K}_{\Sigma,S,T}$ is contained in L_S^T, and by maximality of M, we deduce that $\mathrm{K}_{\Sigma,S,T} \subset \mathrm{M}$. Consequently, $\mathrm{M} = \mathrm{K}_{\Sigma,S,T}$.

In summary, if we denote by $\mathscr{J}_\mathrm{K}$ the idèle group of K, and by $\mathscr{U}_{\mathrm{K},T}^S$ the idèle subgroup given by

$$\mathscr{U}_{\mathrm{K},T}^S := \prod_{v\in S}\mathrm{K}_v^\times \prod_{v\in T} U_v^1 \prod_{v\notin T\cup S} U_v,$$

we have

$$\mathrm{Gal}(\mathrm{K}_{\Sigma,S,T}/\mathrm{K}) \simeq \mathscr{J}_\mathrm{K}/V\mathrm{K}^\times \text{ and } \mathrm{Gal}(\mathrm{K}_T^S/\mathrm{K}) \simeq \mathscr{J}_\mathrm{K}/\mathscr{U}_{\mathrm{K},T}^S\mathrm{K}^\times.$$

Therefore,

$$\mathrm{Gal}(\mathrm{K}_{\Sigma,S,T}/\mathrm{K}_T^S) \simeq \mathscr{U}_{\mathrm{K},T}^S\mathrm{K}^\times/V\mathrm{K}^\times \simeq \mathscr{U}_{\mathrm{K},T}^S/\left(V\mathrm{K}^\times\right)\cap\mathscr{U}_{\mathrm{K},T}^S \simeq \mathscr{U}_{\mathrm{K},T}^S/VE_T^S.$$

We conclude by noticing that $\mathscr{U}_{\mathrm{K},T}^S/V \simeq U_{\mathrm{K},\Sigma'}^S/W$. $\square$

3. Governing fields

Set $\mathrm{K}' = \mathrm{K}(\mu_p)$. We fix a generator ζ_p of μ_p. If B is an $\mathbb{F}_p$-module, let $B^\vee := \mathrm{Hom}(B,\mu_p)$. By Kummer duality, recall that for a subgroup of A of $\mathrm{K}'^\times$, one has $A(\mathrm{K}'^\times)^p/(\mathrm{K}'^\times)^p \simeq \mathrm{Gal}(\mathrm{K}'(\sqrt[p]{A})/\mathrm{K}')^\vee$. Moreover, if $A \subset \mathrm{K}^\times$, then

$$\mathrm{Gal}(\mathrm{K}'(\sqrt[p]{A})/\mathrm{K}')^\vee \simeq A(\mathrm{K}'^\times)^p/(\mathrm{K}'^\times)^p \simeq A/A\cap(\mathrm{K}'^\times)^p \simeq A/A\cap(\mathrm{K}^\times)^p \simeq A(\mathrm{K}^\times)^p/(\mathrm{K}^\times)^p,$$

because $[\mathrm{K}' : \mathrm{K}]$ is coprime to p.

3.1. Frobenius. — For any place v of K, let's define

$$\mathscr{E}^S_{T,v} = \{\varepsilon \in E^S_T,\ \varepsilon \in (\mathrm{K}_v^\times)^p\}.$$

This group of S-units fits into the exact sequence

$$1 \longrightarrow \mathscr{E}^S_{T,v}(\mathrm{K}^\times)^p/(\mathrm{K}^\times)^p \longrightarrow E^S_T(\mathrm{K}^\times)^p/(\mathrm{K}^\times)^p \longrightarrow i_v(E^S_T) \longrightarrow 1,$$

where $i_v : E^S_T \longrightarrow \mathrm{K}_v^\times/(\mathrm{K}_v^\times)^p$ is induced by the embedding ι_v of K into K_v.
Observe that for $v \in \Sigma'$,

$$\iota_v(E^S_T)U_v^p/U_v^p \simeq i_v(E^S_T) := \iota_v(E^S_T)(\mathrm{K}_v^\times)^p/(\mathrm{K}_v^\times)^p.$$

By Kummer duality we have

$$i_v(E^S_T)^\vee \simeq (E^S_T(\mathrm{K}^\times)^p/\mathscr{E}^S_{T,v}(\mathrm{K}^\times)^p)^\vee \simeq \mathrm{Gal}(\mathrm{K}'(\sqrt[p]{E^S_T})/\mathrm{K}'(\sqrt[p]{\mathscr{E}^S_{T,v}})).$$

This latter Galois group is easy to interpret:

Lemma 3.1. — *One has* $\mathrm{Gal}(\mathrm{K}'(\sqrt[p]{E^S_T})/\mathrm{K}'(\sqrt[p]{\mathscr{E}^S_{T,v}})) = D_v(\mathrm{F}^S_T/\mathrm{K}')$.

(We will see later that it does not depend on the choice of a place $w|v$ of K'.)

Proof. — Let's denote by N the subfield of $\mathrm{F}^S_T/\mathrm{K}'$ corresponding, via Galois theory, to $D_v(\mathrm{F}^S_T/\mathrm{K}')$. Clearly, $\mathrm{K}'(\sqrt[p]{\mathscr{E}^S_{T,v}}) \subset \mathrm{N}$. For the reverse inclusion, note that if there exists an intermediate subfield N' of degree p over N, then, as $\mathrm{Gal}(\mathrm{K}'(\sqrt[p]{E^S_T})/\mathrm{K}'(\sqrt[p]{\mathscr{E}^S_{T,v}})$ is an abelian p-elementary group, N' arises from the compositum with a cyclic extension N_0/K' of degree p: there exists $x \in E^S_T$ such that $\mathrm{N}_0 = \mathrm{K}'(\sqrt[p]{x})$. Now, since v splits in N/K', it follows that $x \in (\mathrm{K}'_v)^p$, hence $x \in \mathrm{K}_v^p$ because $[\mathrm{K}'_v : \mathrm{K}_v]$ is coprime to p; thus $\mathrm{N}_0 \subset \mathrm{K}'(\sqrt[p]{\mathscr{E}^S_{T,v}})$, which leads to a contradiction. □

When v is unramified in $\mathrm{F}^S_T/\mathrm{K}'$, the Galois group of $\mathrm{K}'(\sqrt[p]{E^S_T})/\mathrm{K}'(\sqrt[p]{\mathscr{E}^S_{T,v}})$ is generated by the Frobenius element associated to the choice of a place $w|v$ of K'.

From now on, we fix $w|v$ and set $\sigma_v := \sigma_w$, where σ_w is the Frobenius at w in $\mathrm{Gal}(\mathrm{K}'(\sqrt[p]{\mathscr{E}^S})/\mathrm{K}'$.

Next, let D_v be the decomposition group of v in the extension $\mathrm{F}^S_T/\mathrm{K}'$.

Let

$$\Phi_v : \left(E^S_T(\mathrm{K}^\times)^p/\mathscr{E}^S_{T,v}(\mathrm{K}^\times)^p\right)^\vee \longrightarrow \mathrm{Gal}(\mathrm{F}^S_T/\mathrm{K}'(\sqrt[p]{\mathscr{E}^S_{T,v}})) = D_v$$

be the isomorphism arising from Kummer duality. Recall how Φ_v is defined: for $\chi \in \left(E^S_T(\mathrm{K}^\times)^p/\mathscr{E}^S_{T,v}(\mathrm{K}^\times)^p\right)^\vee$, we associate the element $g_\chi := \Phi_v(\chi)$ defined as follows:

$$g_\chi(\sqrt[p]{\varepsilon}) = \chi(\varepsilon) \cdot \sqrt[p]{\varepsilon},$$

for any $\varepsilon \in E^S_T$.

For $v \in \Sigma' \cup S$, consider the local map φ_v also derived from Kummer duality:

$$\varphi_v : (A_v/W_v)^\vee \hookrightarrow (A_v/A_v^p)^\vee \twoheadrightarrow i_v(E^S_T)^\vee \xrightarrow{\simeq} D_v,$$

where $A_v = U_v$ (respectively $A_v = \mathrm{K}_v^\times$) for $v \in \Sigma'$ (resp. $v \in S$).

When $(A_v/W_v)^\vee$ is non-trivial, it is generated by a certain character $\chi_v = \chi_w$. Now observe that if we choose another place $w'|v$ of K′, then $w' = hw$ for some $h \in \mathrm{Gal}(\mathrm{K}'/\mathrm{K})$. Let $\chi_{w'} := \chi_{hw} := \chi_w(h^{-1}(.))$; this is a non-trivial character of $(A_{w'}/W_{w'})^\vee$.

Lemma 3.2. — *Set $g_w := \varphi_w(\chi_w)$ and $g_{w'} := \varphi_{w'}(\chi_{w'})$. Then $\langle g_w\rangle = \langle g_{w'}\rangle$.*

Proof. — This is a consequence of Kummer theory where we have $g_{w'} = g_w^a$ for some $a \in \mathbb{F}_p^\times$ (see, for example, [**4**, Chapter I, §6, Theorem 6.2]). □

Thus, all the subsequent results do not depend on the choice of $w|v$.
Let's define $g_v := \varphi_v(\chi_v)$. We will now describe φ_v more precisely.

(i) This is the most important case. Let $v \in \Sigma'$. Recall that $U_v/W_v \simeq \mathbb{Z}/p$, hence $U_v^p \subset W_v$. There exists a non-trivial element χ_v of $(U_v/W_v)^\vee$ such that

$$\langle\chi_v\rangle = (U_v/W_v)^\vee \hookrightarrow (U_v/U_v^p)^\vee \cdot$$

Then $\varphi_v(\chi_v)$ is an element $g_v := g_{\chi_v}$ of D_v, defined by

$$g_v(\sqrt[p]{\varepsilon}) = \chi_v(\iota_v(\varepsilon)) \cdot \sqrt[p]{\varepsilon},$$

for all $\varepsilon \in E_T^S$.
Let $Pl_{\mathrm{K},p} = \{v \in Pl_{\mathrm{K}}, v|p\}$ be the set of p-adic places of K.
Observe that if $v \notin Pl_{\mathrm{K},p} \cup S_0$, then v is unramified in $\mathrm{F}_T^S/\mathrm{K}'$, and $U_v^p = W_v$. In particular, D_v is a cylic group generated by the Frobenius σ_v at v. Thus

$$\varphi_v : \langle\chi_v\rangle \twoheadrightarrow \langle\sigma_v\rangle\cdot$$

Replacing χ_v by a suitable power, we obtain $\varphi_v(\chi_v) = \sigma_v$.

(ii) Let $v \in S_0 \backslash S_0 \cap \Sigma$. Then v is unramified in L/K.
First, note that if v splits in L/K, then $W_v = \mathrm{K}_v^\times$ and thus φ_v is the trivial map.
Now, suppose v is inert in L/K. Then $W_v = U_v\langle\pi_v^p\rangle$ and thus

$$\mathrm{K}_v^\times/W_v \simeq \mathrm{K}_v^\times/U_v\langle\pi_v^p\rangle \simeq \langle\pi_v\rangle/\langle\pi_v^p\rangle\cdot$$

Let χ_v be the generator of $(\langle\pi_v\rangle/\langle\pi_v^p\rangle)^\vee$ defined by $\chi_v(\pi_v^i) = \zeta_p^i$. Then $g_v := \varphi_v(\chi_v)$ satisfies: for all $\varepsilon \in E_T^S$,

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

Thus $\chi_v(\iota_v(\varepsilon)) = 1$ if and only if the valuation $v(\varepsilon)$ of ε is zero modulo p.

(iii) Let $v \in S_0 \cap \Sigma$. This is analogous to (i), noting that $A_v = \mathrm{K}_v^\times$.

(iv) Here $p = 2$ and v is a real place in S.
As in (ii), if v splits in L/K, then $W_v = \mathrm{K}_v^\times$ and φ_v is the trivial map. Otherwise for $\varepsilon \in E_T^S$

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

where $\mathrm{sign}(\iota_v(\varepsilon))$ is the sign of the embedding $\iota_v(\varepsilon)$ of ε in K_v.

3.2. A restriction. — Let $T = \{v_1, \ldots, v_t\}$, and for $i = 1, \cdots, t$, let σ_{v_i} be the Frobenius at v_i in Γ^S; set $\mathrm{H}_T := \langle \sigma_v,\, v \in T\rangle$.

Proposition 3.3. — *Suppose that the set* $\{\sigma_{v_1}, \ldots, \sigma_{v_t}\}$ *forms a linearly independent family over* $\mathbb{F}_p$ *in* Γ^S. *Then*

$$\Gamma_T^S := \mathrm{Gal}(\mathrm{F}_T^S/\mathrm{K}') \simeq \Gamma^S/\mathrm{H}_T\cdot$$

Proof. — Let's give a proof by induction on the cardinality of T. Recall that for $v \in T$, one has $N_v \equiv 1 \bmod p$.

• Suppose $T = \{v\}$. Let $E^S_{\{v\}} = \{\varepsilon \in E^S,\ \varepsilon \equiv 1\,(v)\}$. Define $\mathscr{E}_v^S = \{\varepsilon \in E^S,\ \varepsilon \in (\mathrm{K}_v^\times)^p\}$. By Hensel's lemma, we have $E^S_{\{v\}} \subset \mathscr{E}_v^S$. Moreover, $E^S/E^S_{\{v\}} \hookrightarrow \mathbb{F}_v^\times$, where $\mathbb{F}_v$ is the residue field at v. Thus, $E^S/E^S_{\{v\}}$ is cyclic. Since $E^S_{\{v\}} \subset \mathscr{E}_v^S$, it follows

$$\mathbb{Z}/p\mathbb{Z} \twoheadrightarrow \frac{E^S(\mathrm{K}^\times)^p}{E^S_{\{v\}}(\mathrm{K}^\times)^p} \twoheadrightarrow \frac{E^S(\mathrm{K}^\times)^p}{\mathscr{E}_v^S(\mathrm{K}^\times)^p}\cdot \tag{1}$$

By Lemma 3.1, we have:

$$\left(\frac{E^S(\mathrm{K}^\times)^p}{\mathscr{E}_v^S(\mathrm{K}^\times)^p}\right)^\vee = \langle \sigma_v\rangle \subset \Gamma^S\cdot$$

Now, since $\sigma_v \neq 0$ by assumption, it follows that $\dfrac{E^S(\mathrm{K}^\times)^p}{\mathscr{E}_v^S(\mathrm{K}^\times)^p} \simeq \mathbb{Z}/p\mathbb{Z}$. Thus, from (1) we have $\dfrac{E^S(\mathrm{K}^\times)^p}{E^S_{\{v\}}(\mathrm{K}^\times)^p} = \langle\sigma_v\rangle^\vee$, or equivalently $\mathrm{Gal}(\mathrm{F}^S/\mathrm{F}^S_T) = \langle\sigma_v\rangle$. This concludes this case.

• Let's suppose $T = T_0 \cup \{v\}$, and that the proposition is true for T_0. Define $\mathscr{E}^S_{T_0,v} = \{\varepsilon \in E^S,\ \varepsilon \equiv 1\,(v'),\ v' \in T_0,\ \varepsilon \in U_v^p\}$. By Hensel's lemma, we have $E_T^S \subset \mathscr{E}^S_{T_0,v}$. As before, $\dfrac{E^S_{T_0}}{E^S_T} \hookrightarrow \mathbb{F}_v^\times$, implying that $\dfrac{E^S_{T_0}}{E^S_T}$ is cyclic, so we have

$$\mathbb{Z}/p\mathbb{Z} \twoheadrightarrow \frac{E^S_{T_0}(\mathrm{K}^\times)^p}{E^S_T(\mathrm{K}^\times)^p} \twoheadrightarrow \frac{E^S_{T_0}(\mathrm{K}^\times)^p}{\mathscr{E}^S_{T_0,v}(\mathrm{K}^\times)^p}\cdot \tag{2}$$

Then we define

$$\left(\frac{E^S_{T_0}(\mathrm{K}^\times)^p}{\mathscr{E}^S_{T_0,v}(\mathrm{K}^\times)^p}\right)^\vee = \langle\overline{\sigma}_v\rangle,$$

where $\overline{\sigma}_v$ is the restriction of the Frobenius $\sigma_v \in \Gamma^S$ to $\mathrm{F}^S_{T_0}$. By the induction hypothesis,

$$\left(\frac{E^S(\mathrm{K}^\times)^p}{E^S_{T_0}(\mathrm{K}^\times)^p}\right)^\vee = \langle\sigma_{v'},\, v' \in T_0\rangle\cdot$$

But $\overline{\sigma}_v = 1$ would imply $\sigma_v \in \langle\sigma_{v'},\, v' \in T_0\rangle$ which contradicts the assumption. Therefore, the surjections in (2) are isomorphisms, and $\mathrm{Gal}(\mathrm{F}^S/\mathrm{F}^S_T)$ is generated by the Frobenius elements σ_v and $\sigma_{v'}$, $v' \in T_0$. This concludes the proof. □

Remark 3.4. — The Galois group $\mathrm{Gal}\left(\mathrm{F}^S/\mathrm{F}^S_{\{v\}}\right)$ may not be generated by the Frobenius at v. Let's give an example.

Take $\mathrm{K} = \mathbb{Q}$ and $p = 2$. Choose $T = \{\ell\}$, where $\ell \equiv 1(\mathrm{mod}\ 4)$ is a prime number.

Let $S = S_\infty = \{v_\infty\}$. We have $E^S = \langle \pm 1\rangle$ and $E^S_{\{\ell\}} = \langle 1\rangle$. Thus

$$\mathrm{F}^S = \mathbb{Q}(\sqrt{E^S}) = \mathbb{Q}(\sqrt{-1}), \text{ and } \mathrm{F}^S_{\{\ell\}} = \mathbb{Q}(\sqrt{E^S_{\{\ell\}}}) = \mathbb{Q}\,.$$

However, since ℓ splits in $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$, it follows that $\sigma_\ell = 1$. Consequently, $\mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q})$ is not generated by the Frobenius at ℓ.

When $p = 2$ we can handle the archimedean places in the same way. Set $\overline{S} := S_0 \cup Pl^{re}_{\mathrm{K},\infty}$. Observe that $E^{\overline{S}}$ is the group of S_0-units in the ordinary sense (with no sign condition).

Proposition 3.5. — *Take $p = 2$. Set $H^{S_\infty} = \langle \sigma_v;\, v \in pl^{re}_{\mathrm{K},\infty}\backslash S_\infty\rangle \subset \Gamma^{\overline{S}}$ and identify H_{S_∞} with its restriction to $\Gamma^{\overline{S}}_T$. Then we have*

$$\Gamma^S_T := \mathrm{Gal}(\mathrm{K}(\sqrt{E^S_T})/\mathrm{K}) \simeq \Gamma^{\overline{S}}_T / H_{S_\infty}\cdot$$

Moreover, if the set $\{\sigma_v,\, v \in T\}$ forms a linearly independent family in $\Gamma^{\overline{S}}$, then

$$\mathrm{Gal}(\mathrm{K}(\sqrt{E^S_T})/\mathrm{K}) \simeq \Gamma^{\overline{S}} / \left(H_{S_\infty} + H_T\right)\cdot$$

Proof. — As in Lemma 3.1, we can show that $\mathrm{K}(\sqrt{E^S_T})$ corresponds, by Galois theory, to the subgroup H_{S_∞} of $\Gamma^{\overline{S}}_T$.
As for the second part, from Proposition 3.3 we know that $\Gamma^{\overline{S}}_T \simeq \Gamma^{\overline{S}}/H_T$; thus, we conclude with the first point. □

4. Main result

We keep the notations from the previous sections. In particular, $\Sigma' = \Sigma\backslash\Sigma\cap(S\cup T)$.

For $v \in \Sigma' \cup S$, let's consider the elements $g_v := \varphi_v(\chi_v) \in \Gamma^S_T$ defined in $(i)-(iv)$ of §3.1. Let $\Theta^S_{\Sigma,T}$ be the following linear map:

$$\Theta^S_{\Sigma,T} \;:\; \left(\frac{U^S_{\mathrm{K},\Sigma'}}{W}\right)^\vee \longrightarrow \Gamma^S_T.$$

defined by $\Theta^S_{\Sigma,T}(\chi_v) = g_v$.

Theorem 4.1. — *The Artin map induces the following isomorphism:*

$$\ker(\Theta^S_{\Sigma,T}) \simeq \mathrm{Gal}(\mathrm{K}_{\Sigma,S,T}/\mathrm{K}^S_T)^\vee.$$

Proof. — Let $\nu : E^S_T \longrightarrow U^S_{\mathrm{K},\Sigma'}$ be the diagonal embedding.
First, by Remark 2.2 we observe that

$$\nu(E^S_T \cap (\mathrm{K}^\times)^p) = 1.$$

It follows that ν factors through $E^S_T \cap (\mathrm{K}^\times)^p$. Now, consider the exact sequence obtained from Proposition 2.4:

$$1 \longrightarrow \nu(E^S_T/E^S_T \cap (\mathrm{K}^\times)^p) \longrightarrow U^S_{\mathrm{K},\Sigma'}/W \longrightarrow \mathrm{Gal}(\mathrm{K}_{\Sigma,S,T}/\mathrm{K}^S_T) \longrightarrow 1.$$

By Kummer duality, we have:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(\mathrm{K}_{\Sigma\cup S}/\mathrm{K}_T^S)^\vee & \longrightarrow & \left(U^S_{\mathrm{K},\Sigma'}/W\right)^\vee & \longrightarrow & \left(\nu(E_T^S/E_T^S\cap(\mathrm{K}^\times)^p)\right)^\vee & \longrightarrow & 1 \\ & & & & \downarrow & & \downarrow & & \\ & & & & \Gamma_T^S & \xleftarrow[\simeq]{\Psi} & \left(E_T^S(\mathrm{K}^\times)^p/(\mathrm{K}^\times)^p\right)^\vee & & \end{array}$$

Now,

$$\left(U^S_{\mathrm{K},\Sigma'}/W\right)^\vee \simeq \prod_{v\in\Sigma'}(U_v/W_v)^\vee \prod_{v\in S}(\mathrm{K}_v^\times/W_v)^\vee.$$

Then, it suffices to observe that the induced map from $\left(U^S_{\mathrm{K},\Sigma'}/W\right)^\vee$ to Γ_T^S corresponds to $\Theta^S_{\Sigma,T}$. Therefore, we finally obtain:

$$\mathrm{Gal}(\mathrm{K}_{\Sigma,S,T}/\mathrm{K}_T^S)^\vee \simeq \ker\left(\left(U^S_{\mathrm{K},\Sigma'}/W\right)^\vee \xrightarrow{\Theta^S_{\Sigma,T}} \Gamma_T^S\right).$$

Hence the result. $\square$

Therefore, it follows that

Corollary 4.2. — *We have $g_T^S = \#\ker(\Theta^S_{\Sigma,T})$.*

Proof. — This is a consequence of Theorem 4.1 and Proposition 2.4. $\square$

If $v \in S$ splits in L/K, then the component at v in $\dfrac{U^S_{\mathrm{K},\Sigma'}}{W}$ is trivial.
Set $S = S^{sp}\cup S^{ns}$, where S^{sp} is the set of places in S that split in L/K, and $S^{ns} = S\backslash S^{sp}$.
Let $s^{ns} = \#S^{ns}$ and $m := \#\Sigma\backslash\Sigma\cap(S\cup T)$.
Then $\left(\dfrac{U^S_{\mathrm{K},\Sigma'}}{W}\right)^\vee$ is isomorphic to $(\mathbb{Z}/p)^{s^{ns}+m}$.

Corollary 4.3. — *We have $m + s^{ns} - r_T^S \le \log_p(g_S^T) \le m + s^{ns}$, where r_T^S is the p-rank of E_T^S.*

Proof. — It suffices to observe that $\dim\Gamma_T^S = \dim E_T^S(\mathrm{K}^\times)^p/(\mathrm{K}^\times)^p \le r_T^S$. $\square$

Remark 4.4. — We have $\dim\Gamma_T^S \le r_{S_0}$, where $r_{S_0} = r_1 + r_2 + |S_0| - \delta_{\mathrm{K},p}$.
When the Frobenius elements of the places $v\in T$ are linearly independent in Γ^S, we also have $\dim\Gamma_T^S = \dim\Gamma^S - |T| \le r_{S_0} - |T|$. (See Proposition 3.3.)

***Corollary 4.5* (Theorem 1.1).** — *If $S^{ns} = \Sigma\cap Pl_{\mathrm{K},p} = \emptyset$, let $\{e_{v_1},\dots,e_{v_m}\}$ be a basis of $(\mathbb{F}_p)^m$ indexed by the places v in $\Sigma\backslash\Sigma\cap(S\cup T)$, and let Θ be the linear map defined by:*

$$\begin{array}{rccc} \Theta\,: & (\mathbb{F}_p)^m & \longrightarrow & \Gamma_T^S \\ & e_v & \longmapsto & \sigma_v. \end{array}$$

Then $g_S^T = \#\ker(\Theta)$.

Proof. — In this case, $g_v = \sigma_v$. $\square$

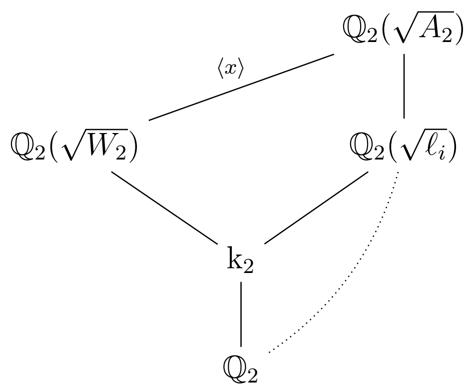
5. Quadratic extensions

We take $p = 2$ and $\mathrm{K} = \mathbb{Q}$.
Let $\mathrm{L}/\mathbb{Q}$ be a quadratic extension with set of ramification $\Sigma = \{p_1, \cdots, p_m\}$.
In the spirit of Proposition 3.3, we assume $T = \emptyset$.
Let $S_0 = \{\ell_1, \ldots, \ell_{s_0}\}$ be a set of primes. We assume that $\Sigma \cap S = \emptyset$.
We denote ℓ_∞ as the infinite place; then $S_\infty = \{\ell_\infty\}$ or $S_\infty = \emptyset$. Set $S = S_\infty \cup S_0$.
Let E^S be the group of S-units of $\mathbb{Q}$. We write $E^S = \langle \ell_0, \ldots, \ell_s \rangle$, with $\ell_0 = -1$ or 1 depending on whether $S_\infty = \{\ell_\infty\}$ or S_∞ is empty.
In this context, the governing field is written as $\mathrm{F}^S = \mathbb{Q}(\sqrt{E^S}) = \mathbb{Q}(\sqrt{\ell_0}, \ldots, \sqrt{\ell_{s_0}})$. Its Galois group $\Gamma^S := \mathrm{Gal}(\mathrm{F}^S/\mathbb{Q})$ is isomorphic to $\prod_{j=0}^{s_0} \mathrm{Gal}(\mathbb{Q}(\sqrt{\ell_j})/\mathbb{Q})$. Note that $\mathrm{Gal}(\mathbb{Q}(\sqrt{\ell_0})/\mathbb{Q})$ may be trivial.
Let's revisit the element g_ℓ defined in Section §3.1 and consider its restriction to $\mathbb{Q}(\sqrt{\ell_j})$: its value is in $\{0, 1\}$. For what follows, the quadratic residue symbol is viewed additively, meaning it takes values in $\mathbb{F}_2$.

Lemma 5.1. — *The elements g_ℓ takes the following values:*
(a) For $\ell \in \Sigma'$ and ℓ odd, the restriction of $g_\ell = \sigma_\ell$ to $\mathbb{Q}(\sqrt{\ell_j})$ equals $\left(\frac{\ell_j}{\ell}\right)$.
(b) For $\ell \in S_0^{ns} \backslash S_0^{ns} \cap \Sigma$, the restriction of g_ℓ to $\mathbb{Q}(\sqrt{\ell_j})$ is trivial if and only if $\ell \neq \ell_j$.
(c) For $\ell = \ell_\infty$, the restriction of g_{ℓ_∞} to $\mathbb{Q}(\sqrt{\ell_j})$ is trivial unless $\ell_j = \ell_0 = -1$ and L is imaginary.

Proof. — (a) is (i) of §3.1, (b) is (ii) and (c) is (iv). □

It remains to describe g_2 when 2 is ramified in $\mathrm{L}/\mathbb{Q}$. So, suppose $2 \in \Sigma$. We identify g_2 with its restriction to $\mathrm{Gal}(\mathbb{Q}(\sqrt{\ell_i})/\mathbb{Q})$. We have the following extensions



Recall that $A_2 = U_2$ (respectively $A_2 = \mathbb{Q}_2^\times$) if $2 \notin S$ (resp. $2 \in S$).
The desired element g_2 is the image of the restriction of x in $\mathrm{Gal}(\mathbb{Q}_2(\sqrt{\ell_i})/\mathbb{Q}_2) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{\ell_i})/\mathbb{Q})$. Therefore g_2 (restricted) is trivial if and only if $\ell_i \in W_2$ modulo $(A_2)^2$.
In general, everything relies on determining W_2, which is the conductor at 2 of L/K; see [**4**, Chapter II, §1, Exercise 1.6.5] for calculations.
For example, suppose $d \equiv -1$ modulo 8. Then $W_2 = \langle 5 \rangle$. Hence, g_2 restricted to $\mathrm{Gal}(\mathbb{Q}(\sqrt{\ell_i})/\mathbb{Q})$ is trivial if and only if, $\ell_i \equiv 1$ modulo 4.

A particularly noteworthy situation arises when we are only dealing with cases of Lemma 5.1 and $\mathrm{L}/\mathbb{Q}$ is unramified at 2. We detail this situation.

We take $S_\infty = \{\ell_\infty\}$, and $S = S_0 \cup S_\infty$.
Let $S_0^{ns} \subset S_0$ be the set of primes of S_0 that do not split in L/$\mathbb{Q}$. Set $n = \# S_0^{ns}$. After renumbering the primes of S_0, we may assume that $S_0^{ns} = \{\ell_1, \cdots, \ell_n\}$.

• Suppose first that L/$\mathbb{Q}$ is imaginary. In this case $S^{ns} = \{\ell_\infty\} \cup S_0^{ns}$.
Let the canonical basis $\mathscr{B} := \{e_{p_1}, \ldots, e_{p_m}, e_{\ell_\infty}, e_{\ell_1}, \ldots, e_{\ell_n}\}$ of $\mathbb{F}_2^{m+n+1}$ be indexed by the places of $\Sigma \cup S^{ns}$.
The map $\Theta := \Theta_\Sigma^S$ on the basis $\mathscr{B}$, taking values in $\prod_{j=0}^{s_0} \mathrm{Gal}(\mathbb{Q}(\sqrt{\ell_j})/\mathbb{Q})$, is defined by

$$\Theta(e_{p_i})_{|\mathbb{Q}(\sqrt{\ell_j})} = \left(\frac{\ell_j}{p_i}\right), \quad \Theta(e_{\ell_i})_{|\mathbb{Q}(\sqrt{\ell_j})} = \delta_{i,j} = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ otherwise} \end{cases}.$$

The matrix A of Θ, of size $(s_0+1) \times (m+n)$, is then written as follows

$$\begin{pmatrix}
\left(\frac{-1}{p_1}\right) & \left(\frac{-1}{p_2}\right) & \cdots & \left(\frac{-1}{p_m}\right) & 1 & 0 & \cdots & 0 \\
\left(\frac{\ell_1}{p_1}\right) & \left(\frac{\ell_1}{p_2}\right) & \cdots & \left(\frac{\ell_1}{p_m}\right) & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
\left(\frac{\ell_n}{p_1}\right) & \left(\frac{\ell_n}{p_2}\right) & \cdots & \left(\frac{\ell_n}{p_m}\right) & 0 & 0 & \cdots & 1 \\
\left(\frac{\ell_{n+1}}{p_1}\right) & \left(\frac{\ell_{n+1}}{p_2}\right) & \cdots & \left(\frac{\ell_{n+1}}{p_m}\right) & 0 & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
\left(\frac{\ell_{s_0}}{p_1}\right) & \left(\frac{\ell_{s_0}}{p_2}\right) & \cdots & \left(\frac{\ell_{s_0}}{p_m}\right) & 0 & 0 & \cdots & 0
\end{pmatrix}.$$

• When L/$\mathbb{Q}$ is a real quadratic extension, then to obtain the matrix, simply remove the $(m+1)$st column of the above matrix A.
Observe that if we take $S_\infty = \emptyset$, then simply remove the first row and the $(m+1)$st column of A.

References

[1] L. J. Federer, *Genera theory for S-class groups*, Houston J. Math. **12, 4** (1986), 497-502.

[2] C. Frei, D. Loughran, R. Newton, *Distribution of genus numbers of abelian number fields*, Journal of the London Mathematical Society **107** (2023), 2197-2217.

[3] Y. Furuta, *The genus field and genus number in algebraic number field*, Nagoya Math. J. **29** (1967), 281-285.

[4] G. Gras, Class Field Theory, From Theory to Practice, corr. 2nd ed., Springer Monographs in Mathematics, Springer (2005), xiii+507 pages.

[5] G. Gras, A. Munnier, *Extensions cycliques T-totalement ramifiées*, Publ. Math. Besançon, 1997/98.

[6] H. Hasse, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3** (1951), 45-51.

[7] J.-F. Jaulent, *L'arithmétique des ℓ-extensions*, Publ. Math. Fac. Sci. Besançon, Fascicule 1 (1986).

[8] H. Koch, A.N. Parshin, and I.R. Săfarevič Eds., Number theory II, Encycl. of Math.Sci., vol. 62, Springer-Verlag 1992; Algebraic Number theory, second edition 1997.

[9] H. W. Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9** (1953), 351-362.

[10] C. Maire, *Finitude de tours et p-tours T-ramifiées modérées, S-décomposées*, J. Théor. Nombres Bordeaux **8** (1996), no. 1, 47-73.

[11] C. Maire, *Genus theory and governing fields*, New York J. Math. **24** (2018), 1056-1067.

April 14, 2025

ROSLAN IBARA NGIZA MFUMU, Faculté des Sciences et Techniques, Université Marien Ngouabi, Brazzaville, Republic of Congo & Université Marie et Louis Pasteur, CNRS, Institut FEMTO-ST, 25000 Besançon, France • *E-mail :* `ribarang@univ-fcomte.fr, roslancello7@gmail.com`

CHRISTIAN MAIRE, Université Marie et Louis Pasteur, CNRS, Institut FEMTO-ST, 25000 Besançon, France • *E-mail :* `christian.maire@univ-fcomte.fr`