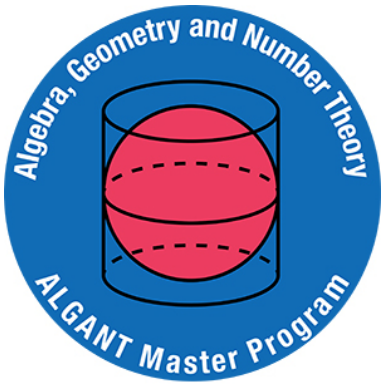
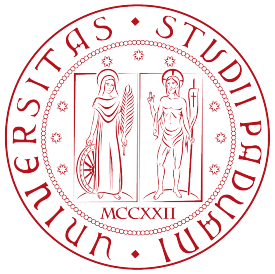


ALGANT Master Thesis in Mathematics

CHARACTERIZING NUMBER FIELDS WITH QUADRATIC L-FUNCTIONS

Matteo Pintonello

Advised by Prof. Bart de Smit



UNIVERSITÀ DEGLI STUDI DI
PADOVA

UNIVERSITEIT
LEIDEN

Academic year 2017/2018
25 June 2018

Acknowledgements

First and foremost I would like to thank my advisor Bart de Smit for helping me and clarifying all my questions, from the silliest ones to the tougher problems. I am extremely grateful to him for proposing me a Thesis with deep links to Group Theory. I also thank the Reading Committee, composed by Prof. R. Griffon and Prof. M. Bright, for having given me a lot of useful corrections.

A huge thanks to my family: you have always supported me in pursuing my dreams. There are no words to express how thankful I am to you.

I have to thank all the people that made this year in Leiden the best time of my life: the great "Italian group", all the friends from boardgame night and all my ALGANT colleagues. I have to address a special mention to three people: to Sergej, for having been like a brother during this year; to Guillermo, for being a wonderful flatmate and friend and to Francesco, for the countless times you have helped me, academically and not, that I will never forget.

Great thanks to the ALGANT consortium and all the professors of Padova and Leiden that have accepted me as a student and helped me during my career. I also thank Indam and Erasmus programme for helping me, and many other students, in our careers and our lives.

Last but not least, great thanks you to my grandparents, uncles and aunts and to all my friends in Italy, from "Carusi" to High school, from University to D&D. Arriving at this point without you would have been incredibly harder.

Contents

Introduction

The first person to introduce an L-function was Leonhard Euler, who introduced the Riemann zeta function as $\zeta(k) = \sum_{n=1}^{\infty} n^{-k}$, even if the first one to define a generalization of this infinite sum and calling it as "L-function" is Dirichlet. In all these series the variable was real; the first one to use complex variables is B. Riemann in his studies on the zeta function. After the breakout of class field theory, Kummer introduced the zeta function of a cyclotomic field (then generalized by Dedekind to arbitrary algebraic extensions) to study the class number of certain number fields. The application to class field theory was very effective: Hecke used the Weber L-function to prove essential results of *abelian* class field theory.

In 1923 Emil Artin hoped, by introducing his Artin L-function, to get results similar to those of Hecke but for *non-abelian* extensions $\mathbb{L}/\mathbb{K}$. This is often considered the first L-function defined as an infinite product instead of as a series. His plan will not have success, but this was an essential step towards the development of the Artin reciprocy law.

The L-functions started to be used more and more often in number theory proofs. For example, in 1880 Kronecker asked if it is possible to determine a number field from the way its primes split. The first, negative, answer to this question is due to Gassmann, even if a more complete theorem was published by Perlis in 1977: two fields are arithmetically equivalent if and only if their Dedekind zeta functions are equal. The proof given by Perlis shows another equivalent property: the Galois groups of the two fields must be in a Gassmann triple. This purely group-theoretical notion was defined by Gassmann in [7] and it had many applications to different areas of mathematics. This connection between number theory and group theory inspired some more results concerning L-functions.

Dedekind zeta functions are a particular instance of Artin L-functions. An Artin L-function associated with the Galois extension $\mathbb{L}/\mathbb{K}$ is $L(s, \rho, \mathbb{L}/\mathbb{K})$, where s is a complex variable and ρ is a representation of the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. When the representation ρ is the 1-dimensional trivial representation, we get exactly the definition of the Dedekind zeta function. As the zeta function doesn't characterize the isomorphism type of the number field, an immediate question is if there is always an Artin L-function characterizing the field. An answer to this question has been given by Bart de Smit in the article [5]: for every $k \geq 3$ there is a one dimensional representation χ of order k of the group $G_{\mathbb{K}}$, absolute Galois group of the field $\mathbb{K}$, such that for every number field $\mathbb{L}$ having a character χ' satisfying $L(\chi, \mathbb{K}/\mathbb{Q}) = L(\chi', \mathbb{L}/\mathbb{Q})$, then $K \cong \mathbb{L}$. The aim of this work is to generalize this result, trying to answer the same question when $k = 2$.

In Chapter 1 we give the basic results that we will use in the rest of the work. In particular we will prove that the Galois group of the Galois closure of a tower of extensions can be always embedded in a wreath product of Galois groups. We will then define the Artin L-functions and we will state their main properties. In the

end of the chapter we will introduce the definition of Gassmann triple and state Perlis' Theorem.

In Chapter 2 we will first prove the main Theorem of B. de Smit, which is the original beginning of this Thesis. In particular, we will prove a Lemma that will allow us to study the problem of L-series in a purely group theoretical way. After the first section, we will get some new results. The main new Theorem of this section is the following one:

Theorem. *Let $\mathbb{K}$ be a number field. Then there are two linear characters $\chi_1, \chi_2 \in \breve{G}_{\mathbb{K}}^{ab}$ of order 2 such that, if $\mathbb{L}$ is a number field with $\chi_1', \chi_2' \in \breve{G}_{\mathbb{L}}^{ab}$ such that $L_{\mathbb{L}}(\chi_1') = L_{\mathbb{K}}(\chi_1)$ and $L_{\mathbb{L}}(\chi_2') = L_{\mathbb{K}}(\chi_2)$, then $\mathbb{L} \cong \mathbb{K}$.*

We will then prove a similar result, with the use of a unique quadratic character but with the additional condition of the equality of the zeta functions.

In Chapter 3 we will discuss whether it is possible to get the same result as B. de Smit's Theorem, so using only *one* character, but with $k = 2$. In the first part we will prove that, under the condition that the Galois group of the Galois closure $\mathbb{N}$ of $\mathbb{K}$ has no non-trivial Gassmann triples containing $\mathrm{Gal}(\mathbb{N}/\mathbb{K})$, it is possible to find an appropriate character to distinguish the isomorphism class of the number field $\mathbb{K}$ from every other isomorphism class of number fields. With the help of MAGMA we will prove that, without the hypothesis of having no non-trivial Gassmann triples, the Theorem would be false:

Theorem. *If $\mathbb{K} = \mathbb{Q}[\sqrt[8]{5}]$, for every quadratic character χ of the absolute Galois group $G_{\mathbb{K}}$ there is another number field $\mathbb{L}$, not isomorphic to $\mathbb{K}$, with a character χ' of $G_{\mathbb{L}}$ such that $L_{\mathbb{K}}(\chi) = L_{\mathbb{L}}(\chi')$.*

We will also show that the number field we use in our counterexample is of minimal possible degree.

Chapter 1

Preliminary Notions

1.1 Galois Closures and Wreath product

In the following chapters we will face the problem of working with the Galois closures of certain extensions. We will have a number field $\mathbb{K}$ of degree n with Galois closure $\mathbb{N}$; we will then consider an extension $\mathbb{K}_\chi$ of $\mathbb{K}$ of degree k. At priori we don't know anything about the degree of the Galois closure $\mathbb{M}$ of the compositum of $\mathbb{K}_\chi$ and $\mathbb{N}$, the aim of this paragraph is to provide a bound on the degree and to give a characterization of the Galois group $\mathrm{Gal}(\mathbb{M}/\mathbb{Q})$. In order to achieve this, we will need some properties of permutation groups.

A permutation group is a couple (G,X) where G is a group acting on a set X. We can define an embedding of permutation groups (G,X) to (G',X') as an injective group homomorphism $G \to G'$ with a G-equivariant bijection $X \to X'$. As usual, there is a natural morphism from G to $\mathrm{Sym}(X)$, we will denote by $G|_X$ the image of G under this morphism. Another interesting construction is the *wreath product* of two permutation groups (G,X) and (H,Y). Define $G^Y = \mathrm{Map}(Y,G)$ as the group of maps of sets from Y to G. This group acts on $X \times Y$ by acting in the first component: $f(x,y) = (f(y)x,y)$ for all $x \in X, y \in Y, f \in G^Y$. The group H acts on $X \times Y$ on the second coordinate and we can also define an action on G^Y by defining $(h \cdot f)(y) = f(h^{-1}(y))$ for all $h \in H, y \in Y$ and $f \in G^Y$. It is easy to verify that $G^Y \rtimes H$ can act on $X \times Y$ by composing these two actions $(f,h)(x,y) = (f(h(y))x, h(y))$; we will denote this permutation group as $G \wr H$.

Let G act both on Z and Y and suppose we have a surjective map $p : Z \to Y$ of G-sets. Suppose moreover that the action of G on Y is transitive. Define $W \leq \mathrm{Sym}(Z)$ as the group of elements $w \in \mathrm{Sym}(Z)$ that satisfy these two properties:

- there is a $g \in G$ such that for every $z \in Z$ we have $p(w(z)) = gp(z)$ (that means w permutes the fibers of p and the element of $\mathrm{Sym}(Y)$ that it induces is in $G|_Y$);
- for every $y \in Y$ there is $g \in G$ such that for every $z \in p^{-1}(y)$ we have $w(z) = gz$ (w acts as a multiplication by an element of G on each fiber).

Such W is a permutation group acting on Z and it is clear that every element of $G|_Z$ satisfies both properties, so $G|_Z$ is a permutation subgroup of W.

Theorem 1.1.1. *In the situation above, fix $y_0 \in Y$ and let $X = p^{-1}(y_0) \leq Z$, $H \subseteq G$ be the stabilizer of y_0. The permutation group (W,Z) is isomorphic to $(H|_X \wr G|_Y, Z)$ and the permutation group $(G|_Z, Z)$ is isomorphic to a subgroup of this wreath product.*

Proof. First of all, as H stabilizes y_0, H acts on X by permuting its elements. We can now notice that the map $f : G \to Y$ given by $g \to gy_0$ is surjective as the

action of G on Y is transitive, therefore there exists a right inverse s, which satisfies $f(s(y)) = s(y)y_0 = y$ for every $y \in Y$. Define now a map $\phi : X \times Y \to Z$ in this way: $\phi(x, y) = s(y)x$. The image of the set $X \times \{y\}$ under ϕ is the set $s(y)X$, and

$$p(s(y)X) = s(y)p(X) = s(y)y_0 = y,$$

so $\phi(X \times \{y\}) \subset p^{-1}(y)$. This is indeed an equality because for every $z \in p^{-1}(y)$ we have $p(s(y)^{-1}z) = s(y)^{-1}p(z) = s(y)^{-1}y = y_0$, so $s(y)^{-1}z \in X$. As p was surjective, it follows that ϕ surjects on Z too. This map is also injective: if $\phi(x, y) = \phi(x', y')$, then both points are in the same fiber so $y = y'$ and therefore $s(y)x = s(y')x'$ only if $x = x'$ too, proving the injectivity. As the wreath product $H|_X \wr G|_Y$ of the permutation groups (H, X) and (G, Y) acts on $X \times Y$, through the map ϕ we get a morphism from $H|_X \wr G|_Y$ to $\mathrm{Sym}(Z)$.

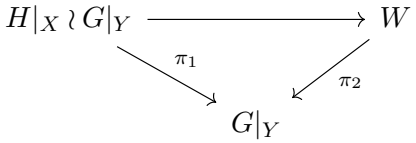
We check that the image of $H|_X \wr G|_Y$ in $\mathrm{Sym}(Z)$ is contained in W. Let $\bar{t} \in G|_Y$ and $f \in \mathrm{Map}(Y, H|_X)$. An element $w = (f, t) \in H|_X \wr G|_Y$ acts on $(x, y) \in X \times Y$ as $(f, t)(x, y) = (f(ty)x, ty)$ and this leads to

$$(f, t)(z) = s(ty)f(ty)x \qquad \text{for } z = \phi(x, y).$$

To check that the image of $H|_X \wr G|_Y$ is a subgroup of W, we verify that every element of the wreath product satisfies the two conditions of the definition of W. To check the first one we have to find a $g \in G$ such that for every $z = \phi(x, y)$ we have the equality $p(w(z)) = p(s(ty)f(ty)x) = gp(s(y)x) = gp(z)$, but recalling that $p(s(y)x) = y$ for every $x \in X, y \in Y$, as $f(ty)x \in X$, we get $ty = gy$ so the first condition is satisfied with $g = t$.

For the second condition, fix $y \in Y$; we have to prove that there is a $g \in G$ such that for every $z \in p^{-1}(y)$ (notice that this implies $z = s(y)x$ for a certain $x \in X$) we have $s(ty)f(ty)x = gs(y)x$. Taking $g = s(ty)f(ty)s(y)^{-1}$ we have that the equality is satisfied. This g is an element of G independent from x so this is well defined.

We still need to prove that the map from $H|_X \wr G|_Y$ to W is surjective. Both groups surject to $G|_Y$: the first one by considering the quotient by $(H|_X)^Y$, the second by considering the induced element of $\mathrm{Sym}(Y)$ (that by the first part of the definition of W is in $G|_Y$) and using that $G|_Y \leq W$. Looking at the proof that the wreath product satisfies the first condition of the definition of W, we have as a consequence that the diagram



commutes, so we only need to prove that the kernel of π_2 can be lifted to the kernel of π_1, which is $\mathrm{Map}(Y, H|_X)$. If $w \in \ker(\pi_2)$, by the second property of W, fixed any $y \in Y$ there exists a $g_y \in G$ such that $w(s(y)x) = g_y s(y)x$ for every $x \in X$. As w is in $\ker(\pi_2)$, we know that the action of w moves the elements of Z within the same fiber over y so we can write $w(s(y)x) = s(y)x'$ for $x' \in X$. We would like to define a function $f \in \mathrm{Map}(Y, H|_X)$ such that $w(s(y)x) = s(y)f(y)x$. This equality is clearly satisfied if we choose $f(y) = s(y)^{-1}g_y s(y)$, but we have to check that this element of G is in H, so that it stabilizes y_0. This is indeed true as $s(y)^{-1}g_y s(y)y_0 = y_0$ if and only if $g_y(s(y)y_0) = s(y)y_0$, that by definition of s is the same as $g_y(y) = y$. This is true as

$$g_y(y) = g_y(p(s(y)x)) = p(g_y(s(y)x)) = p(s(y)x') = y.$$

For every $w \in \ker(\pi_2)$ we have therefore found an $f_w \in \mathrm{Map}(Y, H|_X)$ that acts on Z in the same way as w. It is now clear that the map is surjective: every element of W can be written as gw for $g \in G$ and $w \in \ker(\pi_2)$. The element $(f_w, g) \in H|_X \wr G|_Y$ goes to gw by definition.

With this discussion we have proved that $H|_X \wr G|_Y \cong W$; the statement that $(G|_Z, Z)$ can be embedded in the wreath product is now immediate as this permutation group is a permutation subgroup of (W, Z) as we noticed before.

□

We would like to apply the previous Theorem to Galois groups. If $\mathbb{K}/\mathbb{F}$ is a field extension, we will say that $\mathbb{N}$ is the normal closure of $\mathbb{K}$ over $\mathbb{F}$ if $\mathbb{N}$ is a normal field extension of $\mathbb{F}$ generated by the images of the $\mathbb{K}$-embeddings $\mathbb{F} \to \mathbb{N}$; this normal closure is unique up to isomorphism. In this case we will write $G_{\mathbb{K}/\mathbb{F}}$ to denote the Galois group of the normal closure $\mathbb{N}$ of $\mathbb{K}$ over $\mathbb{F}$. This group acts on the set $X_{\mathbb{K}/\mathbb{F}} := \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{N})$ of the $\mathbb{F}$-embeddings of $\mathbb{K}$ into $\mathbb{N}$ by permuting them in a transitive way. If the degree of the extension $\mathbb{K}/\mathbb{F}$ is finite, it is also equal to the cardinality of $X_{\mathbb{K}/\mathbb{F}}$ is equal. We remark that the isomorphism type of the permutation group $(G_{\mathbb{K}/\mathbb{F}}, X_{\mathbb{K}/\mathbb{F}})$ is not dependant on the choice of $\mathbb{N}$.

Theorem 1.1.2. *Let $\mathbb{F} < \mathbb{K} < \mathbb{L}$ be two finite separable field extensions. The Galois group $G_{\mathbb{L}/\mathbb{F}}$ of the normal closure of $\mathbb{L}$ over $\mathbb{F}$ can be embedded in the wreath product $G_{\mathbb{L}/\mathbb{K}} \wr G_{\mathbb{K}/\mathbb{F}}$ of the Galois groups of the normal closures of $\mathbb{L}$ over $\mathbb{K}$ and of $\mathbb{K}$ over $\mathbb{F}$.*

Proof. Consider $\mathbb{M}$ a Galois closure of $\mathbb{L}$ over $\mathbb{F}$ containing $\mathbb{K}$; now the Galois group $G = \mathrm{Gal}(\mathbb{M}/\mathbb{F})$ acts as usual on the set $Z = \mathrm{Hom}_{\mathbb{F}}(\mathbb{L}, \mathbb{M})$. The group G acts on the quotient $Y = \mathrm{Hom}_{\mathbb{F}}(\mathbb{K}, \mathbb{M})$ of Z and this action is transitive (as every element of the Galois group of the Galois closure of $\mathbb{K}$ over $\mathbb{F}$ can be extended to an element of G). Let $y_0 \in Y$ be the inclusion map of $\mathbb{K}$ in $\mathbb{M}$ and let $H \leq G$ be its stabilizer. The fiber X of elements of Z projecting to y_0 is the subset of Z fixing $\mathbb{K}$, that is $X = \mathrm{Hom}_{\mathbb{K}}(\mathbb{L}, \mathbb{M})$; we know that in this setting H acts on X. We now want to use Theorem 1.1.1, remarking that the permutation group (G, Z) is indeed the Galois group of the Galois closure of $\mathbb{L}$ over $\mathbb{F}$. We have indeed that $(H|_X, X)$ is the subgroup of G that fixes $\mathbb{K}$, so this permutation group is isomorphic to $G_{\mathbb{L}/\mathbb{K}}$ acting on the same set X. Clearly $(G|_Y, Y)$ is the Galois group of the closure of $\mathbb{K}$ over $\mathbb{F}$, hence we get the statement we wanted to prove just by substituting $G_{\mathbb{L}/\mathbb{K}}$ and $G_{\mathbb{K}/\mathbb{F}}$ in the previous Theorem. □

Remark 1.1.3. *Looking at the previous proofs, if $n = [\mathbb{K} : \mathbb{F}]$, we notice that the right square of the diagram*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G_{\mathbb{L}/\mathbb{K}}^n & \longrightarrow & G_{\mathbb{L}/\mathbb{K}} \wr G_{\mathbb{K}/\mathbb{F}} & \longrightarrow & G_{\mathbb{K}/\mathbb{F}} & \longrightarrow & 1 \\ & & & & \uparrow & & \| & & \\ 1 & \longrightarrow & \ker(\pi) & \longrightarrow & G_{\mathbb{L}/\mathbb{F}} & \xrightarrow{\pi} & G_{\mathbb{K}/\mathbb{F}} & \longrightarrow & 1 \end{array}$$

commutes and the two sequences are exact. This is immediate as $G_{\mathbb{L}/\mathbb{F}}$ is a permutation subgroup of the wreath product that surjects to $G_{\mathbb{K}/\mathbb{F}}$.

1.2 Artin L-functions

From now on, we will often work with representations of groups. For us a representation ρ of G is a group homomorphism from G to $\mathrm{GL}(V)$ for V finite dimensional

vector space over $\mathbb{C}$, not the underlying vector space V with the G-action. Two representations are isomorphic if there is a G-equivariant isomorphism between the two underlying vector spaces; if the group G is topological, we also require that ρ is continuous. Every representation has an associated character, defined $\chi_\rho(g) = \mathrm{Tr}(\rho(g))$ and it is a well known fact that, if G is finite, two representations of the same group are isomorphic if and only if their characters are equal. A charachter χ of G is linear if $\chi(1_G) = 1$; it is also well defined the order of the character, that is the minimal positive integer n such that $\chi(g^n) = \chi(1_G)$ for every $g \in G$. We will often call linear characters of order 2 as "quadratic characters" or "quadratic representations". For every representation ρ of H, subgroup of G, it is also well defined the induced representation $\mathrm{Ind}_H^G(\rho)$, that is a representation of G (see [8]).

Let $\mathbb{K}$ be a number field and $\mathbb{L}$ be a finite Galois extension of $\mathbb{K}$ with Galois group G. For every representation $\rho : G \to \mathrm{GL}(V)$ we will define the Artin L-function $L(s, \rho, \mathbb{L}/\mathbb{K})$. In order to define it, we need some facts on decomposition groups and inertia groups.

Let $\mathfrak{p}$ be a prime of $\mathbb{K}$ and $\mathfrak{P}$ a prime of $\mathbb{L}$ lying over $\mathfrak{p}$. We can define the *decomposition group* of $\mathfrak{P}$ as

$$D_\mathfrak{P} := \{\alpha \in G \mid \alpha(\mathfrak{P}) = \mathfrak{P}\} \leq G.$$

This means that $D_\mathfrak{P}$ is the stabilizer of $\mathfrak{P}$ under the action of G and, as G acts transitively on the primes lying over $\mathfrak{p}$, by the orbit-stabilizer Theorem, we have $[G : D_\mathfrak{P}] = g$, where g is the number of primes of $\mathbb{L}$ lying over $\mathfrak{p}$.

Lemma 1.2.1. *The decomposition groups $D_{\mathfrak{P}_i}$ of different primes $\mathfrak{P}_i$ lying over $\mathfrak{p}$ are all conjugate in G.*

Proof. For every $\mathfrak{P}$ prime over $\mathfrak{p}$ we know that, if $\tau \in G$,

$$\tau(\alpha(\tau^{-1}(\mathfrak{P}))) = \mathfrak{P} \Leftrightarrow \alpha(\tau^{-1}(\mathfrak{P})) = \tau^{-1}(\mathfrak{P})$$

and this implies that $\tau\alpha\tau^{-1} \in D_\mathfrak{P}$ if and only if $\alpha \in D_{\tau^{-1}(\mathfrak{P})}$. This proves that $\tau^{-1}D_\mathfrak{P}\tau^{-1} = D_{\tau^{-1}(\mathfrak{P})}$ so using the transitivity of the G-action on the primes lying over $\mathfrak{p}$ we get that all the different decomposition groups of the $\mathfrak{P}_i$ are conjugate. □

The fixed field $\mathbb{F} := \mathbb{L}^{D_\mathfrak{P}}$ is the smallest field such that $\mathfrak{P}$ is the only prime lying over $\mathfrak{P} \cap \mathbb{F}$. Indeed, if that prime does not split in an extension $\mathbb{L}/\mathbb{F}'$, then it is stabilized by the whole $\mathrm{Gal}(\mathbb{L}/\mathbb{F}')$ so this Galois group is contained in $D_\mathfrak{P}$ and thus $\mathbb{F}' \geq \mathbb{F}$. Viceversa, the group $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ acts transitively on the primes lying over $\mathfrak{P} \cap \mathbb{F}$, but the prime $\mathfrak{P}$ is stabilized, therefore the orbit is only of one element.

A consequence of this is that $e(\mathbb{L}/\mathbb{K}) = e(\mathbb{L}/\mathbb{F})$, $f(\mathbb{L}/\mathbb{K}) = f(\mathbb{L}/\mathbb{F})$ (all ramification and inertia degree are of primes lying over $\mathfrak{p}$ and they are equal for all these primes because the extension is Galois). Indeed, $g(\mathbb{L}/\mathbb{K}) = [G : D] = [\mathbb{F} : \mathbb{K}]$, so

$$e(\mathbb{L}/\mathbb{F})f(\mathbb{L}/\mathbb{F}) = [\mathbb{L} : \mathbb{F}] = \frac{[\mathbb{L} : \mathbb{K}]}{[\mathbb{F} : \mathbb{K}]} = \frac{e(\mathbb{L}/\mathbb{K})f(\mathbb{L}/\mathbb{K})g(\mathbb{L}/\mathbb{K})}{[\mathbb{F} : \mathbb{K}]} = e(\mathbb{L}/\mathbb{K})f(\mathbb{L}/\mathbb{K})$$

and, as $e(\mathbb{L}/\mathbb{F}) \leq e(\mathbb{L}/\mathbb{K})$ and $f(\mathbb{L}/\mathbb{F}) \leq f(\mathbb{L}/\mathbb{K})$, we have the equalities we wanted.

Every element of $D_\mathfrak{P}$ induces an automorphism of $\mathrm{Gal}(\overline{\mathbb{L}}/\overline{\mathbb{K}})$, where $\overline{\mathbb{L}}$ and $\overline{\mathbb{K}}$ are the residue fields $\mathcal{O}_\mathbb{L}/\mathfrak{P}$ and $\mathcal{O}_\mathbb{K}/\mathfrak{p}$ respectively. This is clear as every $\alpha \in D_\mathfrak{P}$ fixes

$\mathcal{O}_{\mathbb{L}}$ and $\mathfrak{P}$. Moreover, every such α fixes pointwise $\mathcal{O}_{\mathbb{K}}$ and $\mathfrak{p}$, hence the automorphism $\overline{\alpha}$ of $\mathrm{Gal}(\overline{\mathbb{L}}/\overline{\mathbb{K}})$ induced by α is well defined.

Lemma 1.2.2. *The map $\phi : D_{\mathfrak{P}} \to \mathrm{Gal}(\overline{\mathbb{L}}/\overline{\mathbb{K}})$ that sends α to $\overline{\alpha}$ is a surjective group homomorphism.*

Proof. By easy computations it is clear that the map is a group homomorphism. To prove the surjectivity, we first reduce to the case where we have only one prime lying above $\mathfrak{p}$.

We have noticed that $f(\mathbb{L}/\mathbb{K}) = f(\mathbb{L}/\mathbb{F})$, so $\overline{\mathbb{K}} = \overline{\mathbb{F}}$. For this reason we can always assume that the base field $\mathbb{K}$ is equal to $\mathbb{F}$, the field fixed by the decomposition group, and this group now becomes equal to the whole Galois group of $\mathbb{L}/\mathbb{F}$; moreover the prime $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{\mathbb{F}}$ has only one prime of $\mathbb{L}$ lying over it: the prime $\mathfrak{P}$.

Let $\overline{x}$ be a generator of $\overline{\mathbb{L}}/\overline{\mathbb{F}}$; $x \in \mathcal{O}_{\mathbb{L}}$ a lift of $\overline{x}$ to $\mathbb{L}$ and p the minimal polynomial of x over $\mathbb{F}$. Every element of $\mathrm{Gal}(\overline{\mathbb{L}}/\overline{\mathbb{F}})$ is determined by the image of $\overline{x}$, that must be one root $\overline{y}$ of the minimal polynomial $f_{\overline{x}}$ of $\overline{x}$. In particular $f_{\overline{x}}$ is a factor of $\overline{p}$, reduction modulo $\mathfrak{p}$ of p, therefore $\overline{y}$ is a root of $\overline{p}$ too. As $D_{\mathfrak{P}}$ is now the whole Galois group of $\mathbb{L}/\mathbb{F}$, there is always a $\sigma \in D_{\mathfrak{P}}$ that sends x to y (lifting of $\overline{y}$ to $\mathcal{O}_{\mathbb{L}}$), other root of p, therefore $\phi(\sigma)$ is an element of $\mathrm{Gal}(\overline{\mathbb{L}}/\overline{\mathbb{K}})$ that sends $\overline{x}$ to $\overline{y}$ and this proves the surjectivity of ϕ.

□

Define the *inertia group* as

$$I_{\mathfrak{P}} := \{\alpha \in G | \alpha(x) \equiv x \mod \mathfrak{P} \text{ for all } x \in \mathcal{O}_{\mathbb{L}}\} \leq G;$$

it is clear by the definition that $I_{\mathfrak{P}} \leq D_{\mathfrak{P}}$. We want to show that $I_{\mathfrak{P}}$ is the kernel of the map ϕ.

At priori $\ker(\phi) = \{\alpha \in D_{\mathfrak{P}} | \alpha(x) \equiv x \mod \mathfrak{P} \text{ for all } x \in \mathcal{O}_{\mathbb{L}}\}$. If $\alpha \in G \setminus D_{\mathfrak{P}}$, we show that it cannot be in $\ker(\phi)$, hence the equality. If $\alpha \in G \setminus D_{\mathfrak{P}}$ then $\alpha(\mathfrak{P}) \neq \mathfrak{P}$ and so there is an $x \in \mathfrak{P}$ such that $\alpha(x) \notin \mathfrak{P}$ and in particular $\alpha(x) \not\equiv x \mod \mathfrak{P}$.

We have then established an exact sequence of groups

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \to \mathrm{Gal}(\overline{\mathbb{L}}/\overline{\mathbb{K}}) \to 1$$

hence the isomorphism $D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\overline{\mathbb{L}}/\overline{\mathbb{K}})$. The extension of finite fields $\overline{\mathbb{L}}/\overline{\mathbb{K}}$ is Galois, so it is generated by a Frobenius map that sends x to $x^{N(\mathfrak{p})}$ for every $x \in \overline{\mathbb{L}}$. Let $\mathrm{Frob}_{\mathfrak{P}}$ be an element of $D_{\mathfrak{P}}$ that goes to the Frobenius map under the isomorphism $D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\overline{\mathbb{L}}/\overline{\mathbb{K}})$; we will call $\mathrm{Frob}_{\mathfrak{P}}$ the Frobenius element at $\mathfrak{P}$ and explicitly it is an element such that

$$\mathrm{Frob}_{\mathfrak{P}}(x) \equiv x^{N(\mathfrak{p})} \mod \mathfrak{P} \qquad \text{for all } x \in \mathcal{O}_{\mathbb{L}}.$$

The Frobenius element is defined $\mod I_{\mathfrak{P}}$, so it is uniquely determined if and only if $\mathfrak{p}$ doesn't ramify in $\mathbb{L}$ (so in all but finitely many primes). In the case $\mathfrak{p}$ not ramified it is easier to define the corresponding factor of the Artin L-function because of the following result.

Lemma 1.2.3. *For each $\alpha \in G$ we have*

$$\mathrm{Frob}_{\alpha(\mathfrak{P})} = \alpha \, \mathrm{Frob}_{\mathfrak{P}} \, \alpha^{-1}$$

and in particular all the Frobenius elements of different primes lying over $\mathfrak{p}$ are conjugate in G.

Proof. Let $\alpha \in G$ and $x \in \mathcal{O}_{\mathbb{L}}$. We know that $\mathrm{Frob}_{\mathfrak{P}}(\alpha^{-1}(x)) - \alpha^{-1}(x) \in \mathfrak{P}$ and, letting α act on everything, we have $\alpha(\mathrm{Frob}_{\mathfrak{P}}(\alpha^{-1}(x))) - x \in \alpha(\mathfrak{P})$. As this is true for every $x \in \mathcal{O}_{\mathbb{L}}$ we get that $\alpha\,\mathrm{Frob}_{\mathfrak{P}}\,\alpha^{-1} = \mathrm{Frob}_{\alpha(\mathfrak{P})}$. To get the last result it suffices to use that G acts transitively on the primes lying over $\mathfrak{p}$. □

For this reason in the case $\mathfrak{p}$ unramified $\mathrm{Frob}_{\mathfrak{p}}$ is well defined, the conjugacy class of all the Frobenius symbols $\mathrm{Frob}_{\mathfrak{P}_i}$ for $\mathfrak{P}_i$ primes lying over $\mathfrak{p}$; the conjugacy class $\mathrm{Frob}_{\mathfrak{p}}$ is called the Artin symbol of $\mathbb{L}/\mathbb{K}$ at $\mathfrak{p}$. It is easy to define the $\mathfrak{p}$-th factor of the Artin L-function: it is

$$\left(\det\left(1 - \frac{\rho(\mathrm{Frob}_{\mathfrak{p}})}{N(\mathfrak{p})^s}\right)\right)^{-1} \qquad \text{for } s \in \mathbb{C}.$$

If the prime $\mathfrak{p}$ ramifies, the definition is slightly different. Indeed, the Frobenius symbol is defined only modulo $I_{\mathfrak{P}}$, so instead of considering the whole representation V, we only restrict to the subspace $V_{\mathfrak{P}} \leq V$ where the group $I_{\mathfrak{P}}$ acts trivially. In this way the representation $\rho(\mathrm{Frob}_{\mathfrak{P}})$ assumes the same value whatever representative of the Frobenius symbol we choose. We can say more: the decomposition groups of different primes $\mathfrak{P}_1, \mathfrak{P}_2$ lying over $\mathfrak{p}$ are conjugate and that conjugation sends $I_{\mathfrak{P}_1}$ in $I_{\mathfrak{P}_2}$. This conjugation sends a representative of the Frobenius $\mathrm{Frob}_{\mathfrak{P}_1}$ to a representative of the Frobenius $\mathrm{Frob}_{\mathfrak{P}_2}$. As the different inertia groups are all conjugate in G, the vector space $V_{\mathfrak{P}_i}$ is the same for every $\mathfrak{P}_i$ lying over $\mathfrak{p}$ and on this space the value $\rho(\mathrm{Frob}_{\mathfrak{P}_i})$ is the same for any choice of the prime and any choice of the Frobenius symbol. We can therefore define the $\mathfrak{p}$-th factor of the Artin L-function, in the case $\mathfrak{p}$ ramifies, in this way:

$$\left(\det\left(1 - \frac{\rho(\mathrm{Frob}_{\mathfrak{P}})}{N(\mathfrak{p})^s}\middle| V_{\mathfrak{P}}\right)\right)^{-1} \qquad \text{for } s \in \mathbb{C}.$$

As we have remarked, it is independent of the choice of $\mathfrak{P}$ lying over $\mathfrak{p}$. We can define now the *Artin L-function* of the extension $\mathbb{L}/\mathbb{K}$ attached to the representation ρ as

$$L(s, \rho, \mathbb{L}/\mathbb{K}) := \prod_{\mathfrak{p} \text{ prime of } \mathbb{K}} \frac{1}{\det\left(1 - \frac{\rho(\mathrm{Frob}_{\mathfrak{p}})}{N(\mathfrak{p})^s} | V_{\mathfrak{P}}\right)}$$

that is the product of the $\mathfrak{p}$-th factors defined before (If $V_{\mathfrak{P}} = 0$ the factor has value 1).

Theorem 1.2.4 (Properties of Artin L-function)**.** *The Artin L-function satisfies the following properties:*

1. ***Convergence:*** *The Euler product of an Artin L function converges for all $s \in \mathbb{C}$ such that $Re(s) > 1$;*
2. ***Additivity:*** *If ρ_1, ρ_2 are two representations of the Galois group G of $\mathbb{L}/\mathbb{K}$, then*

$$L(s, \rho_1 \oplus \rho_2, \mathbb{L}/\mathbb{K}) = L(s, \rho_1, \mathbb{L}/\mathbb{K}) L(s, \rho_2, \mathbb{L}/\mathbb{K});$$

3. ***Inflation:*** *If $\mathbb{F} < \mathbb{K} < \mathbb{L}$ is a tower of Galois extensions, every representation ρ of $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ determines a representation $\overline{\rho}$ of $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ by quotient map $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. In this setting we have*

$$L(s, \rho, \mathbb{K}/\mathbb{F}) = L(s, \overline{\rho}, \mathbb{L}/\mathbb{F});$$

4. ***Induction:*** *If $\mathbb{F} < \mathbb{K} < \mathbb{L}$ is a tower of extensions with $\mathbb{L}/\mathbb{F}$ Galois and $G = \mathrm{Gal}(\mathbb{L}/\mathbb{F})$, $H = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, then for every ρ representation of H we have*

$$L(s, \rho, \mathbb{L}/\mathbb{K}) = L(s, \mathrm{Ind}_H^G(\rho), \mathbb{L}/\mathbb{F}).$$

An essential remark is that, for every extension with $\mathbb{K}$ base field, for the induction property we can consider the Artin L-series with the top field equal to $\overline{\mathbb{K}}$, the algebraic closure. In this case every representation ρ of the group $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ is can be factored through the quotient $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})/\ker(\rho)$, that is a finite group because the kernel is always an open subgroup of finite index. Let $\mathbb{L}$ its fixed field; we will write $L_{\mathbb{K}}(s, \rho)$ in place of $L(s, \rho, \overline{K}/K) = L(s, \rho, \mathbb{L}/K)$.

One interesting result is that, if $\rho = \mathbf{1}$ the trivial representation, then we have

$$L(s, \mathbf{1}, \mathbb{L}/\mathbb{K}) = L(s, \mathbf{1}, \mathbb{K}/\mathbb{K}) = \prod_{\mathfrak{p} \text{ prime of } \mathcal{O}_{\mathbb{K}}} \frac{1}{\left(1 - \frac{1}{N(\mathfrak{p})^s}\right)} = \zeta_{\mathbb{K}}(s)$$

where the first equality is because of the inflation property and the last one is exactly the definition of the Dedekind zeta function.

Corollary 1.2.5. *If $\mathbb{K}/\mathbb{F}$ is a finite Galois extension, we have the following decomposition*

$$\zeta_{\mathbb{K}}(s) = \zeta_{\mathbb{F}}(s) \prod_{\rho \neq \mathbf{1}} L(s, \rho, \mathbb{K}/\mathbb{F})^{\dim(\rho)}$$

where the product is over all non-trivial irreducible representations of $G = \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ (up to isomorphism).

Proof. Let G be the Galois group of $\mathbb{K}/\mathbb{F}$ and ρ_{reg} be the regular representation of G. By basic representation theory we have the equalities

$$\mathrm{Ind}_{\mathrm{Gal}(\mathbb{K}/\mathbb{K})}^G(\mathbf{1}) = \rho_{reg} = \bigoplus \rho^{\dim(\rho)}$$

where the sum goes though all the irreducible representations of G up to isomorphism. Using the additivity property and this decomposition, we get

$$\begin{aligned} \zeta_{\mathbb{K}}(s) = L(s, \mathbf{1}, \mathbb{K}/\mathbb{F}) = L(s, \sum_{\rho} \rho^{\dim(\rho)}, \mathbb{K}/\mathbb{F}) = \\ = \prod_{\rho} L(s, \rho, \mathbb{K}/\mathbb{F})^{\dim(\rho)} = \zeta_{\mathbb{F}}(s) \prod_{\rho \neq \mathbf{1}} L(s, \rho, \mathbb{K}/\mathbb{F})^{\dim(\rho)} \end{aligned}$$

where the last equality is due to the fact that $L(s, \mathbf{1}, \mathbb{L}/\mathbb{K}) = \zeta_{\mathbb{K}}(s)$, as remarked before. □

1.3 Characterizing number fields with Dedekind zeta functions

After the definition of the Dedekind zeta function, it is clear that for two isomorphic number fields $\mathbb{K}$ and $\mathbb{L}$ we have that $\zeta_{\mathbb{K}}(s) = \zeta_{\mathbb{L}}(s)$. Every isomorphism of number fields gives a bijection on the set of primes which is norm-preserving, hence the equality of the zeta functions is straight-forward.

An immediate question is if the converse is true or, if not, to what extent the Dedekind zeta function characterizes the extension. The complete answer to this question has been given by Perlis in the articles [12] and [16].

Definition 1.3.1 (Gassmann Triple)**.** *Let G be a finite group and H, H' two subgroups of G. We can say that the triple (G, H, H') is Gassmann if, for every conjugacy class $\mathcal{C}$ of elements of G, we have $|\mathcal{C} \cap H| = |\mathcal{C} \cap H'|$.*

Notice that, if (G, H, H') is a Gassmann triple, the index of H and H' must be equal (because G is the union of all its conjugacy classes) and will be called the *index of the Gassmann triple*. If H and H' are conjugate in G, then they will form a Gassmann triple; all such triples will be called *trivial* Gassmann triples.

Definition 1.3.2 (Arithmetically and Split equivalent fields)**.** *Let $\mathbb{K}$ and $\mathbb{L}$ be two number fields. We will say $\mathbb{K}$ and $\mathbb{L}$ are split equivalent if, for every prime $p \in \mathbb{Z}$ there is a bijection ϕ_p between the set of primes of $\mathcal{O}_\mathbb{K}$ lying above p and the set of primes of $\mathcal{O}_\mathbb{L}$ lying above p.*

We will say $\mathbb{K}$ and $\mathbb{L}$ are arithmetically equivalent if they are split equivalent and the bijection ϕ_p is degree preserving for every prime.

Theorem 1.3.3 (Perlis)**.** *Let $\mathbb{K}$ and $\mathbb{L}$ be number fields and let $\mathbb{N}$ be the normal closure of the compositum. Let $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$, $H = \mathrm{Gal}(\mathbb{N}/\mathbb{K})$, $H' = \mathrm{Gal}(\mathbb{N}/\mathbb{L})$. The following are equivalent:*

- $\zeta_\mathbb{K}(s) = \zeta_\mathbb{L}(s)$*;*
- $\mathbb{K}$ *and* $\mathbb{L}$ *are arithmetically equivalent;*
- $\mathbb{K}$ *and* $\mathbb{L}$ *are split equivalent;*
- (G, H, H') *form a Gassmann triple.*

Sketch of the proof. We will only show the equivalence between the first and last property.

Recalling that $\zeta_\mathbb{K}(s) = L_\mathbb{K}(s, \mathbf{1})$, by Lemma 2.1.2 (that will be proved in the next chapter, without using Perlis' Theorem) we have that the first condition is equivalent to the fact that $\mathrm{Ind}_H^G(\mathbf{1}) = \mathrm{Ind}_{H'}^G(\mathbf{1})$. This condition is clearly equivalent to (G, H, H') being a Gassmann triple: when we compute the induced character of the trivial representation of H on an element $g \in G$ we get $\mathrm{Ind}_H^G(\mathbf{1})(g) = |C_G(g)||H \cap \mathcal{C}|$, where $\mathcal{C}$ is the conjugacy class of g in G. As this is true for H' too, we get that the characters of the two induced representations are equal if and only if $|H \cap \mathcal{C}| = |H' \cap \mathcal{C}|$ for every conjugacy class $\mathcal{C}$ of G, so if and only if (G, H, H') is Gassmann. □

Corollary 1.3.4. *In the notation of the previous Theorem, if $\mathbb{K}$ is Galois, then $\mathbb{K}$ is equal to $\mathbb{L}$.*

Proof. By Perlis' Theorem (G, H, H') form a Gassmann triple, but if K is Galois then H is normal in G. The only Gassmann triple containing H a normal subgroup of G is (G, H, H): H is a union of conjugacy classes so every subgroup H' for which $|\mathcal{C} \cap H| = |\mathcal{C} \cap H'|$ is true for every $\mathcal{C}$ conjugacy class of elements of G must be indeed equal to H. This implies not only an isomorphism but also an equality of $\mathbb{K}$ and $\mathbb{L}$. □

By studying the transitive groups on n elements, Perlis noticed that there are no non-trivial Gassmann triples if $n \leq 6$, so in this case the Dedekind zeta function

characterizes the isomorphism class of the number field. In the article [3] by de Smit and Bosma there is the explicit list of all possible non-trivial Gassmann triples of transitive groups on n elements if $n \leq 15$. In particular we remark that there are no non-trivial Gassmann triple for $n \leq 6$, there is a single Gassmann triple for $n = 7$ (of the group $\mathrm{PSL}(3,2)$ of order 168) and for $n = 8$ there are two groups with non-trivial Gassmann triples (a group of order 32 and one of order 64).

Chapter 2

The two characters case

2.1 Characterizing number fields with one character

In order to study induced representations, we define a monomial structure on a vector space of a representation.

Definition 2.1.1 (Monomial structure)**.** *Let $\rho : G \to \mathrm{GL}(V)$ be a representation of a group G. A monomial structure of G on V is a set $\mathscr{L}$ of 1-dimensional subspaces of V which is G-stable (i.e. $gL \in \mathscr{L}$ for all $g \in G$, $L \in \mathscr{L}$) and such that $V = \bigoplus_{L\in\mathscr{L}} L$. We say that two monomial structures $\mathscr{L}$ and $\mathscr{M}$ of the group G are isomorphic if the two sets are isomorphic as G-sets.*

We remark that, once we choose a basis of V by picking a non-zero vector from each subspace of $\mathscr{L}$, we can see that the action of any $g \in G$ on V is given by a matrix with exactly one non-zero entry in each row and column, usually called generalized permutation matrix or monomial matrix. Moreover, if we have a 1-dimensional representation χ of H with H subgroup of G of index n, then we have a monomial structure on $\mathrm{Ind}_H^G(\chi)$: by the construction, the induced representation acts on n copies of the original 1-dimensional vector space and every $g \in G$ permutes these copies (in the same way it permutes cosets G/H) while acting internally on each one of them. This monomial structure is therefore isomorphic to G/H as a G-set. In particular, if χ_1, χ_2 are two 1-dimensional representations of H subgroup of G, then $\mathrm{Ind}_H^G(\chi_1)$ and $\mathrm{Ind}_H^G(\chi_2)$ give rise to two monomial structures, on two different vector spaces, which are both isomorphic to G/H as G-sets.

We remark that a 1-dimensional representation of a group G is a character of the abelianized group G^{ab}. As usual, these characters form a group, denoted by $\widehat{G^{ab}}$. We will use this notation, usually with $G = G_{\mathbb{K}} = \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ an absolute Galois group of a number field $\mathbb{K}$.

Lemma 2.1.2.

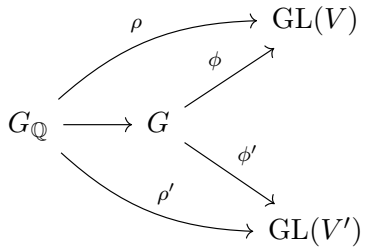
- *Let ρ, ρ' be two representations of $G_{\mathbb{Q}}$; then $L_{\mathbb{Q}}(\rho) = L_{\mathbb{Q}}(\rho')$ if and only if $\rho \cong \rho'$;*
- *If $\mathbb{K}, \mathbb{L} \leq \overline{\mathbb{Q}}$ number fields, if $\chi \in \widehat{G_{\mathbb{K}}^{ab}}$, $\chi' \in \widehat{G_{\mathbb{L}}^{ab}}$ and $L_{\mathbb{K}}(\chi) = L_{\mathbb{L}}(\chi')$, then we have an isomorphism of the two induced representations*

$$\mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi) \cong \mathrm{Ind}_{G_{\mathbb{L}}}^{G_{\mathbb{Q}}}(\chi')$$

  and the two fixed fields $\mathbb{K}_\chi$ of χ and $\mathbb{L}_{\chi'}$ of χ' have the same normal closure over $\mathbb{Q}$.

Proof. If $\rho \cong \rho'$ then clearly $L_{\mathbb{Q}}(\rho) = L_{\mathbb{Q}}(\rho')$.

Let now $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$, $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}(V')$ be two representations of the absolute Galois group $G_{\mathbb{Q}}$ such that $L_{\mathbb{Q}}(\rho) = L_{\mathbb{Q}}(\rho')$. We want to take $\mathbb{K}$ a finite Galois extension of $\mathbb{Q}$ such that there are two maps $\phi : G \to \mathrm{GL}(V)$, $\phi' : G \to \mathrm{GL}(V')$ (with $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$) that make the following diagram commute.



Such a G always exists because there is always an open subgroup of $G_{\mathbb{Q}}$ of finite index contained in the kernels of the two representations, that are open normal subgroups of finite index.

We will now use one of the consequences of Chebotarev Density Theorem (see [15]): for every conjugacy class $\mathcal{C}$ of G the natural density of primes of $\mathbb{Q}$ satisfying $\mathrm{Frob}_p \in \mathcal{C}$ is equal to $|\mathcal{C}|/|G|$ and in particular it is greater than zero. As there is only a finite number of ramified primes in the extension $\mathbb{K}/\mathbb{Q}$, we can assume that every conjugacy class of G contains a Frobenius element of an unramified prime. We can now split the definition of the Artin L-function (with base field $\mathbb{Q}$) in two factors.

$$L(s,\rho,\mathbb{K}/\mathbb{Q}) := \prod_{\substack{p \text{ prime} \\ \text{ramified}}} \frac{1}{\det\left(1 - \frac{\rho(\mathrm{Frob}_p)}{p^s}\middle| V_p\right)} \prod_{\substack{p \text{ prime} \\ \text{unramified}}} \frac{1}{\det\left(1 - \frac{\rho(\mathrm{Frob}_p)}{p^s}\right)}.$$

We want to study in detail the product for p unramified. Computing the determinant, looking at p^{-s} as an indeterminate, we can get a power series of this form

$$\begin{aligned}\det\left(1 - \frac{\rho(\mathrm{Frob}_p)}{p^s}\right)^{-1} &= (1 - \mathrm{Tr}(\rho(\mathrm{Frob}_p))p^{-s} + p^{-2s}(\ldots))^{-1} = \\ &= 1 + \mathrm{Tr}(\rho(\mathrm{Frob}_p))p^{-s} + p^{-2s}(\ldots)\end{aligned}$$

and taking the product for all p prime we have that we can write the L-function as a series

$$L(s,\rho,\mathbb{K}/\mathbb{Q}) = \sum_{n=1}^{\infty} a_n n^{-s}$$

and in particular the coefficient for p prime unramified in $\mathbb{K}$ is $a_p = \mathrm{Tr}(\rho(\mathrm{Frob}_p))$ (while for $\mathfrak{p}$ unramified we cannot conclude anything).

In a similar way we can obtain an expression of the other L-function as a series $L(s,\rho',\mathbb{K}/\mathbb{Q}) = \sum_{n=1}^{\infty} a'_n n^{-s}$ and for the primes unramified in $\mathbb{K}$ we still have $a'_p = \mathrm{Tr}(\rho'(\mathrm{Frob}_p))$. We know that two Dirichlet series are equal if and only if every coefficient is equal (see for example Chapter 11 of [1]), so $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) = \mathrm{Tr}(\rho'(\mathrm{Frob}_p))$ for every p prime unramified in $\mathbb{K}$. Using now Chebotarev's result, we know that every conjugacy class of G contains a Frob_p for p unramified in $\mathbb{K}$, therefore $\mathrm{Tr}(\rho(g)) = \mathrm{Tr}(\rho'(g))$ for every $g \in G$. In particular the two characters associated with the two representations are equal, therefore $\rho \cong \rho'$, as we wanted to prove.

The isomorphism of the second point is straightforward combining the first

point and using the induction property of the L-functions; to complete the proof we need to check that the Galois closure $\mathbb{M}$ of $\mathbb{K}_\chi$ is equal to the fixed field $\mathbb{F}$ of the kernel of $\mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi)$. As $\mathbb{F}$ is Galois over $\mathbb{Q}$ and contains $\mathbb{K}_\chi$ (as it is its Galois closure), then $\mathbb{M} \leq \mathbb{F}$; for the other inclusion notice that every automorphism of $\mathbb{F}$ not fixing $\mathbb{M}$ is indeed in the kernel of $\mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi)$, because $\mathrm{Gal}(\mathbb{F}/\mathbb{M})$ is normal in $\mathrm{Gal}(\mathbb{F}/\mathbb{Q})$ and fixes $\mathbb{K}_\chi$. This proves that $\mathbb{M} = \mathbb{F}$ and, by the isomorphism of the induced representations, it is also the normal closure of $\mathbb{L}_{\chi'}$. □

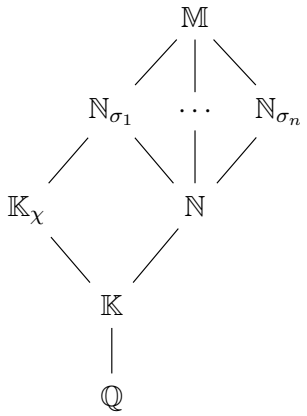
This Lemma allows us to study the problem of studying equalities of L-functions in a completely group theoretical way, as we only have to consider isomorphisms of induced representations. The second part reduces the study to finite groups: we need to consider only the Galois group of the Galois closure of $\mathbb{K}_\chi$, without dealing with the whole absolute Galois group.

To prove the main theorem of this section, we need a Proposition on the existence of certain fields with a chosen Galois group. In the Section 1.1 we proved that certain Galois groups were subgroups of a wreath product; the first step we have to do is to prove that there is always a quadratic extension such that the Galois group of the normal closure is the whole wreath product (that we will write in the more explicit form of semidirect product).

Proposition 2.1.3. *Let C be a finite cyclic group. Given a number field $\mathbb{K}$ of degree n, contained in a Galois extension $\mathbb{N}$ of $\mathbb{Q}$, there exists a Galois extension $\mathbb{M}$ of $\mathbb{Q}$ containing $\mathbb{N}$ such that*

$$\mathrm{Gal}(\mathbb{M}/\mathbb{Q}) = C^n \rtimes G \quad \mathrm{Gal}(\mathbb{M}/\mathbb{K}) = C^n \rtimes H \quad \mathrm{Gal}(\mathbb{M}/\mathbb{N}) = C^n$$

where $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$ and $H = \mathrm{Gal}(\mathbb{N}/\mathbb{K})$. In the semidirect product $C^n \rtimes G$, an element $g \in G$ acts on C^n as a permutation of the cyclic subgroups, in the same way as g permutes the left cosets of G/H by left multiplication. The group $C^n \rtimes H$ is the subgroup of $C^n \rtimes G$ that is generated by C^n and H.



Proof. Let $p \neq 2$ be a prime totally split in $\mathbb{N}$ and let $\mathfrak{p}_1, ..., \mathfrak{p}_n$ be the primes of $\mathbb{K}$ lying over p. As $p \neq 2$, for a consequence of Grünwald-Wang Theorem (see Theorem 5 Chapter 10 of [2]) we know that there is a Galois extension $\widetilde{\mathbb{K}}$ of $\mathbb{K}$ with $\mathrm{Gal}(\widetilde{\mathbb{K}}/\mathbb{K}) = C$ where the prime $\mathfrak{p}_1$ is inert and all the other primes lying over p are totally split.

Define X as the set of field homomorphisms from $\mathbb{K}$ to $\mathbb{N}$; as G acts on $\mathbb{N}$ we can define an action of G on X as $(g \cdot \sigma)(k) = g(\sigma(k))$ for all $g \in G$, $\sigma \in X$, $k \in \mathbb{K}$. Using that G is the Galois group of $\mathbb{N}$ over $\mathbb{Q}$, the action of G on X is transitive; moreover, the only automorphisms that stabilize the natural inclusion map $\iota \in X$ of $\mathbb{K}$ in $\mathbb{N}$ (it

depends on the choice of $\mathbb{N}$) are the automorphisms which fix the whole $\mathbb{K}$, that is the group H. By the orbit-stabilizer Theorem, the set X is isomorphic as G-set to G/H.

Define, for every $\sigma \in X$, $\widetilde{\mathbb{N}}_\sigma := \widetilde{\mathbb{K}} \otimes_{\mathbb{K},\sigma} \mathbb{N}$; we look at $\mathbb{N}$ as a K-algebra through the field homomorphism σ. The two fields $\widetilde{\mathbb{K}}$ and $\mathbb{N}$ are linearly disjoint as $\mathfrak{p}_1$ is inert in $\widetilde{\mathbb{K}}$ but splits completely in $\mathbb{N}$, therefore $\widetilde{\mathbb{N}}_\sigma$ is indeed a field extension of $\mathbb{N}$. The group C acts on $\widetilde{\mathbb{K}}$, so we can define an action of C on $\widetilde{\mathbb{N}}_\sigma$ by letting every element of C act on the first component. This action fixes $\mathbb{N}$ and C acts faithfully. This tells us that we have $|C|$ different automorphisms of $\widetilde{\mathbb{N}}_\sigma/\mathbb{N}$ and therefore this extension is Galois and the Galois group is indeed C.

Define P_σ as the set of primes of $\mathbb{N}$ containing $\sigma(\mathfrak{p}_1)$. The primes of P_σ are inert in $\widetilde{\mathbb{N}}_\sigma$, on the contrary all the primes outside P_σ are totally split both in $\widetilde{\mathbb{K}}$ and in $\mathbb{N}$, so they are totally split in $\widetilde{\mathbb{N}}_\sigma$ too. Now G acts on the set of primes over p by permuting them: as $\mathbb{N}$ is Galois over $\mathbb{Q}$ this action is free (because $\mathfrak{p}$ is totally split) and transitive; moreover the primes in P_ι consist of the primes over $\mathfrak{p}_1$, therefore it is a single H-orbit. By definition of the sets P_σ, we have clearly that $P_{g\sigma} = gP_\sigma$. We want to prove that the sets P_σ are disjoint for $\sigma \in X$. Suppose $\mathfrak{q} \in P_\sigma \cap P_\tau$ for $\sigma, \tau \in X$; as the action of G is transitive on X we can assume $\tau = \iota$. By the transitivity of the action, there is a $g \in G$ such that $g\sigma = \iota$ and therefore $g\mathfrak{q} \in P_\iota$. But therefore $\mathfrak{q}, g\mathfrak{q}$ are both primes of $\mathbb{N}$ lying over $\mathfrak{p}_1$ and, as $H = \mathrm{Gal}(\mathbb{N}/\mathbb{K})$, there is $h \in H$ such that $h\mathfrak{q} = g\mathfrak{q}$. The action of G on the primes is free, so $h = g$ and in particular $\sigma \in H\iota = \{\iota\}$ (H is the stabilizer of ι), so the sets P_σ are disjoint. Now to prove that the $\widetilde{\mathbb{N}}_\sigma$ form a linearly disjoint family of C-extensions of $\mathbb{N}$ we need the following claim.

Claim 2.1.4. *Let L_1, L_2 be two Galois extensions of a number field L. Suppose that there exists a prime $\mathfrak{p}$ of L such that it is inert in L_1 and totally split in L_2. Then the two extensions L_1 and L_2 are linearly disjoint over and so $L_1L_2 = L_1 \otimes_L L_2$.*

Proof of the Claim. Let $\mathfrak{q}$ be a prime of L_1L_2 lying over $\mathfrak{p}$ and let $\mathfrak{q}_1$, $\mathfrak{q}_2$ be the intersections of $\mathfrak{q}$ with L_1, L_2, respectively. As the residue degree is multiplicative in towers of number fields, we have that

$$f(\mathfrak{q}/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{q}_1)f(\mathfrak{q}_1/\mathfrak{p}) = f(\mathfrak{q}/\mathfrak{q}_2)f(\mathfrak{q}_2/\mathfrak{p})$$

As $f(\mathfrak{q}_1/\mathfrak{p}) = [L_1 : L]$, $f(\mathfrak{q}_2/\mathfrak{p}) = 1$ and $1 \leq f(\mathfrak{q}/\mathfrak{q}_2) \leq [L_1 : L]$ we immediately get that $f(\mathfrak{q}/\mathfrak{q}_2) = [L_1 : L]$, therefore $[L_1 : L] = [L_1L_2 : L_2]$ and we have proved the linear disjointness. The other assertions of the claim are always true for linearly disjoint field extensions. □

We can now continue the proof of Theorem 2.1.3. As we know that the sets P_σ are disjoint for $\sigma \in X$ and that the primes in P_σ are inert in $\widetilde{\mathbb{N}}_\sigma$ and totally split in all the other $\widetilde{\mathbb{N}}_\tau$ for $\tau \neq \sigma$, we can apply the claim to the family $\{\widetilde{\mathbb{N}}_\sigma : \sigma \in X\}$ (formally, we would apply it several times adding each extension one by one; to apply the claim more times we use the fact that if a prime is totally split in two extensions it is also totally split in the compositum) and taking the tensor product over $\mathbb{N}$ we can construct an extension $\mathbb{M} = \bigotimes_{\sigma \in X} \widetilde{\mathbb{N}}_\sigma$ of $\mathbb{N}$ with Galois group $\prod_{\sigma \in X} C = C^n$.

We already have an action of G on $\mathbb{N}$ by $y \mapsto gy$ for all $g \in G$, we can extend it for every $\sigma \in X$ to $\tilde{g}_\sigma : \widetilde{\mathbb{N}}_\sigma \to \widetilde{\mathbb{N}}_{g\sigma}$ as $g \cdot (x \otimes y) = x \otimes gy$. All these maps are field isomorphisms because $\tilde{g}_{\sigma^{-1}}\tilde{g}_\sigma$ is the identity, so we can define an action of G letting $g \in G$ act on each factor $\mathbb{N}_\sigma$ as $\tilde{g}_\sigma$. We have an action of C^n and of G on $\mathbb{M}$. By direct

computation it is clear that the action of C commutes with every $\tilde{g}_\sigma$; moreover, we know that G permutes the factors of $\mathbb{M}$ in the same way it permutes the elements of X, or equivalently C^n is isomorphic to G/H as G-set. This proves that the subgroup of Aut($\mathbb{M}$) generated by C^n and G is $C^n \rtimes G$, but the order of this group is $[\mathbb{M} : \mathbb{Q}]$ indeed. This implies that the extension $\mathbb{M}/\mathbb{Q}$ is Galois with $\mathrm{Gal}(\mathbb{M}/\mathbb{Q}) = C^n \rtimes G$. The action of $C^n \rtimes H$ fixes $\mathbb{K}$ and since the order of this subgroup is exactly $[\mathbb{M} : \mathbb{K}]$, we have $\mathrm{Gal}(\mathbb{M}/\mathbb{K}) = C^n \rtimes H$.

□

From now on we will write C_n for the cyclic group of order n (seen as the set of complex n-th root of unity). Using the previous Proposition we get this Theorem of Bart de Smit.

Theorem 2.1.5 (B. de Smit)**.** *Let $\mathbb{K}$ be a number field and $k \geq 3$ an integer. There is a linear character $\chi \in \breve{G}_{\mathbb{K}}^{ab}$ of order k such that, if $\mathbb{L}$ is a number field with $\chi' \in \breve{G}_{\mathbb{L}}^{ab}$ satisfying $L_{\mathbb{L}}(\chi') = L_{\mathbb{K}}(\chi)$, then $\mathbb{L} \cong \mathbb{K}$.*

Proof. First of all we want to prove that we can define a $\chi \in \breve{G}_{\mathbb{K}}^{ab}$ such that $\mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi)$ has a single monomial structure.

Let $C = \langle \zeta \rangle$ for $\zeta = e^{2\pi i/k}$, and n, $\mathbb{N}$, G, H as in Proposition 2.1.3; the same Proposition assures us that there exists an extension $\mathbb{M}$ of $\mathbb{K}$ inside $\overline{\mathbb{Q}}$ such that $\widetilde{G} = C^n \rtimes G = \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ and such that $\widetilde{H} = C^n \rtimes H = \mathrm{Gal}(\mathbb{M}/\mathbb{K})$. As the action of H on the cosets G/H always fixes the coset corresponding to H, we can assume, up to reordering the C^n, that H fixes the first C and so the morphism $\varphi : \widetilde{H} \to C$ (looking at C as a subset of $\mathbb{C}^\times$) defined $\varphi(a_1, ..., a_n, h) = a_1$ is well defined and surjective.

The map ϕ is a representation of $\mathrm{Gal}(\mathbb{M}/\mathbb{K}) = \widetilde{H}$ so we can extend this to a 1-dimensional representation χ of $G_{\mathbb{K}}$ (for every $\sigma \in G_{\mathbb{K}}$ we define $\chi(\sigma) := \varphi(\sigma|_{\mathbb{M}})$) so the induced representation $\rho := \mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi)$ is of dimension n. As by construction χ surjected on C and the absolute Galois group $G_{\mathbb{M}}$ is in the kernel, the induced representation ρ can be factored through the group $G_{\mathbb{Q}}/G_{\mathbb{M}} \cong \mathrm{Gal}(\mathbb{M}/\mathbb{Q}) \cong \widetilde{G}$ and on this group the representation ρ acts as $\mathrm{Ind}_{\widetilde{H}}^{\widetilde{G}}(\varphi)$, so it gives rise to a monomial structure $\mathscr{L} = \{L_1, ..., L_n\}$. The G-action on the set $\mathscr{L}$ and the G-action on the n cyclic factors are both isomorphic to the natural G-action on the cosets G/H, so we can choose the indices of the L_i in a way that the two actions (on the lines and on the cyclic factors) are compatible.

It is really easy to describe the action of an element $a = (a_1, ..., a_n) \in C^n$ on $L_i \in \mathscr{L}$: we have $a \cdot L_i = a_i L_i$, so $\mathscr{L}$ is the set of C^n-submodules of the vector space on which ρ acts (the so called character eigenspaces for the action of $\rho(C^n)$). For a precise proof of this statement we have to use the algebraic construction of the induced representation: considering the representation ρ, seen as a group homomorphisms from $\widetilde{G}$ to $\mathrm{GL}(W)$, we can write $W = \bigoplus_{i=1}^n V_i$, where V_i are copies of the vector space $V \cong \mathbb{C}$ on which G acts (through χ). As we have chosen $\mathscr{L}$ to be the monomial structure associated with the induced representation, clearly $V_i = L_i$. In general every $g \in \widetilde{G}$ acts as a permutation σ on the cosets oh $\widetilde{G}/\widetilde{H}$ therefore, after choosing a set of representatives s_i of the cosets, we can always write $gs_i = s_{\sigma(i)}h_i$ for a certain $h_i \in \widetilde{H}$. For such $g \in \widetilde{G}$, the construction of the induced representation is based on the identity

$$g \cdot \left(\sum_{i=1}^n l_i \right) = \sum_{i=1}^n \chi(h_i) l_{\sigma(i)}$$

where $l_i \in L_i$. The computation of this for $g = a = (a_1, ..., a_n) \in C^n$ is easier: we can choose the representatives s_i of the form $s_i = (1, ..., 1, g_i)$, adding the condition that the identity is the representative of $\widetilde{H}$. Then we have

$$a \cdot s_i = (a_1, ..., a_n, 1)(1, ..., 1, g_i) = (a_{\tau(1)}, ..., a_{\tau(n)}, g_i) = \\ = (1, ..., 1, g_i)(a_{\tau(1)}, ..., a_{\tau(n)}, 1)$$

for τ the permutation associated to g_i. As a consequence $\sigma(i) = i$ for every $i = 1, ..., n$ (this was clear as the elements of C^n don't permute the cyclic factors) and that $\chi(h_i) = \chi(a_{\tau(1)}, ..., a_{\tau(n)}, 1) = a_{\tau(1)} = a_i$, as we wanted to prove.

If there was another monomial structure of $G_{\mathbb{Q}}$ on ρ then, factoring again through the quotient $G_{\mathbb{Q}}/G_{\mathbb{M}}$, it would give rise to another monomial structure $\mathscr{M}$ of $\widetilde{G}$; we will prove that $\widetilde{G}$ has a unique monomial structure on W, so $G_{\mathbb{Q}}$ has a single monomial structure on W too.

Given the two monomial structures $\mathscr{L} = \{L_1, ..., L_n\}$ and $\mathscr{M} = \{M_1, ..., M_n\}$ on W, then the trace of $\rho(g)$ for $g \in \widetilde{G}$ (which is the character of the representation) is the same when computed using $\mathscr{L}$ or $\mathscr{M}$ as basis. We remark that for any choice of non-zero vectors $v_i \in L_i$, (resp. $w_i \in M_i$) the trace is the same, so considering $\mathscr{L}$ (resp. $\mathscr{M}$) as basis and not only sets of lines is not ambiguous.

Consider the element $c = (\zeta, 1, ..., 1) \in C^n$; clearly by the previous discussion $\mathrm{Tr}(c) = n - 1 + \zeta$ when computed with the basis $\mathscr{L}$. When we compute this trace with the basis $\mathscr{M}$, we need to recall that the elements on the diagonal could be either zero or a k-th root of unity. Suppose there is an index i such that $cM_i \neq M_i$; then, as by definition of monomial representation every row and column have exactly one non-zero entry, we must have at least another index $j \neq i$ such that $cM_j \neq M_j$ so the trace of c can be sum of at most $n - 2$ k-th root of unity, so its absolute value can be at most $n - 2$. Using the base $\mathscr{L}$ we had that the trace was $n - 1 + \zeta$, whose absolute value is strictly greater than $n - 2$ (in this inequality we use the fact that $k \geq 3$), but this is a contradiction so $cM_i = M_i$ for all $i = 1, ..., n$ and the action of c on $\mathscr{M}$ is trivial. Since by conjugating c by elements of G we can move the root ζ to any of the n cyclic groups, we have that the conjugates of c generate the whole C^n. Therefore the whole group C^n acts trivially on $\mathscr{M}$ and, as $\mathscr{L}$ is the set of character eigenspaces for the action of $\rho(C^n)$, we must have that $\mathscr{M} \subset \mathscr{L}$. As they are both sets with n elements, we have that $\mathscr{M} = \mathscr{L}$ and so $\mathscr{L}$ is the only monomial representation of ρ. We have constructed out representation χ such that its induced representation on $G_{\mathbb{Q}}$ has an unique monomial structure, the one given by the induction.

Now if $L_{\mathbb{L}}(\chi') = L_{\mathbb{K}}(\chi)$ for a certain $\chi' \in \widetilde{G}_{\mathbb{L}}^{ab}$, then by Lemma 2.1.2 we know that $\mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi) \cong \mathrm{Ind}_{G_{\mathbb{L}}}^{G_{\mathbb{Q}}}(\chi')$ as representations of $G_{\mathbb{Q}}$ and so we have two monomial structures on W, vector space underlying both induced representations: the one we had from $\mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi)$ (with a $G_{\mathbb{Q}}$ action isomorphic to the one of $G_{\mathbb{Q}}/G_{\mathbb{K}}$) and the one that $\mathrm{Ind}_{G_{\mathbb{L}}}^{G_{\mathbb{Q}}}(\chi')$ induces through this isomorphism (with a $G_{\mathbb{Q}}$ action isomorphic to $G_{\mathbb{Q}}/G_{\mathbb{L}}$). Now we know that $\rho = \mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi)$ has a unique monomial structure so, as $G_{\mathbb{Q}}$-sets, we have $G_{\mathbb{Q}}/G_{\mathbb{K}} \cong G_{\mathbb{Q}}/G_{\mathbb{L}}$.

The subgroup $G_{\mathbb{K}}$ of $G_{\mathbb{Q}}$ is the stabilizer of the coset $G_{\mathbb{K}}$ of $G_{\mathbb{Q}}/G_{\mathbb{K}}$, so it stabilizes also a coset $gG_{\mathbb{L}}$ of $G_{\mathbb{Q}}/G_{\mathbb{L}}$. This is possible only if $g^{-1}G_{\mathbb{K}}g \subseteq G_{\mathbb{L}}$ and, as $G_{\mathbb{K}}$ and $G_{\mathbb{L}}$ have the same index n in $G_{\mathbb{Q}}$, they are conjugate. To end the proof we use that two subgroups of a Galois group are conjugate in the common Galois closure if and only if the two extensions are isomorphic.

□

In the theorem, to prove the uniqueness of the monomial structure, we have used that $k \neq 2$. There are indeed counterexamples to this statement if $k = 2$. One example is the group $C_2^2 \rtimes C_2 \cong D_4$, the dihedral group on 4 elements. The group D_4 has an irreducible 2-dimensional representation and we can identify this group to the group of simmetries of a square. Defining $D_4 = \langle a, b | a^4 = b^2 = abab = 1 \rangle$, the action of a is a rotation of $\pi/2$ around the origin and the action of b is the reflection through one axis A_1 of the plane. Let A_2 be the line through the origin orthogonal to A_1 and let B_1, B_2 be the two diagonals. The sets $\mathscr{L}_1 = \{A_1, A_2\}$ and $\mathscr{L}_2 = \{B_1, B_2\}$ are two distinct monomial structures for D_4, with a different D_4-action: the reflexion b fixes each one of the lines A_1, A_2 but swaps the two lines B_1, B_2.

This proves that the method of the proof doesn't work if $k = 2$ and $\mathbb{K}$ is any number field of degree 2. Our aim is to determine if and how it is possible to generalize the results of the previous Theorem under the hypothesis of $k = 2$.

2.2 Characterizing number fields with two quadratic characters

The first extension of Theorem 2.1.5 is by using two quadratic characters instead of one. We will see that this stronger assumption will allow us to use the same method of proof as the uniqueness of the monomial structure is guaranteed by the second representation.

The first step is to extend Proposition 2.1.3 to the case where we replace the cyclic group by the Klein group $V = C_2 \times C_2$. We will often look at this group as the subset $\langle -1 \rangle \times \langle -1 \rangle$ of $\mathbb{C}^2$.

Proposition 2.2.1. *Let $V = C_2 \times C_2$. Given $\mathbb{K}$ number field of degree n, contained in a Galois extension $\mathbb{N}$ of $\mathbb{Q}$, there exists a Galois extension $\mathbb{M}$ of $\mathbb{Q}$ containing $\mathbb{N}$ such that*

$$\mathrm{Gal}(\mathbb{M}/\mathbb{Q}) = V^n \rtimes G \quad \mathrm{Gal}(\mathbb{M}/\mathbb{K}) = V^n \rtimes H \quad \mathrm{Gal}(\mathbb{M}/\mathbb{N}) = V^n$$

where $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$ and $H = \mathrm{Gal}(\mathbb{N}/\mathbb{K})$. In the semidirect product $V^n \rtimes G$, an element $g \in G$ acts on V^n as a permutation of the different Klein subgroups, in the same way as g permutes the left cosets of G/H by left multiplication. The group $V^n \rtimes H$ is the subgroup of $V^n \rtimes G$ that is generated by V^n and H.

Proof. The idea of the proof is the same as the Proposition 2.1.3, but to prove the existence of an extension of $\mathbb{K}$ with Galois group V it is not necessary to use Grünwald-Wang Theorem. Let $p, q \neq 2$ be two prime numbers which are totally split in $\mathbb{N}$ (there exists infinitely many for Chebotarev Density Theorem) and $\mathfrak{p}_1, ..., \mathfrak{p}_n$ and $\mathfrak{q}_1, ..., \mathfrak{q}_m$ the primes of $\mathbb{K}$ lying over p and q respectively. As all the ideals $\mathfrak{p}_i, \mathfrak{q}_j$ are pairwise coprime, we can apply the Chinese Remainder Theorem to these ideals. As $p, q \neq 2$ we know that in the domains $\mathcal{O}_\mathbb{K}/\mathfrak{p}_i$; $\mathcal{O}_\mathbb{K}/\mathfrak{q}_j$ there are elements which are not a square so we can find two elements $x, y \in \mathcal{O}_\mathbb{K}$ such that x is not a square modulo $\mathfrak{p}_1$ and it is a square modulo $\mathfrak{p}_2, ..., \mathfrak{p}_n, \mathfrak{q}_1, ..., \mathfrak{q}_m$ and similarly y is not a square modulo $\mathfrak{q}_1$ and it is a square modulo $\mathfrak{p}_1, ..., \mathfrak{p}_n, \mathfrak{q}_2, ..., \mathfrak{q}_m$. Defining $\mathbb{K}^1 = \mathbb{K}[\sqrt{x}]$ and $\mathbb{K}^2 = \mathbb{K}[\sqrt{y}]$, by the claim in the proof of Proposition 2.1.3 we know that these two extensions are linearly disjoint and that the compositum $\widetilde{\mathbb{K}}$ is Galois with Galois group $C_2 \times C_2 = V$. By construction, the prime $\mathfrak{p}_1$ is inert in $\widetilde{\mathbb{K}}$ and all the other primes $\mathfrak{p}_2, ..., \mathfrak{p}_n, \mathfrak{q}_1, ..., \mathfrak{q}_m$ are totally split in $\mathbb{K}^1$ and similarly the prime $\mathfrak{q}_1$ is inert in $\widetilde{\mathbb{K}}$ and all the other primes $\mathfrak{p}_1, ..., \mathfrak{p}_n, \mathfrak{q}_2, ..., \mathfrak{q}_m$ are totally split in $\mathbb{K}^2$.

Let X be the set of field homomorphisms from $\mathbb{K}$ to $\mathbb{N}$. In the same way as in the previous Proposition, we can get a transitive action of G on X by composition and this action is isomorphic to G/H as G-set. We can consider the extensions $\widetilde{\mathbb{N}}_\sigma := \widetilde{\mathbb{K}} \otimes_{\mathbb{K},\sigma} \mathbb{N}$, with $\mathbb{N}$ that has a structure of $\mathbb{K}$-algebra through the embedding σ. We let V act on the first coordinate; this action fixes $\mathbb{N}$ and every element acts "in a different way"so the extension $\widetilde{\mathbb{N}}_\sigma/\mathbb{N}$ is Galois with Galois group V. Every extension $\widetilde{\mathbb{N}}_\sigma$ of $\mathbb{N}$ is of degree 4 contains two quadratic sub-extensions $\widetilde{\mathbb{N}}^1_\sigma := \mathbb{K}^1 \otimes_{\mathbb{K},\sigma} \mathbb{N}$ and $\widetilde{\mathbb{N}}^2_\sigma := \mathbb{K}^2 \otimes_{\mathbb{K},\sigma} \mathbb{N}$, these fields are the one fixed by the action of each one of the two factors C_2 of V. Equivalently, $\widetilde{\mathbb{N}}^1_\sigma = \mathbb{N}[\sqrt{\sigma(x)}]$ and $\widetilde{\mathbb{N}}^2_\sigma = \mathbb{N}[\sqrt{\sigma(y)}]$. Define P_σ as the primes of $\mathbb{N}$ containing $\sigma(\mathfrak{p}_1)$ and Q_σ as the set of primes of $\mathbb{N}$ containing $\sigma(\mathfrak{q}_1)$. All the primes in P_σ are inert over $\widetilde{\mathbb{N}}^1_\sigma$ (resp. all the primes in Q_σ are inert over $\widetilde{\mathbb{N}}^2_\sigma$) whereas all the other primes of $\mathbb{N}$ lying over p, q are totally split in $\widetilde{\mathbb{N}}^1_\sigma$(resp. $\widetilde{\mathbb{N}}^2_\sigma$). The group G acts on the primes over p and q in a free and transitive way and the primes over $\mathfrak{p}_1$ are exactly the primes in P_ι. As $P_{g\sigma} = gP_\sigma$, we have that the sets P_σ are disjoint. In the same way we prove that the sets Q_σ are also disjoint.

By these remarks, we can apply the claim we proved in Proposition 2.1.3 and we get that all the extensions $\widetilde{\mathbb{N}}^1_\sigma, \widetilde{\mathbb{N}}^2_\sigma$ are linearly disjoint over $\mathbb{N}$ for $\sigma \in X$. In particular the compositum $\mathbb{M}$ of these fields has degree 2^{2n} over $\mathbb{N}$. The field $\mathbb{M}$ is also the compositum of the fields $\widetilde{\mathbb{N}}_\sigma$ and so its Galois group over $\mathbb{N}$ is $V^n = C_2^{2n}$.

We can extend the G-action on $\mathbb{N}$ to a G-action on $\mathbb{M}$ in the same way we did in the previous proposition: define, for every $g \in G$, $\sigma \in X$, a field isomorphism $\widetilde{g}_\sigma : \widetilde{\mathbb{N}}_\sigma \to \widetilde{\mathbb{N}}_{g\sigma}$ by letting g act on the second coordinate. We define the action of g on M as the map that acts on each $\widetilde{\mathbb{N}}_\sigma$ as $\widetilde{g}_\sigma$. By direct computation every $\widetilde{g}_\sigma$ is V-equivariant, so the subgroup of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{M})$ generated by V^n and G is $V^n \rtimes G$. For cardinality reasons this is the whole of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{M})$ and $\mathbb{M}/\mathbb{Q}$ is Galois. The action of $g \in G$ on V^n permutes the factors in the same way g permutes the elements of X, or equivalently in the same way g permutes the cosets G/H. To conclude, it suffices to notice that the fixed field $V^n \rtimes H$ is indeed $\mathbb{K}$.

□

We can finally get an analogous of Theorem 2.1.5 with $k = 2$.

Theorem 2.2.2. *Let $\mathbb{K}$ be a number field. There are two linear characters $\chi_1, \chi_2 \in \breve{G}^{ab}_{\mathbb{K}}$ of order 2 such that, if $\mathbb{L}$ is a number field with $\chi'_1, \chi'_2 \in \breve{G}^{ab}_{\mathbb{L}}$ satisfying $L_{\mathbb{L}}(\chi'_1) = L_{\mathbb{K}}(\chi_1)$ and $L_{\mathbb{L}}(\chi'_2) = L_{\mathbb{K}}(\chi_2)$, then $\mathbb{L} \cong \mathbb{K}$.*

Proof. Let $n, G, H, \mathbb{N}$ be as in Proposition 2.2.1 and let $V = C_2 \times C_2$. By the same proposition we know that there exists an extension $\mathbb{M}$ of $\mathbb{K}$, with $\mathbb{M} \leq \overline{\mathbb{Q}}$, such that $\mathrm{Gal}(\mathbb{M}/\mathbb{Q}) = \widetilde{G} = V^n \rtimes G$, $\mathrm{Gal}(\mathbb{M}/\mathbb{K}) = \widetilde{H} = V^n \rtimes H$. The action of G and H on V^n permutes the factors V in the same way the multiplication by G permutes the left cosets G/H. We order the n copies of V in a way such that the action of H fixes a group V (that we can assume to be the first one) and thus we get two group morphisms $\varphi_1, \varphi_2 : \widetilde{H} \to \langle -1 \rangle \subset \mathbb{C}^\times$ such that

$$\varphi_1((a_1, b_1), ..., (a_n, b_n), h) = a_1 \qquad \varphi_2((a_1, b_1), ..., (a_n, b_n), h) = a_2$$

for all $a_1, b_i \in \langle -1 \rangle, h \in H$. For $i = 1, 2$ we can extend ϕ_i to a representation $\chi_i \in \breve{G}^{ab}_{\mathbb{K}}$ and consider $\rho_i = \mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi_i) : G \to \mathrm{GL}(W_i)$. These induced representations factor over $\widetilde{G} = \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ so we get naturally two monomial structures $\mathscr{L}^1 = \{L^1_1, ..., L^1_n\}$ and $\mathscr{L}^2 = \{L^2_1, ..., L^2_n\}$ on W_1 and W_2 respectively. We can reorder the indices of the L^1_i, L^2_i in a way that makes the G-action on the numbering compatible to the G-action on the Klein subgroups. On $\mathscr{L}^1$ we have that an

element $a = ((a_1, b_1), ..., (a_n, b_n)) \in V^n$ acts on L_i^1 by scalar multiplication by a_i, whereas on $\mathscr{L}^2$ the same element a acts on L_i^2 by scalar multiplication by b_i. The proofs of these statements are done in the same way as in Theorem 2.1.5 and this proves that $\mathscr{L}^1$ (resp. $\mathscr{L}^2$) is the set of character eigenspaces for the action of V^n on the vector space W_1 (resp W_2).

The equalities of the L-series imply that $\mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi_1) \cong \mathrm{Ind}_{G_{\mathbb{L}}}^{G_{\mathbb{Q}}}(\chi_1')$ and $\mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi_2) \cong \mathrm{Ind}_{G_{\mathbb{L}}}^{G_{\mathbb{Q}}}(\chi_2')$. As the absolute Galois group $G_{\mathbb{M}}$ is contained in the kernel of $\mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi_1)$ and $\mathrm{Ind}_{G_{\mathbb{K}}}^{G_{\mathbb{Q}}}(\chi_2)$, these representations factor through $G_{\mathbb{Q}}/G_{\mathbb{M}} = \mathrm{Gal}(\mathbb{M}/\mathbb{Q}) = \widetilde{G}$. In the same way $\mathrm{Ind}_{G_{\mathbb{L}}}^{G_{\mathbb{Q}}}(\chi_1')$ and $\mathrm{Ind}_{G_{\mathbb{L}}}^{G_{\mathbb{Q}}}(\chi_2')$ must factor through $G_{\mathbb{Q}}/G_{\mathbb{M}}$ too; let $\mathscr{M}^1$ and $\mathscr{M}^2$ be the two monomial structures that are induced on W_1 and W_2 by $\mathrm{Ind}_{G_{\mathbb{L}}}^{G_{\mathbb{Q}}}(\chi_1')$ and $\mathrm{Ind}_{G_{\mathbb{L}}}^{G_{\mathbb{Q}}}(\chi_2')$ respectively. The two monomial structures are both isomorphic to $G_{\mathbb{Q}}/G_{\mathbb{L}}$ as $G_{\mathbb{Q}}$-sets, so $\mathscr{M}_1 \cong \mathscr{M}_2$ as $G_{\mathbb{Q}}$ sets.

Let $\mathscr{M}^1 = \{M_1^1, ..., M_n^1\}$ be a monomial structure on W_1 and $\mathscr{M}^2 = \{M_1^2, ..., M_n^2\}$ be a monomial structure on W_2; we want to prove that $\mathscr{M}^1 = \mathscr{L}^1$. Consider the element $c = ((-1, 1), (1, 1), ..., (1, 1)) \in V^n$; clearly by definition of the action on $\mathscr{L}^1$, $\mathscr{L}^2$ we have that $\mathrm{Tr}(c) = n - 2$ on W_1 and $\mathrm{Tr}(c) = n$ on W_2. Suppose by contradiction that the action of c moves some lines of $\mathscr{M}^1$. When we consider the action of c on W_2, whose corresponding matrix has trace n, the only possibility is that c is the identity on W_2 also in the base $\mathscr{M}^2$. This leads to a contradiction: $\mathscr{M}^1$ and $\mathscr{M}^2$ are both isomorphic as $\widetilde{G}$-sets, so it cannot be that c fixes every line of $\mathscr{M}^2$ but not of $\mathscr{M}^1$, therefore c must fix all the lines of $\mathscr{M}^1$ too. Now we can consider the element $d = ((1, -1), (1, 1), ..., (1, 1)) \in C^n$. The trace of d computed with the basis $\mathscr{L}^1$ of ρ_1 is clearly n, so d must act as the identity on every line M_i^1 of $\mathscr{M}_1$ too. Therefore $\mathscr{M}^1$ is stabilized by the subgroup generated by the conjugates by G of c and d, that is the whole V^n. This proves that $\mathscr{M}^1 \subset \mathscr{L}^1$ and for cardinality reasons $\mathscr{M}^1 = \mathscr{L}^1$.

Now with the same argument as in the proof of Theorem 2.1.5 we have that the isomorphism of the two monomial structures implies that, for every $\mathbb{L}$ number field with $\chi_1', \chi_2' \in \widetilde{G}_{\mathbb{L}}^{ab}$ such that $L_{\mathbb{L}}(\chi_1') = L_{\mathbb{K}}(\chi_1)$ and $L_{\mathbb{L}}(\chi_2') = L_{\mathbb{K}}(\chi_2)$, we have $\mathbb{L} \cong \mathbb{K}$.

□

2.3 The different order case

We have just proved that it is always possible to characterize the isomorphism type of a number field with two quadratic characters, whereas we still don't know if it is possible only with one. We also knew, by Theorem 1.3.3 that the equality of the zeta functions is not sufficient. We could then ask if the equality of one quadratic character in addition to the two fields being arithmetically equivalent is a sufficient condition.

Theorem 2.3.1. *Let $\mathbb{K}$ be a number field of degree n. There is a linear character $\chi \in \widetilde{G}_{\mathbb{K}}^{ab}$ of order 2 such that, if $\mathbb{L}$ is a number field with $\chi' \in \widetilde{G}_{\mathbb{L}}^{ab}$ satisfying $L_{\mathbb{L}}(\chi') = L_{\mathbb{K}}(\chi)$ and $\zeta_{\mathbb{K}}(s) = \zeta_{\mathbb{L}}(s)$, then $\mathbb{L} \cong \mathbb{K}$.*

Proof. We follow the proof of Theorem 2.1.5 word by word, using $k = 2$, until the paragraph when we want to prove that $\mathscr{L}$ has a unique monomial structure. To recall, $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$ with $\mathbb{N}$ normal closure of $\mathbb{K}$, and there is a number field $\mathbb{M}$ such that $\mathrm{Gal}(\mathbb{M}/\mathbb{Q}) = C_2^n \rtimes G = \widetilde{G}$. We have a monomial structure $\mathscr{L}$ on the

vector space V on which ρ acts and the G-action of those lines is the same as the $\widetilde{G}$-action on the cosets of $\widetilde{G}/\widetilde{H}$.

Let $\mathscr{M} = \{M_1, ..., M_n\}$ be another monomial structure on V, induced by the isomorphism $\mathrm{Ind}_{\widetilde{H}}^{\widetilde{G}}(\chi) \cong \mathrm{Ind}_{\widetilde{H}'}^{\widetilde{G}}(\chi')$. As it is induced by an induced character, the $\widetilde{G}$-action on the lines of $\mathscr{M}$ is equal to the $\widetilde{G}$-action on the cosets $\widetilde{G}/\widetilde{H}'$.

We want to compute, for each $g \in \widetilde{G}$, the number of fixed points of the action of $\widetilde{G}$, both on $\widetilde{G}/\widetilde{H}$ and on $\widetilde{G}/\widetilde{H}'$. We recall that, as $\zeta_{\mathbb{K}}(s) = \zeta_{\mathbb{L}}(s)$, then $(\widetilde{G}, \widetilde{H}, \widetilde{H}')$ is a Gassmann triple, and in particular $|\mathcal{C} \cap \widetilde{H}| = |\mathcal{C} \cap \widetilde{H}'|$ for every conjugacy class $\mathcal{C}$ of elements of $\widetilde{G}$. Let now $\mathcal{C}$ be the conjugacy class in $\widetilde{G}$ of an element $g \in \widetilde{G}$. We have the equalities

$$|\{a \in \widetilde{G} : ga\widetilde{H} = a\widetilde{H}\}| = |\{a \in \widetilde{G} : a^{-1}ga \in \widetilde{H}\}| = |C_{\widetilde{G}}(g)||\widetilde{H} \cap \mathcal{C}| = \\ = |C_{\widetilde{G}}(g)||\widetilde{H}' \cap \mathcal{C}| = |\{a \in \widetilde{G} : ga\widetilde{H}' = a\widetilde{H}'\}|$$

The number of elements which are fixed by the action of g on the cosets $\widetilde{G}/\widetilde{H}$ is equal to the first term of the equality divided by $|\widetilde{H}|$. In the same way, g fixes a number of cosets of $\widetilde{G}/\widetilde{H}'$ equal to the last term of the equality divided by $|\widetilde{H}'|$. As the indices of $\widetilde{H}$ and $\widetilde{H}'$ in $\widetilde{G}$ are both n, the number of fixed points by the actions of every $g \in \widetilde{G}$ on the two different sets of cosets $\widetilde{G}/\widetilde{H}$ and $\widetilde{G}/\widetilde{H}'$ is equal.

In particular, we know that the action of $c = (-1, 1, ..., 1, 1_G)$ fixed every line of $\mathscr{L}$, therefore the action of the same c fixes all cosets of $\widetilde{G}/\widetilde{H}'$ and so all the lines of of $\mathscr{M}$ too. As the G-conjugates of c generate the whole C^n, we have that $\mathscr{M}$ is fixed pointwise by every element of C^n and therefore, as $\mathscr{L}$ is the set of C^n-submodules of V, we have $\mathscr{M} \subseteq \mathscr{L}$. The equality is then obvious by cardinality reasons.

We have proved that the monomial structure on $\mathrm{Ind}_{\widetilde{H}}^{\widetilde{G}}(\chi)$ is the unique one that can be induced by subgroups corresponding to $\mathbb{L}$, so we can conclude as in Theorem 2.1.5 that $\mathbb{K} \cong \mathbb{L}$.

□

Chapter 3

The single character case

3.1 Characterizing number fields with one quadratic character

As we have remarked in the previous chapter, we cannot generalize Theorem 2.1.5 to the case $k = 2$ using the same proof. In this section we will study if it is anyway possible to get the same result, but with some different types of proofs.

In this chapter we fix a number field $\mathbb{K}$ of degree n with Galois closure $\mathbb{N}$ and we write $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$, $H = \mathrm{Gal}(\mathbb{N}/\mathbb{K})$.

Question 3.1.1. *Is there a linear character $\chi \in \breve{G}_{\mathbb{K}}^{ab}$ of order 2 such that, if $\mathbb{L}$ is a number field with $\chi' \in \breve{G}_{\mathbb{L}}^{ab}$ such that $L_{\mathbb{L}}(\chi') = L_{\mathbb{K}}(\chi)$, then $\mathbb{L} \cong \mathbb{K}$?*

To answer this question, by Lemma 2.1.2 we have to determine all the possible groups $\widetilde{G}$ which have G as a quotient subgroup and study their representations. We clearly can assume that the extension $\mathbb{L}$ has degree n (otherwise the induced representation of a 1-dimensional representation would have a dimension different from n and by Lemma 2.1.2 this is not possible) and, by Lemma 2.1.2, that $\mathbb{L}$ is the fixed field of a subgroup of $\widetilde{G}$ of index n.

In the previous chapter we used the group D_4 as a counterexample to the uniqueness of monomial structures but, studying the different characters of this group, we immediately realize that we cannot use it to get a negative answer for Question 3.1.1.

The group D_4 has three different conjugacy classes of subgroups of index 4; let H_1, H_2, H_3 three representatives. For each of these subgroups (all cyclic of order 2), there is a conjugacy class of elements of G that intersects this subgroup but not the other two subgroup. Once we take χ_1, χ_2, χ_3 the only 1-dimensional representations of order 2 of H_1, H_2, H_3 respectively, the induced representation will have a nonzero value one conjugacy class and for that reason the induced representation cannot be obtained as induced representation of other subgroups of index 4. These three representations give an affirmative answer to Question 3.1.1 for $G = D_4$. We provide the character table of these four induced representations.

D_4	$\{1\}$	$\{a^2\}$	$\{a, a^3\}$	$\{b, ba^2\}$	$\{ba, ba^3\}$
$\mathrm{Ind}_{H_1}^{D_4}(\chi_1)$	4	-4	0	0	0
$\mathrm{Ind}_{H_2}^{D_4}(\chi_2)$	4	0	0	-2	0
$\mathrm{Ind}_{H_3}^{D_4}(\chi_3)$	4	0	0	0	-2

The idea of proof for D_4 can be generalized also to other groups G, it suffices the assumption that there are no Gassmann triples containing the subgroup H.

Proposition 3.1.2. *If $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$ has no non-trivial Gassmann triples (G, H, H') of index n containing $H = \mathrm{Gal}(\mathbb{N}/\mathbb{K})$, then Question 3.1.1 has an affirmative answer.*

Proof. Let $\widetilde{G} := C_2 \times G$, $\widetilde{H} := C_2 \times H$; we know that there exist a field extension $\mathbb{M}/\mathbb{N}$ such that $\widetilde{G} := \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ and $C_2 = \mathrm{Gal}(\mathbb{M}/\mathbb{N})$. Let χ be the one dimensional representation of degree 2 of $\widetilde{H}$ which is the extension of the non-trivial representation of C_2. Suppose that there is another field $\mathbb{L}$ with a linear character χ' of its absolute Galois group such that $L_{\mathbb{L}}(\chi') = L_{\mathbb{K}}(\chi)$ (by Lemma 2.1.2 it must be contained in $\mathbb{M}$). We know that this is equivalent to say that $\widetilde{H}' := \mathrm{Gal}(\mathbb{M}/\mathbb{L})$ is a subgroup of index n of $\widetilde{G}$, not conjugate to $\widetilde{H}$, such that $\mathrm{Ind}_{\widetilde{H}}^{\widetilde{G}}(\chi) = \mathrm{Ind}_{\widetilde{H}'}^{\widetilde{G}}(\chi')$.

The first claim is that $\widetilde{H}'$ must be of the form $\widetilde{H}' = C_2 \times H'$ for a certain subgroup H' of G.

The usual formula to compute the character χ of a representation induced on G by a subgroup H of G is the following:

$$\psi(x) = \frac{1}{|H|} \sum_{g \in G} \chi^\circ(g^{-1} x g)$$

where $\chi^\circ(t) = \begin{cases} \chi(t), & \text{for } t \in H \\ 0 & \text{for } t \notin H \end{cases}$. Let ψ be the induced character on $\widetilde{G}$ of the 1-dimensional representation χ and ψ' the induced character of χ' and let c be the embedding in $\widetilde{G}$ of the generator of C_2; this element is central so we can easily compute $\psi(c) = -n$. As $L_{\mathbb{K}}(\chi) = L_{\mathbb{L}}(\chi')$, we know $\psi(x) = \psi'(x)$ for every $x \in \widetilde{G}$, so $\psi'(c) = -n$ and in particular $c \in \widetilde{H}'$ (otherwise $\psi'(c)$ would be zero). As $\widetilde{H}'$ contains the first factor of the direct product, by taking the quotient we get $\widetilde{H}' = C_2 \times H'$ with H' a subgroup of G. Notice that the index of H' in G is equal to the index of $\widetilde{H}'$ in $\widetilde{G}$, so it is equal to n, hence proving the claim.

Now, suppose for a contradiction that $\mathbb{K}$ and $\mathbb{L}$ are not isomorphic, so H and H' cannot be conjugate and by hypothesis they are not in a Gassmann triple. This implies that there is a conjugacy class $\mathcal{C}$ of elements of G such that $|\mathcal{C} \cap H| > |\mathcal{C} \cap H'|$. We can lift every element $g \in G$ to an element of $\widetilde{G}$ in the obvious way; moreover this lift preserves conjugacy classes, so our conjugacy class $\mathcal{C}$ is lifted to a conjugacy class $\widetilde{\mathcal{C}}$ of $\widetilde{G}$ of the same order. In particular $|\widetilde{\mathcal{C}} \cap \widetilde{H}| > |\widetilde{\mathcal{C}} \cap \widetilde{H}'|$.

We can compute directly the character ψ of $\widetilde{G}$ induced by χ for every $x \in \widetilde{\mathcal{C}}$ (to simplify we can assume $x \in \widetilde{\mathcal{C}} \cap \widetilde{H}$):

$$\psi(x) = \frac{1}{|\widetilde{H}|} \sum_{g \in \widetilde{G}} \chi^\circ(g^{-1} x g) = \frac{1}{|\widetilde{H}|} \chi(x) |\widetilde{\mathcal{C}} \cap \widetilde{H}| |C_{\widetilde{G}}(x)| = \frac{1}{|\widetilde{H}|} |\widetilde{\mathcal{C}} \cap \widetilde{H}| |C_{\widetilde{G}}(x)|$$

because $\chi(x) = 1$ and each one of the values of $\widetilde{\mathcal{C}} \cap \widetilde{H}$ is taken exactly $|C_{\widetilde{G}}(x)|$ times by the function χ°. In a similar way

$$\psi'(x) = \frac{1}{|\widetilde{H}'|} \chi'(y) |\widetilde{\mathcal{C}} \cap \widetilde{H}'| |C_{\widetilde{G}}(y)|$$

where $y \in \widetilde{\mathcal{C}} \cap \widetilde{H}'$. Now $|\chi'(y)| = 1$, $|\widetilde{H}'| = |\widetilde{H}|$ and $|C_{\widetilde{G}}(y)| = |C_{\widetilde{G}}(x)|$. As we noticed $|\widetilde{\mathcal{C}} \cap \widetilde{H}| > |\widetilde{\mathcal{C}} \cap \widetilde{H}'|$ so we have

$$\frac{1}{|\widetilde{H}|}|\widetilde{\mathcal{C}} \cap \widetilde{H}||C_{\widetilde{G}}(x)| = |\psi(x)| = |\psi'(x)| = \\ = \frac{1}{|\widetilde{H}'|}|\chi'(y)||\widetilde{\mathcal{C}} \cap \widetilde{H}'||C_{\widetilde{G}}(y)| < \frac{1}{|\widetilde{H}|}|\widetilde{\mathcal{C}} \cap \widetilde{H}||C_{\widetilde{G}}(x)|$$

and this is a contradiction. We have proved that the assumption that $\mathbb{K}$ and $\mathbb{L}$ are not isomorphic is wrong, so $\mathbb{K} \cong \mathbb{L}$ as we wanted to prove. □

Using this Proposition we can rule out a lot of groups from our study. Using the bounds in the article [3] we have an answer to Question 3.1.1 for all the number fields of degree less than or equal to 6, but also for some infinite families of groups.

Corollary 3.1.3. *If G is an abelian group or $G \cong S_n$, then Question 3.1.1 has an affirmative answer.*

Proof. If G is abelian, every subgroup of G is normal so it is itself a union of conjugacy classes. The only possible Gassmann triples are then of the type (G, H, H), and in particular they are trivial, therefore we can always apply Proposition 3.1.2.

Now we would like to study the subgroups of index n of S_n and prove that for $n \geq 7$ they are all isomorphic to S_{n-1} (all these subgroups are clearly conjugate in S_n). By the study of Gassmann triples of small degree of [3], we already know that our Corollary is true if $n \leq 6$.

Let H be a subgroup of S_n of index $n \geq 7$. We know that S_n acts by left multiplication on the set of left cosets of H and this action gives rise to a group homomorphism $S_n \to \mathrm{Sym}(S_n/H) \cong S_n$. The kernel of this morphism is the normal core of H defined as $\bigcap_{g \in S_n} g^{-1}Hg$, which is the bigger normal subgroup of S_n contained in H; the only non-trivial normal subgroup of S_n for $n > 4$ is A_n with index 2 in S_n, so the kernel is trivial and the morphism is injective (and also surjective by cardinality reasons). The map we have obtained is an automorphism of S_n and we know that if $n \neq 2, 6$ then $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$ (a self-contained proof can be found in [11]).

When we restrict the previous map to H, we notice that every element of H fixes the coset $\{H\}$, so we have a morphism from H to $\mathrm{Sym}(S_n/H \setminus \{H\}) \cong S_{n-1}$. As this map is a restriction of the previous one, it is still injective and, as both H and S_{n-1} have cardinality $(n-1)!$, it is an isomorphism. We have now an automorphism of S_n (that is a conjugation map because $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$), that sends H to a subgroup isomorphic to S_{n-1}, so in particular $H \cong S_{n-1}$. Notice that if $n = 6$ then $[\mathrm{Aut}(S_6) : \mathrm{Inn}(S_6)] = 2$ and indeed S_6 has two non-isomorphic conjugacy classes of subgroups of index 6. As all subgroups of S_n isomorphic to S_{n-1} are conjugate, we can apply Proposition 3.1.2 and the Corollary is proved also for $n \geq 7$. □

3.2 A counterexample of minimal degree

As we have noticed in Section 1.3, the number field of smallest degree which admits a non-isomorphic arithmetically equivalent number field has degree 7 and the Galois closure of this field has Galois group isomorphic to $G = \mathrm{PSL}(3,2) = \mathrm{PSL}_3(\mathbb{F}_2)$. With the help of MAGMA, we can notice that G has only two conjugacy classes of subgroups of index 7. We can choose $\mathbb{K}$ a number field of degree 7, with $\mathbb{N}$ its Galois closure, such that $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q}) = \mathrm{PSL}(3,2)$. A proof of the existence of such

a number field can be found in [3]. We can define $H = \mathrm{Gal}(\mathbb{N}/\mathbb{K})$. By Proposition 2.1.3 the group $C_2^7 \rtimes G$ is the Galois group of an extension $\mathbb{M}$ of $\mathbb{Q}$ satisfying $\mathrm{Gal}(\mathbb{M}/\mathbb{K}) = C_2^7 \rtimes H = \widetilde{H}$, with G acting on the cyclic subgroups in the same way as it permutes the cosets G/H. Similarly to what we did in Theorem 2.1.5, we can choose χ to be the quadratic character associated with the "first" cyclic subgroup of $\widetilde{H}$ (the subgroup fixed by the action of H). Let $\mathbb{L}$ a subfield of M, of index 7 over $\mathbb{Q}$, such that $G_{\mathbb{L}}$ has a one dimensional representation χ' satisfying $L_{\mathbb{K}}(\chi) = L_{\mathbb{L}}(\chi')$.

The first thing we want to check is that $\mathbb{L}$ is a subfield of $\mathbb{N}$. This is true if and only if $\widetilde{H}' = \mathrm{Gal}(\mathbb{M}/\mathbb{L})$ contains the subgroup C_2^7 of $\widetilde{G}$. This group is a normal 2-subgroup of $\widetilde{G}$, so it is contained in the intersection of all the 2-Sylow subgroups of $\widetilde{G}$ (usually denoted by $O_2(\widetilde{G})$) and therefore in all the 2-Sylow subgroups of $\widetilde{G}$. As $\widetilde{H}'$ has index 7, it contains a 2-Sylow subgroup of $\widetilde{G}$, so $\mathbb{L}$ is a subfield of $\mathbb{N}$.

Looking at the structure of the subgroups of G, we notice that (G, H, H') is Gassmann for every H, H' subgroups of index 7 of G, therefore $\mathbb{K}$ and $\mathbb{L}$ are arithmetically equivalent. With this additional hypothesis we can apply Theorem 2.3.1 and have that $\mathbb{K} \cong \mathbb{L}$.

We remark that we can apply the same argument to any field of odd degree n such that, if G is the the Galois group of its Galois closure, any two subgroups of index n of G form a Gassmann triple with G itself.

As we have verified that for $n \leq 7$ there are no number fields $\mathbb{K}$ of degree n that give a negative answer to Question 3.1.1, we have to study number fields of degree 8 or more. There are two transitive groups on 8 elements with non-trivial Gassmann triples and they are of order 32 and of order 48; we will study the first case with the help of MAGMA. This group is isomorphic to $C_8 \rtimes V$ and it is encoded in MAGMA libraries with the code `TransitiveGroup(8,15)`.

Let $\mathbb{N}$ be the Galois closure of $\mathbb{K}$, we now define in MAGMA the groups $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$, $H = \mathrm{Gal}(\mathbb{N}/\mathbb{K})$. We fix a quadratic character χ of $G_{\mathbb{K}}$; let $\mathbb{K}_\chi$ the field fixed by its kernel. By Theorem 1.1.2, we know that the Galois group over $\mathbb{Q}$ of the common Galois closure $\mathbb{M}$ of $\mathbb{N}$ and $\mathbb{K}_\chi$ can be embedded in the wreath product $\mathtt{WG} = C_2^8 \rtimes G = C_2 \wr G$; we will later use also the subgroups $\mathtt{WH} = C_2^8 \rtimes H$, $\mathtt{WH2} = C_2^7 \rtimes H$ (the subgroup of `WH` generated by H and all the cyclic subgroups except the one stabilized by H). We build up a list of all possible subgroups, up to conjugacy, of `WG` that surject on G. Notice that we ask the surjection to be through the natural projection `q` because of Remark 1.1.3. The last condition is to remove from the list the group G itself, as this can be easily checked (every induced representation from a quadratic character of H can be obtained also from an induced representation of a character of a subgroup which is in a non-trivial Gassmann triple with H by direct computation) and it would be an exception to the next tests the program will do.

```
sage: G:=TransitiveGroup(8,15);
sage: d:=Degree(G);
sage: H:=Stabilizer(G,1);
sage: WG, emb, embG, q:=WreathProduct(CyclicGroup(2),G);
sage: N:=Kernel(q);
sage: WH:=sub<WG|embG(H),N>;
sage: WH2:=sub<WG|[emb[i+1](Sym(2)!((1,2))): i in [1..d-1]], embG(H)>;

sage: list:=[s`subgroup: s in Subgroups(WG:OrderMultipleOf:=#G) |
      q(s`subgroup) eq G and IsEmpty(Fix(sub<WG|N, embG(H)>
      meet s`subgroup))];
```

We now want to test if any subgroup $\widetilde{G} = \texttt{GG}$ of $\texttt{WG}$ surjecting to G could provide a negative answer to Question 3.1.1. After having fixed $\widetilde{G}$, we will define $\widetilde{H}$, the subgroup of $\widetilde{G}$ fixing $\mathbb{K}$, and $\widetilde{H}_\chi$, the subgroup of $\widetilde{G}$ fixing $\mathbb{K}_\chi$. For every $\widetilde{G}$ we will define the set `badchars`, whose elements are all the induced characters of linear characters of subgroups of index 7 in `GG`, of course not conjugate to $\widetilde{H}$. We have to check if the character $\chi = \texttt{chi0}$ of the representation $\mathrm{Ind}_{\widetilde{H}}^{\widetilde{G}}(\chi)$ is in the set `badchars` of characters induced from other subgroups.

In order to explicitly find χ in the easiest way, we will use some properties of the Artin L-series and of the wreath product. The only two characters of the extension $\mathbb{K}_\chi/\mathbb{K}$ are the trivial one and χ (because the extension is quadratic), so by the factorization of Remark 1.2.5 we have the equality $\zeta_{\mathbb{K}}(s)L(s,\chi,\mathbb{K}_\chi/\mathbb{K}) = \zeta_{\mathbb{K}_\chi}(s)$. Using the induction property to "lift" everything with $\mathbb{Q}$ as base field, we have

$$L_{\mathbb{Q}}(s, \mathrm{Ind}_{\widetilde{H}}^{\widetilde{G}}(\chi))L_{\mathbb{Q}}(s, \mathbf{1}_{\widetilde{H}}^{\widetilde{G}}) = L_{\mathbb{Q}}(s, \mathbf{1}_{\widetilde{H}_\chi}^{\widetilde{G}})$$

where $\mathbf{1}_{\widetilde{H}}^{\widetilde{G}}$ is a short notation for $\mathrm{Ind}_{\widetilde{H}}^{\widetilde{G}}(\mathbf{1})$, also denoted as coset character on $\widetilde{G}$ from $\widetilde{H}$. Using the additivity property, we can get the equality

$$L_{\mathbb{Q}}(s, \mathrm{Ind}_{\widetilde{H}}^{\widetilde{G}}(\chi)) = L_{\mathbb{Q}}(s, \mathbf{1}_{\widetilde{H}_\chi}^{\widetilde{G}} - \mathbf{1}_{\widetilde{H}}^{\widetilde{G}}). \qquad (*)$$

Notice that the representation on the right hand side is indeed a representation, not only a virtual one, because of Lemma 2.1.2. Now we need a way to determine the subgroups $\widetilde{H}$ and $\widetilde{H}_\chi$. We recall some structures that we defined in Theorem 1.1.2. The group $\widetilde{G}$ acts on the set $X_1 = \mathrm{Hom}_{\mathbb{Q}}(\mathbb{K}, \mathbb{N})$ of cardinality 8 (this action factors through the quotient G), but also on the set $X_2 = \mathrm{Hom}_{\mathbb{Q}}(\mathbb{K}_\chi, \mathbb{M})$ of cardinality 16. In this setting $\widetilde{H}$ is the stabilizer of the identity map of the set X_1 and $\widetilde{H}_\chi$ is the stabilizer of the identity map of X_2. We now use that $\widetilde{G}$ is a permutation subgroup of $\texttt{WG} = C_2^8 \rtimes G$: in this group the stabilizers of the two identity maps are respectively $\texttt{WH} = C_2^8 \rtimes H$ and $\texttt{WH2} = C_2^7 \rtimes H$. This is the reason why we define $\widetilde{H} = \texttt{HH} := \texttt{WH} \cap \texttt{GG}$ and $\widetilde{H}_\chi = \texttt{HH2} := \texttt{WH2} \cap \texttt{GG}$.

```
sage: characterizing:=[];
sage: for i in [1..#list] do
       GG:=list[i];
       HH:= WH meet GG; HH2:=WH2 meet GG;
       chi0:=PermutationCharacter(GG,HH2)-PermutationCharacter(GG,HH);
       S:=Subgroups(GG: OrderEqual:=#GG div d);
       badchars:={Induction(chi, GG): chi in LinearCharacters(s‘
           subgroup),
              s in S | not IsConjugate(GG,s‘subgroup,HH)};
       characterizing[i]:= not (chi0 in badchars);
sage: end for;
```

We can now collect in the list `char_gps` all the $\widetilde{G}$ that cannot provide χ as induced character from another subgroup. This list contains four subgroups: two of order 64, one of order 128 and one of order 512; we will refer to these groups as "bad groups".

```
sage: char_gps:=[list[i]: i in [1..#list] | characterizing[i]];
sage: char_gps;
[Permutation group acting on a set of cardinality 16
Order = 64 = 2^6
(1, 9)(2, 10)(5, 13)(6, 14)
...
```

```
Permutation group acting on a set of cardinality 16
Order = 64 = 2^6
(1, 9)(2, 10)(5, 13)(6, 14)
...
Permutation group acting on a set of cardinality 16
Order = 128 = 2^7
(1, 9)(2, 10)(5, 13)(6, 14)
...
Permutation group acting on a set of cardinality 16
Order = 512 = 2^9
(1, 3, 5, 7, 10, 11, 13, 16, 2, 4, 6, 8, 9, 12, 14, 15)
...]
```

In general, once we fix a Galois group $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$, a covering of G is a group $\widetilde{G}$ such that there exists a group homomorphism with image G (or equivalently that G is as a quotient subgroup of $\widetilde{G}$). We know that this condition is necessary in order to have a Galois extension $\mathbb{M}$ of $\mathbb{Q}$ containing $\mathbb{N}$ with Galois group $\widetilde{G}$. Anyway, this condition is often not sufficient: in the case that there doesn't exist any number field $\mathbb{M}$ with Galois group $\widetilde{G}$ we will say that the covering $\widetilde{G}$ of G is *obstructed*.

As an example of an obstructed covering, consider $\mathbb{N}$ a quadratic extension of $\mathbb{Q}$ which is not contained in $\mathbb{R}$. There cannot be extensions of $\mathbb{Q}$ containing $\mathbb{N}$ with Galois group C_4: the conjugation map would be the only element of order 2 of C_4, so it would fix the only quadratic field contained in the extension, which must be $\mathbb{N}$. As $\mathbb{N}$ is not real, it cannot be fixed by the conjugation map, so the covering C_4 of $\mathrm{Gal}(\mathbb{N}/\mathbb{Q}) = C_2$ is obstructed.

We would like to determine explicitly a number field such that its Galois group is G but all the coverings in the list `char_gps` are obstructed.

The first property that a covering must satisfy is the one at infinity primes. Let f be a polynomial whose splitting field over $\mathbb{Q}$ is $\mathbb{N}$. If the field $\mathbb{N}$ is not contained in $\mathbb{R}$, the complex roots of f are symmetric with respect to the real axis, so the Galois group G must contain the complex conjugation map. For the same reason, $\widetilde{G}$ has a complex conjugation map which, when restricted to $\mathbb{N}$, must be equal to the conjugation map of $\mathbb{N}$. In particular, if $\sigma \in G$ is the complex conjugation and we have a candidate group $\widetilde{G}$ which surjects to G, if σ cannot be lifted to an involution of $\widetilde{G}$, then there are no possible extensions of $\mathbb{N}$ with Galois group $\widetilde{G}$.

We now count all the involutions of G up to conjugation, getting 5 elements of the Galois group G that could correspond to a complex conjugation map. We can find the involutions of the different $\widetilde{G}$, groups in `char_gps`, and project these involutions to the ones of G. We print all the original involutions of G that cannot be lifted to another involution of GG; in particular the involutions number 4 or 5 cannot be lifted to an involution of the bad groups of order 128 and 512.

The last line provides the number of fixed points of each involution and we notice that the only involutions with 2 fixed points are indeed the number 4 and 5.

```
sage: invol:=[c[3]: c in Classes(G) | c[1] eq 2];
sage: print "involutions:", #invol, "  not liftable:";
sage: for i in [1..#char_gps] do
     GG:=char_gps[i];
     liftable:={q(x): x in GG | Order(x) eq 2};
     print i, #GG, {j: j in [1..#invol] | not invol[j] in liftable};
sage: end for;
sage: [#Fix(invol[i]): i in [1..#invol]]

involutions: 5   not liftable:
```

```
1 64 {}
2 64 { 3 }
3 128 { 4, 5 }
4 512 { 1, 2, 4, 5 }
[ 0, 4, 0, 2, 2 ]
```

The obstruction at the conjugation map is not sufficient to exclude all the four bad groups at once, therefore we have to use some more obstructions, this time at finite primes $p \in \mathbb{Z}$. Fix p a prime and G an abstract group. We will denote as *p-decomposition couple* a couple (g, x) of elements of G satisfying the following conditions:

- $D = \langle g, x \rangle$ is a 2-generated subgroup of G, $I = \langle g \rangle$ is a normal subgroup of D and the quotient D/I is cyclic;
- the order of g is coprime with p;
- the coset xI is a generator of D/I;
- the elements x, g satisfy $x^{-1}gx = g^p$.

We will say that a couple (g, x) (with associated groups D, I) is equivalent to (g', x') (with associated groups D', I') if there is an $y \in G$ such that $D' = D^y$, $I' = I^y$ (conjugation by y sends D to D' and I to I') and then $y^{-1}xyI' = x'I$. This relation is indeed an equivalence relation on the set of all possible p-decomposition couples (g, x); let $S_p(G)$ be the quotient of this set by the equivalence relation. With a little abuse of notation, we will denote a class of elements of $S_p(G)$ in the same way we denote a p-decomposition couple.

Fix a Galois extension $\mathbb{N}$ of $\mathbb{Q}$ and a prime $\mathfrak{p}$ of $\mathcal{O}_\mathbb{N}$ lying over p. We have proved that there is an exact sequence

$$1 \to I_\mathfrak{p} \to D_\mathfrak{p} \to \mathrm{Gal}(\overline{\mathbb{N}}/\mathbb{F}_p) \to 1$$

where $I_\mathfrak{p}$, $D_\mathfrak{p}$ are the inertia and decomposition groups at $\mathfrak{p}$ of $\mathbb{N}/\mathbb{Q}$ and $\overline{\mathbb{N}} = \mathcal{O}_\mathbb{N}/\mathfrak{p}$. Suppose that the extension of the completions $\overline{\mathbb{N}}/\mathbb{Q}_p$ is tamely ramified; in this case the inertia group $I_\mathfrak{p}$ is cyclic (see Corollary 5.3 in [14]) and of order coprime with p. The group $\mathrm{Gal}(\overline{\mathbb{N}}/\mathbb{F}_p)$ is also cyclic (generated by the Frobenius element) as it is an extension of finite fields, therefore the decomposition group $D_\mathfrak{p}$ is 2-generated, by a generator g of the inertia group and by a lifting $\mathrm{Frob}_\mathfrak{p}$ of the Frobenius element. We also know that for every $x \in I_\mathfrak{p}$ we have $\mathrm{Frob}_\mathfrak{p}^{-1}\, x\, \mathrm{Frob}_\mathfrak{p} = x^p$. It is clear that $(g, \mathrm{Frob}_\mathfrak{p})$ are a p-decomposition couple of G.

Now, let $\mathbb{M}$ be a Galois extension of $\mathbb{Q}$ containing $\mathbb{N}$ and let $\mathfrak{P}$ be a prime of $\mathbb{M}$ lying over $\mathfrak{p}$ (and so lying over p too). If the extension of the completions $\mathbb{M}_\mathfrak{P}/\mathbb{Q}_p$ is tamely ramified, with the same argument as before we have that the decomposition group $D_\mathfrak{P} \leq \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ is 2-generated. The group $D_\mathfrak{P}$ surjects to $D_\mathfrak{p}$: every element d of $D_\mathfrak{P}$ must fix $\mathfrak{p}$ so the projection $\pi(d) \in G$ goes to $D_\mathfrak{p}$; moreover every element of $D_\mathfrak{p}$ can be extended to an element of $D_\mathfrak{P}$ by Galois theory. Aa a consequence, the restriction to $\mathbb{N}$ of the two generators of $D_\mathfrak{P}$ must generate $D_\mathfrak{p}$. In a similar way it is possible to show that $I_\mathfrak{P} = \langle \tilde{g} \rangle$ goes to $I_\mathfrak{p}$ and $\mathrm{Frob}_\mathfrak{P} \in D_\mathfrak{P}$ goes to $\mathrm{Frob}_\mathfrak{p} \in D_\mathfrak{p}$, so the p-decomposition couple $(\tilde{g}, \mathrm{Frob}_\mathfrak{P})$ of $\widetilde{G}$ must be projected to a p-decomposition couple of G, and in particular to a p-decomposition couple equivalent to $(g, \mathrm{Frob}_\mathfrak{p})$.

We can now state in a Lemma the criterion we will use to get obstructions to extensions at finite primes.

Lemma 3.2.1. *Fix p prime and $G = \mathrm{Gal}(\mathbb{N}/\mathbb{Q})$, let $\widetilde{G}$ be a covering of G. Let D and I the decomposition and inertia subgroups of G at $\mathfrak{p}$, prime of $\mathcal{O}_{\mathbb{N}}$ lying over p, x a generator of I and Frob a Frobenius element of D. If there are no couples of $S_p(\widetilde{G})$ such that, once projected to G, are equal to the p-decomposition couple $(x, \mathrm{Frob}) \in S_p(G)$, then the covering $\widetilde{G}$ of G is obstructed.*

We can continue "analyzing the code", where we define two functions `pconj` and `localgps`.

The function `pconj`, that takes as an input the group G and two lists l_1 and l_2 of length 2 each, tests if the two couples $l_1 = (l_1[1], l_1[2])$, $l_2 = (l_2[1], l_2[2])$ define the same element of $S_p(G)$. The first step is to check if the inertia subgroups $I_1 = \langle l_1[1] \rangle$ and $I_2 = \langle l_2[1] \rangle$ are conjugate, providing, in case of a positive output, the element $g \in G$ that moves I_1 to I_2. Then we define $y = g^{-1} l_1[2]\ g$ and check if the projection of y modulo I_2 is conjugate to the projection of $l_2[2]$ modulo I_2 (to reduce the computational cost, we check if the groups are conjugated only by element of the normalizer). The function `pconj` has as an output a boolean value telling if l_1 and l_2 are equivalent inside G.

The other function `localgps`, taking as input a group G and a prime p, provides the set $S_p(G)$, encoded as a list. At first it searches the candidate subgroup I among all non-trivial cyclic subgroups of G, checking if they are of order coprime with p (as we want to consider only tamely ramified extensions). In order to "find the lifting" of the Frobenius element, we take a generator g of I and we check for all the representatives of the cosets of the quotient N/I, with N normalizer of I in G, if $g^p = xgx^{-1}$. If we have found such an x, after checking through the function `pconj` that the p-decomposition couple (g, x) is not equivalent to any p-decomposition couple we had found, we add it to the list L. The output is the list $S_p(G)$.

```
sage: pconj:=function(G,l1,l2)
       I1:=sub<G|l1[1]>; I2:=sub<G|l2[1]>;
       isc,g:=IsConjugate(G,I1,I2);
       if not isc then return false; end if;
       y:=l1[2]^g;
       if not sub<G|l1[1]^g> eq sub<G|l2[1]> then
       print "Problem"; end if;
       Nor:=Normalizer(G,I2);
       NNor,pr:=Nor/I2;
       isc, g2:=IsConjugate(NNor, pr(y), pr(l2[2]));
       return isc;
sage: end function;
sage: localgps:=function(G,p)
     L:=[];
     for I in [s`subgroup: s in Subgroups(G:IsCyclic:=true)|
     (GCD(p, s`order) eq 1) and #s`subgroup ne 1 ] do
       for x in Transversal(Normalizer(G,I),I) do
           g:=Rep({t: t in I| Order(t) eq Order(I)});
           if g^p eq x*g*(x^(-1)) and forall(t){l: l in L |
            not pconj(G,l,<g,x>)} then Append(~L,<G!g,G!x>);
           end if;
       end for;
     end for;
     return(L);
sage: end function;
```

We choose $p = 5$ and we let the function `localgps` act on G, our original Galois group, giving the list `lg` as output. Printing firstly the order of g and then the order of x in the quotient $\langle g, x \rangle / \langle g \rangle$ (that correspond to ramification and residue degree of the extension with $\langle g, x \rangle, \langle g \rangle$ as decomposition and inertia group respectively)

for each couple (g,x) of $S_p(G)$, we notice that the only couples where the order of g (i.e. the ramification degree) is 8 are the couples number 37 and 38.

```
sage: p:=5;
sage: lg:=localgps(G,p);
sage: for i in [1..#lg] do t:=lg[i];
     print i,<#sub<G|t[1]>,Index(sub<G|t[1],t[2]>,sub<G|t[1]>)>;
sage: end for;
1 <2, 1>
2 <2, 4>
3 <2, 2>
4 <2, 2>
5 <2, 2>
...
36 <4, 2>
37 <8, 2>
38 <8, 2>
```

We now let the function `localgps` act on each of the bad groups. We project to G every element of the list `localgps(GG,p)` with `GG` a bad group and check what element of `lg` corresponds to this projection (so what p-decomposition couples of G at p can be lifted to p-decomposition couples of the bad groups). For every bad group, we print the list of elements of `lg` that cannot be lifted. All decomposition groups can be lifted in the third and fourth bad group, but in the first two groups some elements of `lg`, like number 37 and 38, cannot be lifted.

```
sage: for i0 in [1..#char_gps] do
     GG:=char_gps[i0];
     llg:=localgps(GG,p);
     sl:=[0: x in lg];
     for i in [1..#lg] do for t in llg do
         if pconj(G,lg[i],<q(t[1]),q(t[2])>) then
         sl[i]:=sl[i]+1; end if;
     end for; end for;
     print i0,  [i: i in [1..#lg] | sl[i] eq 0];
sage: end for;

1 [ 26, 27, 30, 36, 37, 38 ]
2 [ 26, 27, 30, 36, 37, 38 ]
3 []
4 []
```

We are now ready to give a number field providing a negative answer to Question 3.1.1. We want to remark that the proof of this Theorem is based on the computations we have done in MAGMA.

Theorem 3.2.2. *If $\mathbb{K}=\mathbb{Q}[\sqrt[8]{5}]$, for every quadratic character χ of the absolute Galois group $G_{\mathbb{K}}$ there is another number field $\mathbb{L}$, not isomorphic to $\mathbb{K}$, and a character χ' of $G_{\mathbb{L}}$ such that $L_{\mathbb{K}}(\chi,s)=L_{\mathbb{L}}(\chi',s)$.*

Proof. The field $\mathbb{K}$ has degree 8 over $\mathbb{Q}$ and the minimal polynomial of $\sqrt[8]{5}$ is $f(x)=x^8-5$. With the help of MAGMA it is possible to verify that the Galois closure $\mathbb{N}$ of $\mathbb{K}$ has Galois group $G=C_8\rtimes V$. Out of the 8 distinct roots of the polynomial $f(x)$, two of them are real so the complex conjugation fixes two elements. Looking back at the discussion of the obstructions to extension at the infinity prime, out of all the involutions of G, the only two ones with two fixed points are the fourth and fifth, and in both cases the bad groups of order 128 and 512 are obstructed.

As the Galois group of $\mathbb{N}$ over $\mathbb{Q}$ is a 2-group (of order 32), the extension of the completions $\mathbb{N}_{\mathfrak{p}}/\mathbb{Q}_p$ with respect to the prime $\mathfrak{p}$ lying over $p=5$ is tamely ramified.

With an easy computation we get that the ramification degree of 5 in the extension $\mathbb{N}/\mathbb{Q}$ is equal to 8, so the p-decomposition couple associated with the decomposition group D of the prime $p = 5$ corresponds to the number 37 or 38 of the list `lg` provided before. By the previous discussion, there are no Galois extension of $\mathbb{N}$ with Galois group over $\mathbb{Q}$ equal to one of the two bad groups of order 64.

As we have excluded all the bad groups, there exists always a number field $\mathbb{L}$, non-isomorphic to $\mathbb{K}$, such that every character induced from any character of order 2 of $G_{\mathbb{K}}$ can be induced also from a character of $G_{\mathbb{L}}$. As a consequence, Question 3.1.1 has a negative answer for $G = C_8 \rtimes V$. □

One consequence of this Theorem is that the results we have obtained in Theorems 2.2.2 and 2.3.1 are optimal.

Bibliography

[1] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[2] E. Artin, J. Tate *Class Field Theory*, W.A.Benjamin inc. publishers, 1967.

[3] W. Bosma, B. de Smit *On Arithmetically equivalent Number Fields of small degree*, Algorithmic Number Theory, volume 2369 of Lecture notes in Comp. Sci., Pages 67-79. Springer, Berlin, 2002.

[4] J.W. Cogdell, *On Artin L-function*, `https://people.math.osu.edu/cogdell.1/artin-www.pdf`, 2006.

[5] G. Cornelissen, B. de Smit, X. Li, M. Marcolli, H. Smit, *Reconstructing global fields from Dirichlet L-series*, `https://arxiv.org/abs/1706.04515`, 2017.

[6] B. de Smit, *Galois groups and Wreath Products*, `http://www.math.leidenuniv.nl/~desmit/notes/krans.pdf` , 2007.

[7] F. Gaßmann, Bemerkungen zur Vorstehenden Arbeit von Hurwitz: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppen., Math. Z. 25, 1926.

[8] M. Isaacs, *Character Theory of Finite Groups*, Academic Press, London/New York, 1976.

[9] S. Lang, *Algebraic Number Theory*, Springer-Verlag New York, 1970.

[10] D. Marcus, *Number Fields*, Springer-Verlag New York, 1977.

[11] P.J. Morandi, *Automorphisms of S_n and of A_n*, `http://sierra.nmsu.edu/morandi/notes/AutGroups.pdf` .

[12] R. Perlis, *On the equation $\zeta_k(s) = \zeta'_k(s)$*, Journal of Number Theory, Volume 9, Pages 342-360, 1977.

[13] P. Solomatin, *On Artin L-functions and Gassmann equivalence for Global Function Fields*, `https://arxiv.org/pdf/1610.05600.pdf`, 2016.

[14] P. Stevenhagen, *Local Fields Lecture Notes*, `http://www.math.leidenuniv.nl/~psh/VGT.pdf`, 2018.

[15] P. Stevenhagen, J.H. Lenstra Jr., *Chebotarev and his Density Theorem*, The Mathematical Intelligencer, Vol. 18 no. 2, 1996.

[16] D. Stuart, R. Perlis, *A new characterization of arithmetic equivalence*, Journal of Number Theory, Volume 53, Pages 300-308, 1995.