UNIVERSITAT DE BARCELONA

ADVANCED MATHEMATICS
MASTER'S FINAL PROJECT

Non-existence of mod 2 and mod 3 Galois Representations

Author:
Jon Ferreras

Supervisor:
Luis Dieulefait

Facultat de Matemàtiques i Informàtica

June 13th, 2025

Motivation and Summary

This project studies the non-existence of irreducible Galois representations of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ unramified outside $p = 2$ and $p = 3$. This topic was studied mainly by John Tate ([22]) and J.P. Serre ([18] and [20]), with further results obtained in recent years, but the literature for the original problem consists on very disperse, informal and outdated notes that rely on deep topics or that do not go over the details. Our goal is to provide a simplified proof using everything that has been studied after Tate and Serre introduced it, while including the details needed to follow the proof.

The main tool for this project is the study of local fields and how they ramify, to simplify the problem through an upper bound for the discriminant of extensions introduced by Tate.

In Chapter 1 we introduce everything necessary for the proof of Tate's bound, focusing on local field theory and class field theory.

In Chapter 2 we present the problem and how to work with it locally, and we state and prove Tate's bound (actually a refinement of Tate's original bound by Moon and Taguchi, introduced in [12]).

Chapter 3 focuses on the applications of Tate's bound to $p = 2$ and $p = 3$ and analysing the particular Galois groups and corresponding extensions that arise, to finally prove the non-existence of Galois representations unramified outside these values of p.

Acknowledgements

I would like to express my deepest gratitude to my supervisor, Dr. Luis Dieulefait, for his guidance and support. In the course of the six years I have spent in this faculty, he has taught me essentially everything that I know about number theory; this project is the result of that journey.

I am also profoundly grateful to my parents and friends, who have always supported me throughout my studies. I wish to thank my classmates as well, for their help and collaboration, particularly Xisco and Sergio for their cooperation during the entire master's program.

Contents

Chapter 1
Preliminaries

In this chapter we go over some basic results on algebraic number theory, including the notion of ramification, and then move on to valuations and the construction of local fields, some results regarding ramification in local fields, local class field theory and finishing with some concepts on representations and characters.

1.1 Prime factorization in extensions

In this section we explain the notions of prime factorization and ramification in extensions of number fields L/K. When $K = \mathbb{Q}$, the prime ideals are of primes $p \in \mathbb{Z}$. The results of this section are available in [14], Chapter I.

Let L/K be an algebraic number field extension, $[L : K] = n$, with $\mathcal{O}_L$ and $\mathcal{O}_K$ their corresponding rings of integers. It is well known that $\mathcal{O}_L$ and $\mathcal{O}_K$ are Dedekind domains, that is, Noetherian integral domains, integrally closed in which every non-zero prime ideal is maximal.

Theorem 1.1. *If $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_L$, then there is a unique prime ideal $\mathcal{P} \subset \mathcal{O}_K$ such that $\mathfrak{p}|\mathcal{P}\mathcal{O}_L$, i.e., $\mathcal{P}\mathcal{O}_L \subseteq \mathfrak{p}$.*

The degree f of the extension $(\mathcal{O}_L/\mathfrak{p})/(\mathcal{O}_K/\mathcal{P})$ is called the *inertia index of* $\mathfrak{p}$ or the *residue class degree of* $\mathfrak{p}$ *in* L/K.

Theorem 1.2. *For a prime ideal $\mathcal{P} \subset \mathcal{O}_K$, the ideal $\mathcal{P}\mathcal{O}_L$ of $\mathcal{O}_L$ factorizes uniquely in primes of $\mathcal{O}_L$*

$$\mathcal{P}\mathcal{O}_L = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

Moreover, if f_i is the inertia index of $\mathfrak{p}_i$, then

$$\sum_{i=1}^{g} e_i f_i = n$$

Each of the e_i in the previous theorem is called the *ramification index of* $\mathfrak{p}_i$.

Definition 1.1. We say that L/K is *ramified at* $\mathcal{P}$ if there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ in the factorization of $\mathcal{P}$ such that its ramification index is bigger than one. Otherwise we say that L/K is *unramified at* $\mathcal{P}$, and if $f_i = 1$ for all i as well, we say that $\mathcal{P}$ *splits* in L.

If the extension L/K is a Galois extension, the ramification and inertia indices of each $\mathfrak{p}_i$ do not depend on the ideal. In this situation, we have

$$\mathcal{P}\mathcal{O}_L = \prod_{i=1}^{g} \mathfrak{p}_i^e$$

and $efg = n = [K : \mathbb{Q}]$. From now on, we assume that the extension L/K is a Galois extension, and let $G = Gal(L/K)$.

Let $\mathcal{P}$ be a prime ideal in $\mathcal{O}_K$ and $\mathfrak{p} \subset \mathcal{O}_L$ be a prime in the factorization of $\mathcal{P}$ in $\mathcal{O}_L$.

Definition 1.2. The *decomposition group* $D_\mathfrak{p}$ of $\mathfrak{p}$ is the subgroup of G of elements that fix $\mathfrak{p}$, that is,

$$D_\mathfrak{p} = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

If we let $\lambda = \mathcal{O}_L/\mathfrak{p}$ and $\kappa = \mathcal{O}_K/\mathcal{P}$, there is a natural reduction morphism

$$\phi : D_\mathfrak{p} \to Gal(\lambda/\kappa)$$

which is surjective (because every element in $Gal(\lambda/\kappa)$ fixes $\mathfrak{p}$). We define the *inertia group* of $\mathfrak{p}$ as the kernel of ϕ and we write it as $I_\mathfrak{p}$.

Observation 1.1. The order of the decomposition group is ef for every $\mathfrak{p}$ in the decomposition of $\mathcal{P}$, and the order of the inertia group is e.

Remark 1.1. The definitions of decomposition and inertia group are also valid for infinite extensions of $\mathbb{Q}$ such as $\overline{\mathbb{Q}}/\mathbb{Q}$.

1.2 Valuations and completions

The results of this and the two following sections are available at [14], Chapter II.

Definition 1.3. A *valuation* of a field K is a function

$$|\cdot| : K \to \mathbb{R}$$

such that

1. $|x| \geq 0$ and $|x| = 0$ if and only if $x = 0$
2. $|x||y| = |xy|$
3. $|x + y| \leq |x| + |y|$

A field together with a valuation is called a *valued field*. Defining $d(x, y) := |x - y|$ for $x, y \in K$ turns K into a metric space.

Definition 1.4. A valuation $|\cdot|$ is called *non-archimedean* if $|n|$ stays bounded for all $n \in \mathbb{N}$. Otherwise it is called *archimedean*.

A valuation is non-archimedean if and only if it satisfies the strong triangle inequality

$$|x + y| \leq \max\{|x|, |y|\}.$$

Given a nonarchimedean valuation $|\cdot|$, if we put $v(x) = -\log|x|$ for $x \neq 0$ and $v(0) = \infty$, we obtain a function

$$v : K \to \mathbb{R} \cup \{\infty\}$$

which we call an *exponential valuation* of K. We can recover a valuation from this exponential valuation by choosing any real number $q > 1$ and defining $|x| := q^{-v(x)}$.

Definition 1.5. The subset

$$o = \{x \in K : v(x) \geq 0\} = \{x \in K : |x| \leq 1\}$$

is an integral domain with field of fractions K which we call *valuation ring*. Its group of units is

$$o^* = \{x \in K : v(x) = 0\} = \{x \in K : |x| = 1\}$$

and its unique maximal ideal is

$$\mathfrak{p} = \{x \in K : v(x) > 0\} = \{x \in K : |x| < 1\}.$$

The field $o/\mathfrak{p}$ is called the *residue class field* of o.

An exponential valuation is called *discrete* if it admits a smallest positive value s, in which case $v(K^*) = s\mathbb{Z}$, and it is called *normalized* if $s = 1$. Dividing by s always yields a normalized valuation that does no affect o, o^* and $\mathfrak{p}$, which prompts the following definition:

Definition 1.6. A *uniformizer* of a valuation ring o is an element π such that $v(\pi) = 1$. Every element $x \in K^*$ admits a unique representation $x = u\pi^m$ with $m \in \mathbb{Z}$ and $u \in o^*$, because if $v(x) = m$, then $v(x\pi^{-m}) = 0$ which means that $u = x\pi^{-m} \in o^*$.

Proposition 1.1. *If v is a discrete exponential valuation of K, then o is a principal ideal domain, and we say it is a discrete valuation ring. If v is normalized, the nonzero ideals of o are given by*

$$\mathfrak{p}^n = \pi^n o = \{x \in K : v(x) \geq n\}, \quad n \geq 0$$

where π is a uniformizer. Moreover,

$$\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong o/\mathfrak{p}$$

In a field K with a discrete value, we get the following descending chains:

$$o \supseteq \mathfrak{p} \supseteq \mathfrak{p}^2 \supseteq \mathfrak{p}^3 \supseteq \dots$$

$$o^* = U^{(0)} \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \dots$$

where

$$U^{(n)} = 1 + \mathfrak{p}^n$$

are subgroups of o^*, with $U^{(1)}$ being called the group of *principal units* and $U^{(n)}$ the n-th *higher unit groups* for $n > 1$. For $n \geq 1$, these groups satisfy

$$o^*/U^{(n)} \cong (o/\mathfrak{p}^n)^* \quad \text{and} \quad U^{(n)}/U^{(n+1)} \cong o/\mathfrak{p}.$$

Valuations give raise to the completion of a field in the same way as the field of real numbers is constructed from the field of rational numbers.

Definition 1.7. A valued field $(K, |\cdot|)$ is called *complete* if every Cauchy sequence $\{a_n\}_{n\in\mathbb{N}}$ in K converges to an element $a \in K$.

The process of completion starts by taking the ring R of all Cauchy sequences of $(K, |\cdot|)$ and considering the maximal ideal $\mathfrak{m}$ of all nullsequences with respect to $|\cdot|$, i.e., all the

sequences that converge to zero. Define

$$\hat{K} = R/\mathfrak{m}.$$

K is embedded into $\hat{K}$ by sending every $a \in K$ to the class of the constant Cauchy sequence $(a, a, \dots)$. The valuation $|\cdot|$ is extended to $\hat{K}$ by giving the element $a \in \hat{K}$ (represented by the Cauchy sequence $\{a_n\}_{n\in\mathbb{N}}$) the absolute value

$$|a| := \lim_{n\to\infty} |a_n|.$$

As with the real numbers, the last step of the proof is to check that $\hat{K}$ is complete with respect to the extended valuation and that each $a \in \hat{K}$ is a limit of a sequence $\{a_n\}$ in K.

Proposition 1.2. *If $o \subset K$ is the valuation ring of v with maximal ideal $\mathfrak{p}$, and $\hat{o} \subset \hat{K}$ is the valuation ring of the extension of v with maximal ideal $\hat{\mathfrak{p}}$, then*

$$\hat{o}/\hat{\mathfrak{p}} \cong o/\mathfrak{p}.$$

With the general theory discussed, let us see a particular, very well known valuation.

Definition 1.8. Let p be a prime. The *p-adic exponential valuation* of an integer $n \neq 0$ is defined as

$$v_p(n) := \max\{k \in \mathbb{N}_0 \,:\, p^k | n\}$$

and $v_p(0) = \infty$. It can be extended to the rational numbers by defining

$$v_p\left(\frac{r}{s}\right) := v_p(r) - v_p(s).$$

Definition 1.9. The *p-adic absolute value* on $\mathbb{Q}$ is the function

$$|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$$

defined by

$$|x|_p := p^{-v_p(x)}.$$

This absolute value is a non-archimedean discrete valuation.

The *set of p-adic numbers* $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the metric defined by $d(x, y) := |x - y|_p$.

Remark 1.2. This p-adic completion can be generalized to prime ideals of Dedekind domains. Let K be an algebraic number field and $\mathcal{O}_K$ its ring of integers. Given an ideal $\mathfrak{a}$ of $\mathcal{O}_K$, it can be written as a product of powers of prime ideals of $\mathcal{O}_K$. Let $\mathfrak{p}$ be one of these prime ideals, and let n be the exponent of $\mathfrak{p}$ in the factorization. Then $v_\mathfrak{p}(\mathfrak{a}) := n$ defines an exponential valuation. The exponential valuation of an element x is defined as $v_\mathfrak{p}(x) := v_\mathfrak{p}((x))$ and we can choose a number $q > 1$ to define a valuation

$$|x|_\mathfrak{p} := q^{-v_\mathfrak{p}(x)}.$$

Completing K with respect to this valuation yields a complete field $K_{\mathfrak{p}}$. The number q is usually the cardinality of $\mathcal{O}_K/\mathfrak{p}$ when it is finite.

1.3 Local fields

The notion of completion with respect to a valuation yields the concept of local fields. A more in-depth study of local fields can be found in [17].

Definition 1.10. A *local field* is a field complete with respect to a discrete valuation such that the residue class field of its valuation ring is finite.

Local fields are exactly characterized as follows:

Proposition 1.3. *Every local field is isomorphic to one of the following:*

- $\mathbb{R}$ *or* $\mathbb{C}$*, if they are archimedean and have characteristic zero.*
- *Finite extensions of* $\mathbb{Q}_p$*, if they are non-archimedean and have characteristic zero.*
- *Finite extensions of* $\mathbb{F}_p((t))$*, if they are non-archimedean and have characteristic* $p > 0$*.*

The local fields with which we work in this project, $\mathbb{Q}_p$ and finite extensions of it, arise as completions of algebraic number fields with respect to generalizations of p-adic valuations. We do not discuss the other types of local fields.

Definition 1.11. The *ring of integers* of a local field K complete with respect to a discrete valuation $|\cdot|$ is

$$\mathcal{O} = \{x \in K : |x| \leq 1\},$$

that is, its discrete valuation ring.

The use of the term ring of integers makes sense in that integrality behaves well under completion (with A and B being integral domains, if B is integral over A then $\hat{B}$ is integral over $\hat{A}$) and that in an extension of local fields L/K, extending K's valuation to L yields that the discrete valuation ring corresponding to L is the integral closure of the discrete valuation ring corresponding to K. For example, the ring of integers of $\mathbb{Q}_p$, $\mathbb{Z}_p$, is the valuation ring corresponding to the extension of $|\cdot|_p$ to $\mathbb{Q}_p$. Its unique maximal ideal is the one generated by p and its residue class field is $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$.

In short, in a global extension $K/\mathbb{Q}$ we have that the ring of integers of K is the integral closure of $\mathbb{Z}$ in K. For the local extension $K_{\mathfrak{p}}/\mathbb{Q}_p$ the ring of integers of $K_{\mathfrak{p}}$ is the integral closure of $\mathbb{Z}_p$ in $K_{\mathfrak{p}}$.

Now suppose we have a Galois extension $K/\mathbb{Q}$, with $\mathcal{O}$ the ring of integers of K, and a prime $p \in \mathbb{Z}$ that factors as

$$p\mathcal{O} = \prod_{i=1}^{g} \mathfrak{p}_i^e.$$

We can complete $\mathbb{Q}$ with respect to p and K with respect to any $\mathfrak{p}_i$. This yields the extension $K_{\mathfrak{p}_i}/\mathbb{Q}_p$, which is still Galois, and the factorization is now

$$p\mathcal{O}_{\mathfrak{p}_i} = \mathfrak{p}_i^e,$$

where $\mathcal{O}_{\mathfrak{p}_i}$ is the ring of integers of $K_{\mathfrak{p}_i}$ and p is the only maximal ideal in $\mathbb{Z}_p$. This means that the ramification index e remains invariant under completion, and by Proposition 1.2 the residue class degree f is also invariant. Moreover, $[K_{\mathfrak{p}_i} : \mathbb{Q}_p] = ef$.

Since the maximal ideal of the ring of integers of a local field is unique, e and f are now intrinsic to the extension instead of being dependant on the prime. We define these formally in the next section.

To finish this section, we introduce how the logarithm and the exponential work in $\mathfrak{p}$-adic fields.

Proposition 1.4. *Take an extension $K/\mathbb{Q}$, a prime p in $\mathbb{Q}$ and a prime $\mathfrak{p}$ in K in the factorization of p. In the local field $K_\mathfrak{p}$, with ring of integers $\mathcal{O}_\mathfrak{p}$, there is a uniquely determined continuous homomorphism*

$$\log : K_\mathfrak{p}^* \to K_\mathfrak{p}$$

such that $\log p = 0$ which on the principal units $U^{(1)}$ of $\mathcal{O}_\mathfrak{p}^*$ is given by the series

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

Proposition 1.5. *In the same setting, with $p\mathcal{O}_\mathfrak{p} = \mathfrak{p}^e$, the power series*

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots$$

$$\exp(z) = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots$$

yield, for $n > e/(p-1)$, two mutually inverse isomorphisms

$$\mathfrak{p}^n \leftrightarrows U^{(n)}$$

where the arrow going right is exp *and the other one is* log.

1.4 Ramification in extensions of local fields

For this section, let L/K be a finite Galois extension of local fields, with v_L and v_K their normalized discrete exponential valuations, $\mathcal{O}_L$ and $\mathcal{O}_K$ their rings of integers, $\mathfrak{p}_L = (\pi_L)$ and $\mathfrak{p}_K = (\pi_K)$ their prime ideals generated by their corresponding uniformizers and $\lambda = \mathcal{O}_L/\mathfrak{p}_L$ and $\kappa = \mathcal{O}_K/\mathfrak{p}_K$ their residue class fields. Also let $p > 0$ be the characteristic of λ and κ.

First, notice that since $\mathfrak{p}_K \subseteq \mathfrak{p}_L$ and $\mathcal{O}_K \subseteq \mathcal{O}_L$, we get an injection $\kappa \hookrightarrow \lambda$, which means that we have an extension λ/κ. This extension is Galois because separability is kept modulo reduction by prime ideals and every element of $Gal(L/K)$ induces a well-defined automorphism on λ over κ, so normality is also kept. One can check that the projection $Gal(L/K) \to Gal(\lambda/\kappa)$ is surjective.

Definition 1.12. The *inertia index* of $L(K)$ is

$$f(L/K) = [\lambda : \kappa].$$

Definition 1.13. The *ramification index* of L/K is

$$e(L/K) = v_L(\pi_K).$$

This can be written as $\mathfrak{p}_K\mathcal{O}_L = \mathfrak{p}_L^{e(L/K)}$.

Remark 1.3. Since $\mathfrak{p}_K$ and $\mathfrak{p}_L$ are the unique prime ideals of $\mathcal{O}_K$ and $\mathcal{O}_L$, $v_K = v_{\mathfrak{p}_K}$ and $v_L = v_{\mathfrak{p}_L}$ as defined in Remark 1.2. For example, let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. We have that $\mathfrak{a} = \mathfrak{p}_K^n$, so $v_K(\mathfrak{a}) = n$. Since $\mathfrak{p}_K\mathcal{O}_L = \mathfrak{p}_L^{e(L/K)}$, $v_L(\mathfrak{a}) = e(L/K)v_K(\mathfrak{a})$. Conversely, we can define the valuation in $\mathcal{O}_K$ of ideals in $\mathcal{O}_L$: given an ideal $\mathfrak{b} \subseteq \mathcal{O}_L$, we define $v_K(\mathfrak{b}) := v_L(\mathfrak{b})/e(L/K)$.

Theorem 1.3.

$$[L : K] = e(L/K)f(L/K).$$

With this concepts, we can introduce the different types of extensions in terms of ramification.

Definition 1.14. The extension L/K is called *unramified* if

$$[L : K] = [\lambda : \kappa],$$

i.e., $e(L/K) = 1$.

Proposition 1.6. *Let L/K and K'/K be two extensions inside an algebraic closure $\overline{K}/K$ and let $L' = LK'$ be the composite of the fields L and K'. Then if L/K is unramified, L'/K' is unramified. Moreover, each subextension of an unramified extension is unramified.*

Corollary 1.1. *The composite of two unramified extensions of K is again unramified.*

Definition 1.15. The composite L_0/K of all unramified subextensions of L/K is called the *maximal unramified (sub)extension* of L/K.

Proposition 1.7. *The residue class field λ_0 of L_0 is equal to λ.*

Proof. We will see that λ_0 is the separable closure of κ in λ/κ, but since λ/κ is Galois, the separable closure is precisely λ. Let $\overline{\alpha} \in \lambda$ be separable over κ. Let $\overline{f}(x) \in \kappa[x]$ be the minimal polynomial of $\overline{\alpha}$ and $f(x) \in \mathcal{O}_K[x]$ a monic polynomial such that $\overline{f} \equiv f \mod \mathfrak{p}_K$. Then $f(x)$ is irreducible and has a root $\alpha \in L$ such that $\overline{\alpha} \equiv \alpha \mod \mathfrak{p}_L$, which means that $[K(\alpha) : K] = [\kappa(\overline{\alpha}) : \kappa]$. Hence, $K(\alpha)/K$ is unramified, so $K(\alpha) \subseteq L_0$ and $\overline{\alpha} \in \lambda_0$. ■

Corollary 1.2. $[L_0 : K] = f(L/K)$, *so* $[L : L_0] = e(L/K)$.

Proof. $[L_0 : K] = [\lambda_0 : \kappa]$ because L_0/K is unramified, and then by the previous proposition $[\lambda_0 : \kappa] = [\lambda : \kappa] = f(L/K)$. The consequence stems from Theorem 1.3. ■

Now we introduce the concepts of tame and wild ramification. Recall that p is the characteristic of λ and κ.

Definition 1.16. An extension L/K is called *tamely ramified* if $e(L/K) > 1$ and it is coprime with p.

As with unramified extensions, the composite of tamely ramified extensions is tamely ramified.

Definition 1.17. The composite L_1/K of all tamely ramified subextensions of L/K is called the *maximal tamely ramified (sub)extension* of L/K.

As with L_0, one can prove that the residue class field of L_1 is equal to λ.

In short, we have the chain $K \subseteq L_0 \subseteq L_1 \subseteq L$, where each intermediate extension is Galois as well. The extension L/K is called *totally ramified* if $L_0 = K$, i.e. $f = 1$, and is called *wildly ramified* if it is not tamely ramified, i.e. $L_1 \neq L$, i.e. p divides $e(L/K)$.

The well-known Eisenstein criterion for irreducibility of polynomials also has a consequence regarding totally ramified extensions.

Proposition 1.8. *Given an Eisenstein polynomial $E(X) \in K[X]$, if π is a root of $E(X)$ then $K(\pi)$ is totally ramified and $v_{K(\pi)}(\pi) = 1$ (that is, π is a uniformizer of $K(\pi)$). Conversely, if L is totally ramified over K and $v_{K(\pi)}(\pi) = 1$, then the minimal polynomial of π over K is Eisenstein, $\mathcal{O}_L = \mathcal{O}_K(\pi)$ and $L = K[\pi]$.*

A proof of this Proposition can be found in [4], Chapter I, §6.

Now we introduce higher ramification groups. In terms of the valuation v_L, recall that $\mathcal{O}_L = \{x \in L : v_L(x) \geq 0\}$.

Definition 1.18. Let $s \in \mathbb{Z}_{\geq -1}$. The *$s$-th ramification group of L/K* is

$$G_s(L/K) = \{\sigma \in Gal(L/K) : v_L(\sigma(x) - x) \geq s + 1 \text{ for all } x \in \mathcal{O}_L\}$$

We sometimes write just G_s for simplicity.

Observation 1.2. $G_{-1}(L/K) = Gal(L/K)$, because for any $\sigma \in Gal(L/K)$, $\sigma(x) - x \in \mathcal{O}_L$ for all $x \in \mathcal{O}_L$.

Observation 1.3. When s grows, the elements in G_s are closer to being the identity (recall that $v_L(0) = \infty$). Hence, the intersection of all G_s for $s \geq -1$ is the identity.

Consider $G_0(L/K) = \{\sigma \in Gal(L/K) : v_L(\sigma(x) - x) \geq 1 \text{ for all } x \in \mathcal{O}_L\}$. From Proposition 1.1, we have that $\mathfrak{p}_L = \{x \in L : v_L(x) \geq 1\}$, so in G_0 we get that $\sigma(x) \equiv x \mod \mathfrak{p}_L$. This means that σ is the identity when we reduce it to $Gal(\lambda/\kappa)$. This yields the following definition:

Definition 1.19. In an extension L/K as above its *inertia group* is

$$I(L/K) = G_0(L/K),$$

which is precisely the kernel of the natural homomorphism

$$Gal(L/K) \to Gal(\lambda/\kappa).$$

Observation 1.4. This definition is consistent with Definition 1.2 because in local fields, the decomposition group of $\mathfrak{p}_L$ is exactly $Gal(L/K)$.

Proposition 1.9. *If L_0/K is the maximal unramified extension of L/K,*

$$I(L/K) = Gal(L/L_0),$$

which means that the inertia group of L/K is trivial if and only if the extension L/K is unramified.

Proof. The maps $Gal(L/K) \to Gal(\lambda/\kappa)$ and $Gal(L_0/K) \to Gal(\lambda_0/\kappa)$ are surjective. By Proposition 1.7 we know that $\lambda_0 = \lambda$, and we know that $[L_0 : K] = [\lambda : \kappa]$, so the latter map is actually an isomorphism. Finally, there is a surjective map $Gal(L/K) \to Gal(L_0/K)$ because $Gal(L_0/K)$ is normal in $Gal(L/K)$. Hence we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \twoheadrightarrow & \mathrm{Gal}(\lambda/\kappa) \\ \downarrow & & \| \\ \mathrm{Gal}(L_0/K) & \xrightarrow{\sim} & \mathrm{Gal}(\lambda_0/\kappa) \end{array}$$

which means that the kernel of the map $Gal(L/K) \to Gal(\lambda/\kappa)$ is also the kernel of the map $Gal(L/K) \to Gal(L_0/K)$. Hence $I(L/K) = Gal(L/L_0)$. ■

Corollary 1.3. *$I(L/K)$ has order $e(L/K)$.*

Proof. $e(L/K)f(L/K) = [L : K] = [L : L_0][L_0 : K] = [L : L_0]f(L/K)$, hence $[L : L_0] = e(L/K)$. The previous proposition then yields the result. ■

Now we go back to the higher ramification groups. Recall the definition of unit groups that we gave after Proposition 1.1, and let $U^{(s)} = 1 + \mathfrak{p}_L^s = 1 + \pi_L^s \mathcal{O}_L$ be the s-th unit group of $\mathcal{O}_L$.

Proposition 1.10. *G_{s+1} is a normal subgroup of G_s and for $s \geq 0$ there is an injection*

$$G_s/G_{s+1} \hookrightarrow U^{(s)}/U^{(s+1)}.$$

A proof of this Proposition is available at [5], §6.

Proposition 1.11. *G_1 is the unique Sylow p-subgroup of G_0.*

Proof. Since we know that $U^{(s)}/U^{(s+1)} \cong \mathcal{O}_L/\mathfrak{p}_L = \lambda$ for $s \geq 1$, we get that there is an injection

$$G_s/G_{s+1} \hookrightarrow \lambda.$$

λ is a finite extension of $\mathbb{F}_p$, so $(\lambda, +)$ is a p-group and thus $|G_s/G_{s+1}|$ is a power of p. Hence, for any t, $|G_1/G_t|$ is also a power of p. But by Observation 1.3 the intersection of all G_s is the identity, and since $Gal(L/K)$ is finite we get that $G_t = 1$ for a sufficiently large t. Hence G_1 is a p-group. We also know that $U^{(0)}/U^{(1)} \cong (\mathcal{O}_L/\mathfrak{p}_L)^* = \lambda^*$, the order of which is coprime to p. So G_1 is the Sylow p-subgroup of G_0, and it is unique because it is normal. ■

Corollary 1.4. *$Gal(L/K)$ is solvable.*

Proof. By the previous propositions, the G_s form a subnormal series and, for $s \geq 0$, the quotients G_s/G_{s+1} embed into $(\lambda, +)$, which is abelian, so they are abelian. For $s = -1$, $G_{-1}/G_0 = Gal(L/K)/I(L/K)$ is isomorphic by definition to $Gal(\lambda/\kappa)$, which is an abelian group, particularly cyclic of order $[\lambda : \kappa]$. ■

G_1 splits the inertia group into two parts, one wild and one tame:

Definition 1.20. In an extension L/K as above, its *wild inertia group* is

$$I_w(L/K) = G_1(L/K),$$

and the *tame inertia group* is

$$I_t(L/K) = I/I_w.$$

Observation 1.5. Similarly to Proposition 1.9, one can check that $I_w = Gal(L/L_1)$, where L_1 is the maximal tamely ramified extension of L/K. Consequently, $I_t = Gal(L_1/L_0)$.

1.5 Norm, discriminant and different

Let L/K be a Galois extension, $[L : K] = n$, and let $\mathcal{O}_L$ and $\mathcal{O}_K$ be the corresponding rings of integers. The results of this first part of the section are taken from [14], Chapter I.

Definition 1.21. The *norm* of an element $\alpha \in \mathcal{O}_L$ is

$$N_{L/K}(\alpha) = \prod_{\sigma \in Gal(L/K)} \sigma(\alpha) \in \mathcal{O}_K$$

Definition 1.22. The *norm of an ideal* $\mathfrak{a} \subseteq \mathcal{O}_L$, $N_{L/K}(\mathfrak{a})$, is defined as the ideal in $\mathcal{O}_K$ generated by the norms of elements of $\mathfrak{a}$.

Remark 1.4. The norm of an ideal behaves well with prime factorization, in the sense that if $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$ then $N(\mathfrak{a}) = N(\mathfrak{p}_1)^{e_1} \dots N(\mathfrak{p}_r)^{e_r}$. In particular, the norm of a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ lying over a prime $\mathcal{P}$ of $\mathcal{O}_K$ is $N_{L/K}(\mathfrak{p}) = \mathcal{P}^f$, where $f = [\mathcal{O}_L/\mathfrak{p} : \mathcal{O}_K/\mathcal{P}]$ is the inertia degree.

The discriminant similarly applies to both elements and ideals:

Definition 1.23. The *discriminant* of a basis $\{\alpha_1, \dots, \alpha_n\}$ of elements of L is

$$d(\alpha_1, \dots \alpha_n) = \det((\sigma_i(\alpha_j)))^2$$

where $\sigma_i(\alpha_j)$ is the i-th conjugate of α_j.

Proposition 1.12. *If $\{\alpha_1, \dots, \alpha_n\}$ is a basis, the discriminant is not zero and it is an element of K. If $\alpha_1, \dots, \alpha_n \in \mathcal{O}_L$, then the discriminant is in $\mathcal{O}_K$.*

Definition 1.24. Given a non-zero ideal $\mathfrak{a} \subseteq \mathcal{O}_L$, we define its discriminant as the discriminant of any basis of I, and we write $d(\mathfrak{a})$. The discriminant of $\mathcal{O}_L$, that is, the discriminant of a basis of $\mathcal{O}_L$, is called the *discriminant of the number field L* and we write d_L.

Example 1.1. The discriminant of a quadratic extension $\mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$, with $D \neq 0, 1$ a square-free integer, is

$$d_{\mathbb{Q}\sqrt{D}} = \begin{cases} D & \text{if } D \equiv 1 \mod 4 \\ 4D & \text{if } D \equiv 2, 3 \mod 4 \end{cases}$$

Notice that the last definition does not depend at all on the extension, it's a definition intrinsic to the field L. The notion of discriminant of a field extension is the following:

Definition 1.25. Let $\alpha_1, \ldots, \alpha_n$ be a basis of L as a K-vector space contained entirely in $\mathcal{O}_L$, and consider its discriminant $d(\alpha_1, \ldots, \alpha_n)$. The ideal $\mathfrak{d}_{L/K} \subseteq \mathcal{O}_K$ generated by all such discriminants is called the *discriminant of the extension* L/K. If $\alpha_1, \ldots, \alpha_n$ is an integral basis of $\mathcal{O}_L/\mathcal{O}_K$, then $\mathfrak{d}_{L/K}$ is the principal ideal generated by $d(\alpha_1, \ldots, \alpha_n) = d_{L/K}$.

Observation 1.6. $d_{L/\mathbb{Q}} = d_L$.

Now we introduce two lower bounds for the discriminant in extensions $K/\mathbb{Q}$. The first one is a consequence of Minkowski's theorem and its upper bound for norms of ideals, and the second one was obtained by Odlyzko after further work with Minkowski's bound.

Theorem 1.4. *Let $K/\mathbb{Q}$ be an algebraic number field extension with $[K : \mathbb{Q}] = n$ and d_K the discriminant of K. Then*

$$|d_K| \geq \left(\frac{n^n}{n!}\right)^2 \left(\frac{\pi}{4}\right)^n.$$

A proof of this theorem can be found in [14], Chapter I, §5.

Theorem 1.5. *In the same setting as before, with $n = r + 2s$ where r are the number of real embeddings and $2s$ the number of complex embeddings, we have that*

$$|d_K|^{\frac{1}{n}} \geq (C_1 - o(1))^{r/n}(C_2 - o(1))^{2s/n} \quad \text{as} \quad n \to \infty$$

with

$$C_1 = \exp(\gamma + \log 4\pi + 1) = 60.8395\ldots$$
$$C_2 = \exp(\gamma + \log 4\pi) = 22.3816\ldots$$

where γ is the Euler constant.

Odlyzko computed explicit values of this bound for different values of n. The proof of the previous theorem can be found in [15], and we give some of these values in Table A.1 in the Appendix.

To finish this section, we introduce the different of an extension. The results here are taken from [14], Chapter III.

Definition 1.26. Let $\alpha \in \mathcal{O}_L$ and let $f(X) \in \mathcal{O}_K[X]$ be the minimal polynomial of α. The *different of α* is

$$\delta_{L/K}(\alpha) = \begin{cases} f'(\alpha) & \text{if } L = K(\alpha), \\ 0 & \text{if } L \neq K(\alpha). \end{cases}$$

Definition 1.27. The *different* $\mathfrak{D}_{L/K}$ of the extension L/K is the ideal of $\mathcal{O}_L$ generated by all differents of elements $\delta_{L/K}(\alpha)$ for $\alpha \in \mathcal{O}_L$. If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, then $\mathfrak{D}_{L/K} = (f'(\alpha))$, where $f(X) \in \mathcal{O}_K[X]$ is the minimal polynomial of α.

Proposition 1.13. *For a a tower of extensions $K \subset L \subset M$, $\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L} \cdot \mathfrak{D}_{L/K}$.*

The different characterises the ramification of the extension L/K:

Theorem 1.6. *A prime ideal $\mathfrak{p}$ of L is ramified over K if and only if $\mathfrak{p} | \mathfrak{D}_{L/K}$. Moreover, if $v_{\mathfrak{p}}(\mathfrak{D}_{L/K}) = n$ and $e > 1$ is the ramification index of $\mathfrak{p}$ over K, then $n = e - 1$ if e is coprime with p (tamely ramified), and $e \leq n \leq e - 1 + v_{\mathfrak{p}}((e))$ if p divides e (wildly ramified).*

Finally, there is the following relation between the discriminant and the different:

Theorem 1.7.

$$\mathfrak{d}_{L/K} = N_{L/K}(\mathfrak{D}_{L/K})$$

Corollary 1.5. *A prime ideal $\mathfrak{p}$ of L is ramified over K if and only if $\mathfrak{p}|\mathfrak{d}_{L/K}$. In particular, for an extension $K/\mathbb{Q}$ with $\mathfrak{d}_{K/\mathbb{Q}} = (d_K)$, a prime p of $\mathbb{Z}$ ramifies in K if and only if $p|d_K$.*

Corollary 1.6. *There are no unramified extensions of $\mathbb{Q}$.*

Proof. By either Minkowski or Odlyzko's bounds, for any extension $K/\mathbb{Q}$ one can check that $|d_K| > 1$ for $n > 2$. Since $d_K \in \mathbb{Z}$, there is a prime dividing d_K, which means that it ramifies in K. ■

1.6 Class field theory

In this section we introduce some notions of class field theory, without going into detail, taken from [10], Introduction and Chapters I and V, as well as [21].

We begin by defining some concepts on infinite Galois theory, because we work with the infinite extension $\overline{\mathbb{Q}}/\mathbb{Q}$. Let Ω/K be an extension, not necessarily of finite degree.

Proposition 1.14. *Ω is said to be Galois over K if it is separable and normal over K. Ω is Galois over K if and only if it is a union of finite Galois extensions of K.*

Definition 1.28. The *Galois group* $Gal(\Omega/K)$ of a Galois extension Ω/K is defined to be the group of automorphisms of Ω fixing K, endowed with the topology for which the sets $Gal(\Omega/L)$, with $K \subset L \subset \Omega$ and such that $[L : K]$ is finite, form a fundamental system of neighbourhoods of 1. $Gal(\Omega/K)$ is compact and Hausdorff.

The fundamental theorem of Galois theory is applied to infinite Galois extensions as follows:

Theorem 1.8. *Let Ω/K be a Galois extension with Galois group G. Then there is a one-to-one correspondence between the subfields of Ω and the closed subgroups of G. Moreover, the normal closed subgroups of G correspond to the Galois extensions of K, and the open subgroups of G correspond to the finite extensions of K.*

Infinite extensions often arise from sets of finite extensions.

Definition 1.29. A partially ordered set $(I, \preceq)$ is *directed* if, for any $\alpha, \beta \in I$, there exists a $\gamma \in I$ such that $\alpha, \beta \preceq \gamma$. For a directed set I, a *projective system* over I is a family $\{X_i, f_{ij} \,|\, i, j \in I, i \leq j\}$ of topological spaces X_i and continuous maps $f_{ij} : X_j \to X_i$ such that f_{ii} is the identity and $f_{ij} \circ f_{jk} = f_{ik}$ where $i \leq j \leq k$.

Remark 1.5. The *projective limit*

$$X = \varprojlim_{i \in I} X_i$$

of the projective system $\{X_i, f_{ij}\}$ is defined to be the subset

$$X = \{(x_i)_{i \in I} \in \prod_{i \in I} X_i \,|\, f_{ij}(x_j) = x_i \text{ for } i \leq j\}$$

of the product $\prod_{i \in I} X_i$.

Example 1.2. The ring of p-adic integers $\mathbb{Z}_p$ arises as a projective limit $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$, where the functions of the projective system are the canonical projections $\lambda_i : \mathbb{Z}/p^{i+1}\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$.

Definition 1.30. A topological group that is a projective limit of finite groups is called a *profinite group.*

Example 1.3. The Galois group $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is a profinite group, because it is the projective limit of the groups $Gal(L/K)$, where L runs over the subfields of $\overline{\mathbb{Q}}$ that are finite and Galois over K. This can be generalized to any Galois extension Ω/K with the groups being the finite Galois extensions of K.

Example 1.4. Consider the algebraic closure of $\mathbb{F}_p$, $\overline{\mathbb{F}}_p = \bigcup_{i=1}^{\infty} \mathbb{F}_{p^i}$. The linear group $GL_2(\overline{\mathbb{F}}_p)$ is a profinite group as well, as it is the projective limit of the groups $GL_2(\mathbb{F}_{p^i})$ where the maps are the restrictions $GL_2(\mathbb{F}_{p^{i+1}}) \to GL_2(\mathbb{F}_{p^i})$.

Now consider a non-archimedean local field K and fix an algebraic closure $\overline{K}$ of K. Every extension considered in this section is a subextension of $\overline{K}/K$. For simplicity, we sometimes skip writing the base field K for an extension. Recall that we say that an extension L/K is abelian if $Gal(L/K)$ is abelian.

If L/K and M/K are Galois extensions, then LM/K is Galois, and the map $Gal(LM/K) \hookrightarrow Gal(L/K) \times Gal(M/K)$ is an injection. Hence, if L/K and M/K are abelian, $Gal(LM/K)$ is a subgroup of an abelian group so LM/K is abelian as well.

Definition 1.31. By composition of every abelian extension, we can obtain a *maximal abelian extension* K^{ab}. Note that the extension K^{ab}/K is not necessarily finite.

Remark 1.6. The maximal unramified extension K^{ur}/K is abelian, because it is isomorphic to the extension κ^{ur}/κ of residue class fields, which has a cyclic Galois group generated by the Frobenius automorphism of order $|\kappa|$. Let $Frob_K$ be this automorphism.

Definition 1.32. The subgroups of K^* of the form $N_{L/K}(L^*)$ for some finite abelian extension L of K are called the *norm groups* in K.

Theorem 1.9 (Local reciprocity law)**.** *There exists a unique homomorphism*

$$\phi_K : K^* \to Gal(K^{ab}/K)$$

with the following properties:

- *For every uniformizer π of K and every finite unramified extension L of K, $\phi_K(\pi)|_L = Frob_K$.*
- *For every finite abelian extension L of K, $N_{L/K}(L^*)$ is contained in the kernel of $a \to \phi_K(a)|_L$ and ϕ_K induces an isomorphism*

$$\phi_{L/K} : K^*/N_{L/K}(L^*) \to Gal(L/K).$$

The theorem implies that we have the following commutative diagram:

$$\begin{array}{ccc} K^* & \xrightarrow{\phi_K} & \mathrm{Gal}(K^{ab}/K) \\ \downarrow & & \downarrow{\scriptstyle \sigma \to \sigma|_L} \\ K^*/N(L^*) & \xrightarrow{\phi_{L/K}} & \mathrm{Gal}(L/K) \end{array}$$

We say that ϕ_K and $\phi_{L/K}$ are the *local Artin maps* for K and L/K.

Observation 1.7. The local reciprocity law, the fact that $K^* = \pi^{\mathbb{Z}} \cdot \mathcal{O}_K^*$ (see Definition 1.6) and Remark 1.6 imply that for an arbitrary extension L/K, the local Artin map sends the uniformizer part of K^* to the unramified part of $Gal(L/K)$ (the part generated by $Frob_K$) and $\mathcal{O}_K^*$ to the inertia group. Hence, if the extension L/K is totally ramified, we can restrict the maps to $\mathcal{O}_K^*$.

To finish local class field theory, we state Kronecker-Weber's theorem:

Theorem 1.10 (Local Kronecker-Weber)**.** *Every finite abelian extension of $\mathbb{Q}_p$ is contained in a field $\mathbb{Q}_p(\zeta)$, where ζ is a root of unity.*

This theorem has its global equivalent:

Theorem 1.11 (Global Kronecker-Weber)**.** *Every finite abelian extension of $\mathbb{Q}$ is contained in a field $\mathbb{Q}(\zeta)$, where ζ is a root of unity.*

Now let K be a number field and let I_K be the group of fractional ideals in the ring of integers $\mathcal{O}_K$. Let $i : K^* \to I_K$ be the map which sends an element $a \in K^*$ to the ideal $a\mathcal{O}_K$. Its image is the set of principal ideals.

Definition 1.33. The quotient $Cl_K = I_K/i(K^*)$ is the *class group of K*. A subgroup H of Cl_K is equivalent to a subgroup $\tilde{H}$ of I_K containing $i(K^*)$.

Before moving on, we need to introduce the notion of *infinite primes* of K. The *finite primes* are the primes that we already know, identified with the prime ideals of $\mathcal{O}_K$. The *real* infinite primes are identified with embeddings of K into $\mathbb{R}$, while *complex* infinite primes are identified with a conjugate pair of embeddings of K into $\mathbb{C}$.

Definition 1.34. For an extension L/K, we say that a real prime of K *splits in L* if every prime lying over it is real, otherwise we say it *ramifies in L*.

Definition 1.35. We say that a finite extension L/K is *unramified* if each prime ideal in $\mathcal{O}_K$ is unramified in L and each real prime of K remains real, i.e., every real embedding of K extends to a real embedding of L.

Definition 1.36. Let H be a subgroup of Cl_K. A finite unramified abelian extension L of K is said to be a *class field for H* if the prime ideals of $\mathcal{O}_K$ splitting in L are exactly those in $\tilde{H}$.

Theorem 1.12. *A class field exists for each subgroup of Cl_K, it is unique, and every finite unramified abelian extension of K arises as the class field of some subgroup of Cl_K. If L is the class field of H, then $Gal(L/K) \cong C/H$.*

The subgroup H of Cl_K corresponding to a finite unramified abelian extension L of K is that generated by the primes that split in L. In particular, the class field of the trivial subgroup of Cl_K is called the *Hilbert class field* of K, and it is the largest abelian extension L of K unramified at all primes of K.

This notion can be generalized to ramified extensions by generalizing ideal class groups.

Definition 1.37. A *modulus* $\mathfrak{m}$ of a number field K is the product $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ of an ideal $\mathfrak{m}_0$ of $\mathcal{O}_K$ with the product $\mathfrak{m}_\infty$ of certain real primes of K.

Let $S(\mathfrak{m})$ be the set of primes dividing $\mathfrak{m}$ and define $I^{S(\mathfrak{m})}$ to be the group of fractional ideals generated by the prime ideals of $\mathcal{O}_K$ not in $S(\mathfrak{m})$.

Definition 1.38. The *ray class group* $Cl_K^{\mathfrak{m}}$ is defined to be the quotient of $I^{S(\mathfrak{m})}$ by the subgroup generated by elements $a \in K^*$ such that $a > 0$ at all real primes dividing $\mathfrak{m}_\infty$ and $v_{\mathcal{P}}(a-1) \geq v_{\mathcal{P}}(\mathfrak{m}_0)$ for all prime ideals $\mathcal{P}$ dividing $\mathfrak{m}_0$.

The subgroup described in the previous definition is analogous to the set of principal ideals. For example, if $\mathfrak{m} = 1$, then $Cl_K^{\mathfrak{m}} = Cl_K$. If $K = \mathbb{Q}$ and $\mathfrak{m} = (m)\infty$ for some integer m, then $Cl_K^{\mathfrak{m}} \cong (\mathbb{Z}/m\mathbb{Z})^*$.

Definition 1.39. Let H be a subgroup of $Cl_K^{\mathfrak{m}}$ for some modulus $\mathfrak{m}$, and let $\tilde{H}$ be its inverse image in $I^{S(\mathfrak{m})}$. An abelian extension L of K, unramified at the primes dividing $\mathfrak{m}$, is said to be a *class field for* H if the prime ideals of $\mathcal{O}_K$ not dividing $\mathfrak{m}_0$ that split in L are exactly those in $\tilde{H}$.

Theorem 1.13. *A class field exists for each subgroup of a ray class group $Cl_K^{\mathfrak{m}}$, it is unique, and every finite abelian extension of K arises as the ray class field of some subgroup of a ray class group. If L is the class field of $H \subset Cl_K^{\mathfrak{m}}$, then $Gal(L/K) \cong Cl_K^{\mathfrak{m}}/H$ and the prime ideals $\mathcal{P}$ of K not dividing $\mathfrak{m}$ are unramified in L with residue class degree equal to the order of the image of $\mathcal{P}$ in the group $Cl_K^{\mathfrak{m}}/H$.*

The class field of the trivial subgroup of $Cl_K^{\mathfrak{m}}$ is called the *ray class field modulo* $\mathfrak{m}$ of K, and it is the largest abelian extension L of K unramified at all primes not dividing $\mathfrak{m}$. Thus, this theorem implies that we can determine the abelian Galois extensions L/K ramified only at primes in S for any finite set S of primes of K.

1.7 Galois representations and characters

In this section, we introduce Galois representations, characters and how they are related to the concepts we have already studied. The first part of the section is taken from [7], §6.

Definition 1.40. A *Galois representation* of $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ is a continuous morphism

$$\rho : G_{\mathbb{Q}} \to Aut_K(V),$$

where V is a finite dimensional vector space over a field K. We often write $Aut_K(V)$ as $GL(V)$ or $GL_n(K)$, where n is the dimension of V, and we say that this n is the *dimension of* ρ.

Remark 1.7. Since $G_{\mathbb{Q}}$ is a profinite group (see Example 1.3), any continuous representation of $G_{\mathbb{Q}}$ acts through a finite quotient, which is the invariant field of the kernel of ρ. This means that we can restrict representations of $G_{\mathbb{Q}}$ to Galois groups of finite Galois extensions to study them.

Definition 1.41. A subspace $W \subset V$ is *ρ-invariant* if $\rho(\sigma)(w) \in W$ for all $\sigma \in G$ and all $w \in W$. We say that a representation ρ is *irreducible* if there is no proper $W \subset V$ that is ρ-invariant; otherwise we say that ρ is *reducible*.

Definition 1.42. Let ρ be a Galois representation. Given a prime p, we say that ρ is *unramified at* p if $\rho(I_{\mathfrak{p}}) = 1$ for any prime $\mathfrak{p} \subset \overline{\mathbb{Z}}$ which contains p. Conversely, we say that ρ is *ramified at* p if the image of the inertia group is not trivial.

Now we introduce the concept of character:

Definition 1.43. The *character* $\chi : G \to K$ *of a representation* $\rho : G \to GL(V)$ of a group G is the trace of the representation:

$$\chi(g) = Tr(\rho(g)) \text{ for } g \in G.$$

A character is said to be *irreducible* if ρ is irreducible. If the representation is one-dimensional, the character is identical to the representation.

Remark 1.8. The term "character" is also used for group homomorphisms from a group G to the multiplicative group of a field, which we call *characters of* G. When a representation is one-dimensional, its character is also a character in the other sense, so we can understand characters of groups as a particular case of characters of representations. The *trivial character of* G is the character that sends all elements of G to one.

Remark 1.9. Every one-dimensional character is irreducible, because every one-dimensional representation is irreducible. In general, not every irreducible character is one-dimensional, but this is true if G is abelian. In this case, if G is a finite abelian group of order n, it has exactly n irreducible characters.

The rest of the section is taken from [4], Chapter 6. Let L/K be a finite abelian Galois extension with $G = Gal(L/K)$. Let $\phi_{L/K}$ be the local Artin map of L/K and $U^{(n)}$ the unit groups of K. Let $\chi : G \to \mathbb{C}^*$ be an irreducible character of G.

Definition 1.44. The *Artin conductor* of χ is the positive (or zero) integer

$$f(\chi) = \min\{k \,|\, U^{(k)} \subset \ker(\chi \circ \phi_{L/K})\}.$$

This definition can be extended to be an ideal as follows. Let $\mathcal{P}$ be a prime ideal in K and choose a prime ideal $\mathfrak{p}$ in L which divides $\mathcal{P}$. Let $D_{\mathfrak{p}}$ be the decomposition group of $\mathfrak{p}$ and let $f(\chi, \mathcal{P})$ be the Artin conductor of the restriction of χ to $D_{\mathfrak{p}}$. Clearly $f(\chi, \mathcal{P}) = 0$ when $\mathcal{P}$ is unramified.

Definition 1.45. The *global conductor* of χ is the ideal

$$\mathfrak{f}(\chi) = \prod_{\mathcal{P}} \mathcal{P}^{f(\chi,\mathcal{P})}$$

where the product runs through the prime ideals in K.

Hence, the global conductor of a character encodes information about ramification. This relation is explicit in the following formula, known as the "Führerdiskriminantenprodukt-formel":

Proposition 1.15 (Conductor-discriminant formula)**.** *Let* $\hat{G}$ *be the set of all irreducible characters of* G*. Then*

$$\mathfrak{d}_{L/K} = \prod_{\chi \in \hat{G}} \mathfrak{f}(\chi)^{\chi(1)}$$

where $\mathfrak{d}_{L/K}$ is the discriminant of the extension L/K from Definition 1.25. Since the extension is abelian, $\chi(1) = 1$ for all χ by Remark 1.9.

Remark 1.10. The original definition of Artin conductor involves the higher ramification groups G_i (see Definition 1.18), as follows: given a character χ, its Artin conductor is the number

$$f(\chi) = \sum_{i=0}^{\infty} \frac{|G_i|}{|G_0|}(\chi(1) - \chi(G_i))$$

where $\chi(G_i) = \frac{1}{|G_i|}\sum_{g \in G_i} \chi(g)$. The two definitions are equivalent.

Chapter 2
Tate's upper bound

In this chapter we establish the setting of the problem and we prove Tate's upper bound.

Let

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_p)$$

be a continuous Galois representation, where $GL_2(\overline{\mathbb{F}}_p)$ is as described in Example 1.4 and p is a prime. Continuity here implies, as stated in Remark 1.7, that ρ factorizes through a Galois group $Gal(K/\mathbb{Q})$ such that the extension $K/\mathbb{Q}$ is a finite Galois extension. Let $\mathfrak{p}$ be a prime in K in the factorization of p, and complete K with respect to $\mathfrak{p}$, obtaining $K_\mathfrak{p}$. Let $D_\mathfrak{p} = Gal(K_\mathfrak{p}/\mathbb{Q}_p)$ be the decomposition group of $\mathfrak{p}$. We get the faithful representation

$$\rho : Gal(K_\mathfrak{p}/\mathbb{Q}_p) \to GL_2(\overline{\mathbb{F}}_p).$$

Now let K_0 be the maximal unramified extension of $\mathbb{Q}_p$ inside of $K_\mathfrak{p}$ and K_1 the maximal tamely ramified extension of $\mathbb{Q}_p$ inside of $K_\mathfrak{p}$. The tower of extensions is

$$\mathbb{Q}_p \subseteq K_0 \subseteq K_1 \subseteq K_\mathfrak{p}.$$

Define the groups

$$I = Gal(K_\mathfrak{p}/K_0), \text{ the inertia group;}$$

$$I_w = Gal(K_\mathfrak{p}/K_1), \text{ the wild inertia group.}$$

For the purpose of this project, we assume that I_w is not trivial, that is, $K_1 \subsetneq K_\mathfrak{p}$, and $[K_\mathfrak{p} : K_1] = p^m$. Recall by Proposition 1.11 that I_w is a p-group, and in fact in our setting it is an elementary abelian p-group, that is, an abelian p-group where every element of has order p. To prove this, we need the following Proposition:

Proposition 2.1. *The subgroup T of $GL_2(\mathbb{F}_q)$ of upper triangular matrices with 1's in the diagonal is a Sylow p-subgroup of $GL_2(\mathbb{F}_q)$.*

Proof. We know that $|GL_2(\mathbb{F}_q)| = (q^2-q)(q^2-1) = q(q-1)(q^2-1)$. Since p does not divide $(q-1)(q^2-1)$, we get that $GL_2(\mathbb{F}_q)$ has a Sylow p-subgroup of order q. T has order precisely q, because there are q possible elements to choose for the element above the diagonal, so it is a Sylow p-subgroup. ■

T being a Sylow p-subgroup means that $\rho(I_w) \subseteq T$ for some q, and T is elementary abelian because it is isomorphic to $\mathbb{F}_q$, so I_w is elementary abelian as well.

The next step is studying the construction of the extensions K_0 and K_1:

Lemma 2.1. *The field $\mathbb{Q}_p(\zeta_p)$ contains an element π such that $\pi^{p-1} = -p$.*

Proof. First we prove that $\mathbb{Q}_p(\zeta_p)/\mathbb{Q}$ is totally ramified of degree $\varphi(p) = p-1$. ζ_p satisfies

$$\zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + 1 = 0,$$

and hence if we consider the polynomial

$$P(X) = X^{p-1} + X^{p-2} + \cdots + 1 = 0,$$

we see that $\pi = \zeta_p - 1$ is a root of $P(X+1)$. $P(X+1)$ satisfies Eisenstein's criterion for p, so by Proposition 1.8 this proves what we wanted and also that $\zeta_p - 1$ is a uniformizer of $\mathbb{Q}_p(\zeta_p)$. In particular, the prime ideal $\mathfrak{p}$ of $\mathbb{Q}_p(\zeta_p)$ is generated by $\zeta_p - 1$, so $((\zeta_p - 1))^{p-1} = (p)$, i.e. $(\zeta_p - 1)^{p-1} = up$ with u a unit of $\mathbb{Z}_p[\zeta_p]$, which is the ring of integers of $\mathbb{Q}_p(\zeta_p)$.

On the other hand, consider the polynomial

$$E(X) = X^{p-1} + p$$

over $\mathbb{Q}_p$. $E(X)$ is also an Eisenstein polynomial for p, so a root π of this polynomial generates a totally ramified extension $\mathbb{Q}_p(\pi)$ of degree $p-1$ with π as a uniformizer. $(\pi)^{p-1} = (p)$ and by construction of π, it satisfies $\pi^{p-1} = -p$.

Then we can write

$$\pi = (\zeta_p - 1)/u^{1/p-1}$$

and this proves that $\pi \in \mathbb{Q}_p(\zeta_p)$. Since the extensions have the same degree, this also proves that $\mathbb{Q}_p(\zeta_p) = \mathbb{Q}_p(\pi)$. In particular, the ideals $(\zeta_p - 1)$ and (π) are the same, which means that $(\zeta_p - 1)$ can be generated by a power of π. ■

Lemma 2.2. *There exists a divisor d of $p-1$ such that $K_1 = K_0(\pi^d)$ where π is as in the previous Lemma. Moreover, the ramification index of K_1/K_0 is $e = (p-1)/d$, which is also the degree $[K_1 : K_0]$ since K_1/K_0 is totally ramified.*

Proof. By Corollary 1.4, I/I_w and $D_\mathfrak{p}/I$ are abelian, so $D_\mathfrak{p}/I_w = Gal(K_\mathfrak{p}/\mathbb{Q}_p)/Gal(K_\mathfrak{p}/K_1) \cong Gal(K_1/\mathbb{Q}_p)$ is also abelian. Hence, the extension $K_1/\mathbb{Q}_p$ is abelian, and by Theorem 1.10 any abelian extension of $\mathbb{Q}_p$ can be generated by roots of unity. Since $K_0 \subset K_1$, this means that $K_0/\mathbb{Q}_p$ can be generated by roots of unity whose order is prime to p (otherwise the extension would ramify, as we saw in the previous lemma). Then $K_1 \subseteq K_0(\zeta_p)$, and by the previous lemma we can find a $d|p-1$ such that $K_1 = K_0(\pi^d)$. Since π has order $p-1$, we get that $[K_1 : K_0] = (p-1)/d$. ■

Observation 2.1. e is also the ramification index of $K_1/\mathbb{Q}_p$, because $K_0/\mathbb{Q}_p$ is unramified.

Let $\mathcal{O}_1$ and $\mathcal{O}_{K_\mathfrak{p}}$ be the rings of integers of K_1 and $K_\mathfrak{p}$ respectively, with π^d a generator of the maximal ideal in $\mathcal{O}_1$. Recall that $\pi^{p-1} = -p$.

Let $U = \mathcal{O}_1^*$. The higher unit groups are of the form $U^{(i)} = 1 + \pi^{di}\mathcal{O}_1$. We denote the p-th powers of elements of $U^{(i)}$ by $(U^{(i)})^p$.

Lemma 2.3. *We have*

$$U^{(e+2)} \subset (U^{(1)})^p \subset U^{(e+1)}.$$

If $d > 1$ then $(U^{(1)})^p = U^{(e+1)}$. If $d = 1$ then $(U^{(1)})^p$ has index p in $U^{(e+1)}$.

Proof. First we check that $(U^{(1)})^p \subset U^{(e+1)}$. An element $x \in (U^{(1)})^p$ has the form $x =$

$(1+\pi^d\alpha)^p$ with $\alpha \in \mathcal{O}_1$. If we expand this, we get

$$\begin{aligned} x &= \sum_{k=0}^{p} \binom{p}{k} (\pi^d\alpha)^k = \\ &= 1 + \pi^{dp}\alpha^p + \sum_{k=1}^{p-1} \binom{p}{k} (\pi^d\alpha)^k = \\ &= 1 + \pi^{d(p-1)}\pi^d\alpha^p + p\pi^d P(\pi^d, \alpha) = \\ &= 1 + \pi^{(d-1)(p-1)}\pi^{p-1}\pi^d\alpha^p + p\pi^d P(\pi^d, \alpha) = \\ &= 1 + (-p)^{d-1}\pi^{p-1}\pi^d\alpha^p - \pi^{p-1}\pi^d P(\pi^d, \alpha) = \\ &= 1 + \pi^{p-1+d}\tilde{P}(\pi^d, \alpha) = \\ &= 1 + \pi^{d(e+1)}\tilde{P}(\pi^d, \alpha) \end{aligned}$$

where P and $\tilde{P}$ are polynomials with coefficients in $\mathbb{Z}$, so that $P(\pi^d, \alpha)$ and $\tilde{P}(\pi^d, \alpha)$ are elements in $\mathcal{O}_1$. Hence $x \in (U^{(1)})^p$ is also in $U^{(e+1)}$.

To check that $U^{(e+2)} \subset (U^{(1)})^p$, we see that $U^{(e+2)} = (U^{(2)})^p$. By Proposition 1.5, given that $2 > e/(p-1) = 1/d$, the exponential and logarithm functions define mutually inverse isomorphisms

$$(\pi^d)^n \leftrightarrows U^{(n)}$$

for $n \geq 2$. Then with

$$\begin{aligned} (U^{(2)})^p &= \exp(p \cdot \log(U^{(2)})) = \\ &= \exp(p \cdot (\pi^{2d})) = \\ &= \exp((\pi^{p-1+2d})) = \\ &= \exp((\pi^d)^{(p-1)/d+2}) = \\ &= \exp((\pi^d)^{e+2}) = \\ &= U^{(e+2)} \end{aligned}$$

we obtain the equality.

With what we have seen, we can consider the p-th power surjection

$$\alpha : U^{(1)}/U^{(2)} \to (U^{(1)})^p/(U^{(2)})^p$$

and the inclusion

$$(U^{(1)})^p/(U^{(2)})^p \subseteq U^{(e+1)}/U^{(e+2)}.$$

The kernel of α is precisely the p-th roots of unity in K_1.

If $d > 1$, there are no p-th roots of unity in K_1, so α is a bijection. Hence, knowing that all quotients $U^{(i)}/U^{(i+1)}$ have the same cardinality and that $U^{(e+2)} = (U^{(2)})^p$, we get $(U^{(1)})^p = U^{(e+1)}$. This case can also be proved with the exponential-logarithm argument.

If $d = 1$, $K_1 = K_0(\zeta_p)$, and the map α has kernel of order p. By the same argument as

before, $U^{(e+1)}$ now has the same cardinality as $(U^{(1)})^p$ quotiented by a group of order p, so $(U^{(1)})^p$ has index p in $U^{(e+1)}$. ■

Now we take the local Artin map (see Theorem 1.9) of the extension $K_\mathfrak{p}/K_1$, and we get a surjective map

$$\phi : K_1^* \to Gal(K_\mathfrak{p}/K_1) = I_w,$$

with kernel $N(K_\mathfrak{p}^*)$. Since $K_\mathfrak{p}/K_1$ is a totally ramified extension, by Observation 1.7 we can restrict this map to the units, obtaining

$$\phi : U \to I_w$$

with kernel $N(K_\mathfrak{p}^*) \cap U = N(\mathcal{O}_{K_\mathfrak{p}}^*)$. We know that $U/U^{(1)} \cong (\mathcal{O}_1/\mathfrak{p})^*$, which has order coprime to p. Since I_w is a p-group, every element of U with order coprime to p must be mapped to the trivial element. Hence, we can further restrict the mapping to

$$\phi : U^{(1)} \to I_w.$$

On the other hand, consider a one-dimensional character $\chi_w : I_w \to \mathbb{C}^*$, and take its Artin conductor

$$f(\chi_w) = \min\{k \,|\, U^{(k)} \subset \ker(\chi_w \circ \phi)\},$$

with $f(\chi_w) = 0$ if χ_w is the trivial character. Notice that $f(\chi_w, (\pi^d)) = f(\chi_w)$, because I_w is already the decomposition group of (π^d). Moreover, (π^d) is the only prime ideal in K_1. Hence, the global conductor of χ_w is

$$\mathfrak{f}(\chi_w) = \pi^{df(\chi_w)}.$$

Here we are abusing notation for the sake of simplicity, because π^d is not the element but the ideal; we do this from now on where there is no risk of confusion.

With this, we can apply the conductor-discriminant formula (Proposition 1.15) to the extension $K_\mathfrak{p}/K_1$. We know that I_w is abelian, so by Remark 1.9, all the elements of $\hat{I_w}$ are one-dimensional characters like χ_w. Hence we get

$$\mathfrak{d}_{K_\mathfrak{p}/K_1} = \prod_{\chi \in \hat{I_w}} \mathfrak{f}(\chi) = \prod_{\chi \in \hat{I_w}} \pi^{df(\chi)}.$$

Using Remark 1.3, we can take the valuation in $\mathbb{Q}_p$, which is the exponential p-adic valuation v_p (normalized with $v_p(p) = 1$), on both sides to get

$$v_p(\mathfrak{d}_{K_\mathfrak{p}/K_1}) = \left(\sum_{\chi \in \hat{I_w}} f(\chi) \right) v_p(\pi^d).$$

Finally, by the discriminant-different relation (Theorem 1.7), we have

$$v_p(\mathfrak{d}_{K_\mathfrak{p}/K_1}) = v_p(N_{K_\mathfrak{p}/K_1}(\mathfrak{D}_{K_\mathfrak{p}/K_1})) = [K_\mathfrak{p} : K_1] v_p(\mathfrak{D}_{K_\mathfrak{p}/K_1})$$

where this last equality comes from the fact that the norm of each element of $\mathfrak{D}_{K_\mathfrak{p}/K_1}$ is the multiplication of all its I_w-conjugates, but the elements of the different are derivatives of

minimal polynomials, so they are invariant by the conjugates. Hence the norm is just the element to the power of $|I_w| = [K_\mathfrak{p} : K_1]$. In the end, we get

$$[K_\mathfrak{p} : K_1] v_p(\mathfrak{D}_{K_\mathfrak{p}/K_1}) = \left(\sum_{\chi \in \hat{I_w}} f(\chi) \right) v_p(\pi^d). \tag{2.1}$$

With this, we are finally ready to prove Tate's upper bound. Recall that $[K_\mathfrak{p} : K_1] = p^m$.

Theorem 2.1 (Tate's upper bound)**.**

$$v_p(\mathfrak{D}_{K_\mathfrak{p}/\mathbb{Q}_p}) \leq 2 + \frac{1}{p(p-1)} - \frac{2}{p^m(p-1)}. \tag{2.2}$$

Proof. First we see that $(U^{(1)})^p \subset \ker(\phi)$. Consider $u \in U^{(1)}$ and its image $\phi(u) = \sigma$. Then, since ϕ is an homomorphism, $u^p \in (U^{(1)})^p$ satisfies $\phi(u^p) = \phi(u)^p = \sigma^p$. Given that every element in I_w has order p, σ^p is trivial, which proves our statement.

We start with the case $d > 1$. In this case, $(U^{(1)})^p = U^{(e+1)}$, and since $(U^{(1)})^p \subset \ker(\phi)$ this means that $f(\chi) \leq e + 1$ for all non-trivial characters $\chi \in \hat{I_w}$, which are exactly $[K_\mathfrak{p} : K_1] - 1 = p^m - 1$ by Remark 1.9. From (2.1) we get

$$v_p(\mathfrak{D}_{K_\mathfrak{p}/K_1}) \leq \frac{1}{p^m}(p^m - 1)(e+1) v_p(\pi^d).$$

By Proposition 1.13 we have $\mathfrak{D}_{K_\mathfrak{p}/\mathbb{Q}_p} = \mathfrak{D}_{K_\mathfrak{p}/K_1}\mathfrak{D}_{K_1/\mathbb{Q}_p}$, so taking v_p at both sides we have $v_p(\mathfrak{D}_{K_\mathfrak{p}/\mathbb{Q}_p}) = v_p(\mathfrak{D}_{K_\mathfrak{p}/K_1}) + v_p(\mathfrak{D}_{K_1/\mathbb{Q}_p})$. By Theorem 1.6 and Remark 1.3,

$$v_p(\mathfrak{D}_{K_1/\mathbb{Q}_p}) = \frac{e(K_1/\mathbb{Q}_p) - 1}{e(K_1/\mathbb{Q}_p)} = \frac{e-1}{e} = 1 - \frac{1}{e}.$$

With this,

$$v_p(\mathfrak{D}_{K_\mathfrak{p}/\mathbb{Q}_p}) \leq \frac{1}{p^m}(p^m - 1)(e+1) v_p(\pi^d) + 1 - \frac{1}{e}.$$

(π^d) is the only prime ideal in K_1, thus the valuation in K_1 is v_{π^d} so $v_{\pi^d}(\pi^d) = 1$. Using Remark 1.3, we know that

$$v_p(\pi^d) = \frac{v_{\pi^d}(\pi^d)}{e(K_1/\mathbb{Q}_p)} = \frac{1}{e}.$$

Hence

$$\begin{aligned} v_p(\mathfrak{D}_{K_\mathfrak{p}/\mathbb{Q}_p}) &\leq \frac{1}{p^m e}(p^m - 1)(e+1) + 1 - \frac{1}{e} \\ &= \frac{(p^m - 1)(e+1) + p^m e - p^m}{p^m e} \\ &= \frac{2p^m e - e - 1}{p^m e} \\ &= 2 - \frac{e+1}{p^m e}. \end{aligned}$$

This expression satisfies (2.2) because

$$\frac{e+1}{p^m e} = \frac{(p-1)/d+1}{p^m(p-1)/d} = \frac{p-1+d}{p^m(p-1)} > \frac{2}{p^m(p-1)}.$$

Now we move to the case $d = 1$. In this case, $e = p-1$ (so $U^{(e+1)} = U^{(p)}$ and $U^{(e+2)} = U^{(p+1)}$) and $(U^{(1)})^p$ has index p in $U^{(p)}$. We know that $(U^{(1)})^p \subset \ker(\phi)$, and also $U^{(p+1)} \subset (U^{(1)})^p$, so $f(\chi) \leq p+1$ for every character χ. From the fact that $(U^{(1)})^p \subset \ker(\phi)$, we have that

$$U^{(1)}/(U^{(1)})^p \supset U^{(1)}/\ker(\phi) \cong I_w,$$

which means that we can identify $\hat{I_w}$ as a subgroup of the homomorphism group

$$Hom(U^{(1)}/(U^{(1)})^p, \mathbb{C}^*).$$

Consequently, the characters with $f(\chi) \leq i$ can be identified with a subgroup of

$$Hom(U^{(1)}/(U^{(i)}(U^{(1)})^p), \mathbb{C}^*).$$

Since $(U^{(1)})^p$ has index p in $U^{(p)}$,

$$Hom(U^{(1)}/(U^{(p)}(U^{(1)})^p), \mathbb{C}^*) \text{ has index } p \text{ in } Hom(U^{(1)}/(U^{(1)})^p, \mathbb{C}^*),$$

which means that at least a p-th part of the characters in $\hat{I_w}$ have Artin conductor $\leq p$, obviously including the trivial character, which has Artin conductor 0. By a result of Moon and Taguchi in [12] (already remarked by Serre in [19]), every non-trivial character has $f(\chi)$ either 2 or $p-1$, so $p^{m-1}-1$ characters have conductor 2 and the rest have conductor $\leq p+1$. Hence

$$v_p(\mathfrak{D}_{K_\mathfrak{p}/K_1}) \leq \frac{1}{p^m}\left[(p^m - p^{m-1})(p+1)v_p(\pi) + (p^{m-1}-1)(2)v_p(\pi)\right].$$

We have $v_p(\pi) = 1/(p-1)$ now, and $v_p(\mathfrak{D}_{K_1}/\mathbb{Q}_p) = 1 - 1/(p-1)$. Thus

$$\begin{aligned} v_p(\mathfrak{D}_{K_\mathfrak{p}/\mathbb{Q}_p}) &\leq 1 + \frac{1}{p^m(p-1)}\left[p^{m+1} - p^{m-1} + 2p^{m-1} - 2 - p^m\right] = \\ &= 1 + \frac{p}{p-1} + \frac{1}{p(p-1)} - \frac{1}{p-1} - \frac{2}{p^m(p-1)} = \\ &= 1 + 1 + \frac{1}{p-1} + \frac{1}{p(p-1)} - \frac{1}{p-1} - \frac{2}{p^m(p-1)} = \\ &= 2 + \frac{1}{p(p-1)} - \frac{2}{p^m(p-1)} \end{aligned}$$

which is exactly (2.2).

■

Remark 2.1. For the case $d = 1$, under certain conditions, all non-trivial characters have conductor 2, but we take the worst case because we only need an upper bound. These conditions were described by Serre in [19]; when they met, he called the extension $K_\mathfrak{p}$ "peu ramifiée", otherwise, the extension was called "très ramifiée".

Chapter 3
Application of Tate's bound

In this chapter we apply Tate's bound to $p = 2$ and $p = 3$. The case $p = 5$ requires assuming the Generalized Riemann Hypothesis, as proven in [2], and we do not study it. Let $n = [K : \mathbb{Q}] = [K_\mathfrak{p} : \mathbb{Q}_p]$.

3.1 Case $p = 2$

For $p = 2$, from Theorem 2.1 we have

$$v_2(\mathfrak{D}_{K_\mathfrak{p}/\mathbb{Q}_2}) \leq 2 + \frac{1}{2} - \frac{2}{2^m} < \frac{5}{2},$$

which means that

$$v_2(\mathfrak{d}_{K_\mathfrak{p}/\mathbb{Q}_2}) = v_2((d_{K_\mathfrak{p}/\mathbb{Q}_2})) < \frac{5}{2}n.$$

Now, if we assume that ρ is unramified outside of 2, the only prime dividing $d_{K/\mathbb{Q}}$ is 2, so the local result for $p = 2$ applies to the global extension, and we get

$$|d_{K/\mathbb{Q}}| \leq 2^{5n/2}$$

i.e.

$$|d_{K/\mathbb{Q}}|^{1/n} \leq 2^{5/2} < 5.66.$$

Odlyzko's bound (see Theorem 1.5 and Table A.1 in the Appendix) says that $|d_{K/\mathbb{Q}}|^{1/n} > 6$ for $n \geq 9$. Hence, if there is such an extension $K/\mathbb{Q}$, it must be of degree smaller than 9.

Proposition 3.1. *There are no non-trivial continuous irreducible Galois representations*

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_2)$$

unramified at every prime except 2.

Proof. We only need to study extensions $K/\mathbb{Q}$ of degree $n \leq 8$. First, we rule out every odd n, that is, every tamely ramified extension. If the extension $K/\mathbb{Q}$ is tamely ramified, then the higher ramification groups G_i are trivial for $i \geq 1$. Hence, by Remark 1.10, the conductor $f(\chi)$ is 0 or 1 for every character. The discriminant of an extension unramified outside 2 only has 2 as a prime factor, so the global conductor is either 1 or 2. By the conductor-discriminant formula (Proposition 1.15), the discriminant $|d_{K/\mathbb{Q}}|$ is then at most 2^n, which means that $|d_{K/\mathbb{Q}}|^{1/n} \leq 2$. This contradicts Odlyzko's bounds for every odd n, so there are no extensions $K/\mathbb{Q}$ unramified outside of 2 of odd degree.

Now we study the case $n = 6$. Since $6 = 3 \cdot 2$, the wild ramification index of this extension is 2 ($m = 1$). Hence, using Tate's bound, we get that $|d_{K/\mathbb{Q}}|^{1/n} \leq 2^{5/2-1} = 2^{3/2} < 2.83$, but this contradicts Odlyzko's bound. So this case is not possible either.

The only possible cases left are $n = 2$, $n = 4$ and $n = 8$, that is, the cases where G is a 2-group. This implies that the image $\rho(G)$ has to be a 2-group in $GL_2(\mathbb{F}_{2^t})$, for some $t \geq 1$. By Proposition 2.1 a Sylow 2-subgroup of $GL_2(\mathbb{F}_{2^t})$ is

$$T = \left\{ \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \mid x \in \mathbb{F}_{2^t} \right\} \cong \mathbb{F}_{2^t}.$$

So $\rho(G) \subseteq T$, which means that T is ρ-invariant. Since T is a proper subgroup of $GL_2(\mathbb{F}_{2^t})$, by Definition 1.41 ρ is reducible. ■

3.2 Case $p = 3$

For $p = 3$, we have

$$v_3(\mathfrak{D}_{K_\mathfrak{p}/\mathbb{Q}_3}) \leq 2 + \frac{1}{6} - \frac{1}{3^m} < \frac{13}{6},$$

which means that

$$v_3(\mathfrak{d}_{K_\mathfrak{p}/\mathbb{Q}_3}) = v_3((d_{K_\mathfrak{p}/\mathbb{Q}_3})) < \frac{13}{6}n.$$

By the same argument as before, we get

$$|d_{K/\mathbb{Q}}| \leq 3^{13n/6}$$

i.e.

$$|d_{K/\mathbb{Q}}|^{1/n} \leq 3^{13/6} < 10.81.$$

Odlyzko's bound says that $|d_{K/\mathbb{Q}}|^{1/n} > 10.829$ for $n \geq 25$. Hence, if there is such an extension $K/\mathbb{Q}$, it must be of degree smaller than 25. For this case, the bounds are not enough and we need to study the subgroups of $GL_2(\mathbb{F}_{3^t})$. To do so, we have the following proposition:

Proposition 3.2. *The maximal subgroups of $PSL_2(\mathbb{F}_q)$, for $q > 3$ odd, are:*

- *Dihedral groups of order $q - 1$ for $q \geq 13$;*
- *Dihedral groups or order $q + 1$ for $q \neq 7, 9$;*
- *A group of order $q(q-1)/2$ which stabilizes a point;*
- *$PSL_2(\mathbb{F}_{q_0})$ where q is an odd prime power of q_0;*
- *$PGL_2(\mathbb{F}_{q_0})$ where $q = q_0^2$.*
- *S_4 when $q \equiv \pm 1 \mod 8$ with either q prime or $q = p^2$ and $3 < p \equiv \pm 3 \mod 8$;*
- *A_4 when $q \equiv \pm 3 \mod 8$ with $q > 3$ prime;*
- *A_5 when $q \equiv \pm 1 \mod 10$ with either q prime or $q = p^2$ and $p \equiv \pm 3 \mod 10$.*

Using that $PGL_2(\mathbb{F}_q) \subset PSL_2(\mathbb{F}_{q^2})$, maximal subgroups of $PGL_2(\mathbb{F}_q)$, for $q > 3$ odd, are:

- *Dihedral groups of order $2(q-1)$ for $q \geq 13$;*
- *Dihedral groups or order $2(q+1)$ for $q \neq 7, 9$;*
- *A group of order $q(q-1)$ which stabilizes a point;*

- $PSL_2(\mathbb{F}_q)$;
- $PGL_2(\mathbb{F}_{q_0})$ *where* q *is an odd prime power of* q_0;
- S_4 *when* $q \equiv \pm 3 \mod 8$ *with* $q > 3$ *prime.*

A proof of this Proposition can be found in Dickson's classic book [6], summarized in [9].

Proposition 3.3. *There are no non-trivial continuous irreducible Galois representations*

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_3)$$

unramified at every prime except 3.

Proof. We start using the same strategy as before. Seeing that all tamely ramified extensions have discriminant smaller or equal than 3, we can rule out all of them except $n = 2$, because Odlyzko's bounds yield no contradiction in that case. For $n = 2$, the Galois group is C_2, which in $GL_2(\overline{\mathbb{F}}_{3^t})$ is conjugate to the subgroup

$$C = \left\langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \right\rangle .$$

Since $\rho(G) \subseteq C$, C is ρ-invariant, so ρ is reducible.

Moving on to the wildly ramified extensions, the cases $n = 6$, $n = 12$, $n = 15$, $n = 21$ and $n = 24$ (wild ramification index 3, so $m = 1$) yield Tate's bound $3^{11/6} < 7.5$, which by Odlyzko is a contradiction for $n = 15, 21, 24$. The case $n = 18$ (wild ramification index 9, so $m = 2$) yields Tate's bound $3^{37/18}$, which is not a contradiction with Odlyzko.

The cases $n = 3$ and $n = 9$, i.e., the cases where G is a 3-group, are solved the same way as the case $p = 2$ with the 2-groups: the Sylow 3-subgroup of $GL_2(\mathbb{F}_{3^t})$

$$T = \left\{ \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \mid x \in \mathbb{F}_{3^t} \right\} \cong \mathbb{F}_{3^t}$$

is ρ-invariant, so ρ is reducible.

For the cases $n = 6, 12, 18$, we first check the *L-functions and modular forms database* (LMFDB, see [23]), which contains a complete list of number fields unramified outside some sets of primes, including 3. There, we see that Galois extensions $K/\mathbb{Q}$ of degree 6 and 18 unramified outside 3 do exist, but not of degree 12. The process by which these extensions can be found is explained in Remark 3.1 below this proof, taking advantage of the fact that $6, 12, 18 < 60$ and thus every possible Galois group is solvable.

Now, for each of the Galois groups of the extensions that do exist, we have to consider how they fit in $GL_2(\overline{\mathbb{F}}_3)$. The goal is to find contradictions (the group does not fit) or seeing that a representation of the group would be reducible (in a suitable base). To do this, we take advantage of projection to $PGL_2(\mathbb{F}_{3^t})$ and $PSL_2(\mathbb{F}_{3^t})$ and use Proposition 3.2. The centre of $GL_2(\mathbb{F}_{3^t})$ consists on the matrices λId with $\lambda \in \mathbb{F}_{3^t}^*$, so it is always a subgroup of the cyclic group of order $3^t - 1$. For $PGL_2(\mathbb{F}_3)$, for example, the projection consists on the quotient of $GL_2(\mathbb{F}_3)$ by $\pm Id$.

Starting with C_6, a generator of this group is a matrix A such that $A^3 = -Id$, so its projective image is a C_3. Going over the classification of subgroups in $PGL_2(\mathbb{F}_{3^t})$ and $PSL_2(\mathbb{F}_{3^t})$, the dihedral maximal subgroups have order coprime to 3, so C_3 is not a subgroup of those, but it can be a subgroup of $PSL_2(\mathbb{F}_3) \cong A_4$, $PGL_2(\mathbb{F}_3) \cong S_4$, $A_5 \subset PGL_2(\mathbb{F}_9)$ or of groups of order $3^t(3^t - 1)$ that stabilize a point. The latter case implies an invariant subspace, so the representation would be reducible. For the other cases, the presentations are

$$\langle A, B, C \,|\, A^2 = B^3 = C^k = ABC = Id \rangle$$

with $k = 3$ for A_4 and $k = 4$ for S_4, and

$$\langle A, B \,|\, A^2 = B^3 = (AB)^5 = Id \rangle$$

for A_5. For A_4, the matrices

$$A = \left(\begin{smallmatrix} 1 & 2 \\ 2 & 2 \end{smallmatrix}\right), B = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), C = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$$

of $SL_2(\mathbb{F}_3)$ satisfy the conditions in $PSL_2(\mathbb{F}_3)$. For S_4, the matrices

$$A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), B = \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), C = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$$

of $GL_2(\mathbb{F}_3)$ satisfy the conditions in $PGL_2(\mathbb{F}_3)$. For A_5, the matrices

$$A = \left(\begin{smallmatrix} 0 & 2 \\ 1 & 0 \end{smallmatrix}\right), B = \left(\begin{smallmatrix} 1 & \alpha+1 \\ 0 & 1 \end{smallmatrix}\right).$$

of $SL_2(\mathbb{F}_9)$, with $\alpha^2 = 2$, satisfy the conditions in $PSL_2(\mathbb{F}_9)$. In all three cases, C_3 can be generated by B, which is an upper triangular matrix with ones in the diagonal, so again $\rho(G) \subseteq T$ with T as defined above, so ρ is reducible.

Moving on to $D_6 \cong S_3$, the classification tells us that there are no dihedral groups of order divisible by 3 in $PGL_2(\mathbb{F}_{3^t})$ for any $t \geq 1$, which means that the projective image of D_6 has to be in the reducible case of groups that stabilize a point. Thus, ρ is reducible as well.

Finally, for every group of order 18, even under projection to PGL or PSL it will remain a group of order divisible by 9, and A_4, S_4 and A_5 do not have order divisible by 9. These groups, hence, do not fit in $GL_2(\overline{\mathbb{F}}_3)$ or have reducible image, so we are done.

■

Remark 3.1. Given a solvable group, we can use class field theory to obtain the corresponding field extension unramified outside a certain set of primes, or to check that such an extension does not exist. The main tool for this are ray class groups, which we introduced after Theorem 1.13. A solvable Galois group $G = Gal(K/\mathbb{Q})$ can be split into a tower $1 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_k = G$ such that G_i/G_{i-1} is abelian for $i = 1, \ldots k$, so the corresponding extension $K/\mathbb{Q}$ is actually a tower of abelian extensions $K/K_{k-1}, K_{k-1}/K_{k-2}, \ldots, K_1/\mathbb{Q}$. For each of the fields $\mathbb{Q}, K_1, \ldots K_{k-1}$, we can take the modulus $\mathfrak{m}$ corresponding to the prime 3 and calculate their ray class field modulo $\mathfrak{m}$, which yields their largest abelian extension unramified outside of 3. If, at some point, the ray class group is trivial, then there is not an extension corresponding to G.

Appendix A
Odlyzko's lower bounds

Here we write the unconditional lower bounds that Odlyzko found for the root discriminant $|d_{K/\mathbb{Q}}|^{1/n}$ of Galois extensions $K/\mathbb{Q}$ of degree n, for $n \leq 25$. Odlyzko gives different bounds for totally real fields and not totally real fields, but here we just write the lowest bound. These values are extracted from [16].

n	Lower bound for $\lvert d_{K/\mathbb{Q}}\rvert^{1/n}$
2	1.719
3	2.513
4	3.250
5	3.927
6	4.549
7	5.121
8	5.646
9	6.134
10	6.585
11	7.004
12	7.395
13	7.760
14	8.102
15	8.423
16	8.725
17	9.010
18	9.280
19	9.536
20	9.779
21	10.010
22	10.229
23	10.438
24	10.638
25	10.829

Table A.1: Odlyzko's lower bounds for root discriminants

Bibliography

[1] F. Beukers. Upper bounds for discriminants. https://websites.math.leidenuniv.nl/edixhoven/ics/AG_Fall_2005/notes/beukers.pdf, 2005. Lecture notes, October 17, 2005.

[2] Sharon Brueggeman. The nonexistence of certain galois extensions unramified outside 5. *University of Illinois at Urbana-Champaign*, 1997. Available at CORE.

[3] Roger W. Carter and Paul Fong. The sylow 2-subgroups of the finite classical groups. *Journal of Algebra*, 1(2):139–151, 1964.

[4] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory*. Academic Press, 1967.

[5] Dexter Chua. Part iii — local fields: Based on lectures by h. c. johansson. https://dec41.user.srcf.net/notes/, 2016. Lecture notes from Michaelmas 2016, University of Cambridge.

[6] Leonard Eugene Dickson. *Linear Groups, with an Exposition of the Galois Field Theory*. Teubner, Leipzig, 1901. Reprinted by Dover Publications, 1958.

[7] Luis Dieulefait, Ariel Pacetti, and Fernando Rodríguez Villegas. Representaciones de galois. https://sweet.ua.pt/apacetti/cursos/Final.pdf, 2019. Notas del curso dictado en la escuela AGRA III, Aritmética, Grupos y Análisis, Córdoba, Argentina, 9–20 de julio de 2018.

[8] Shinya Harada. On the finiteness of mod p galois representations of a local field. *Tohoku Mathematical Journal*, 59(1):67–77, 2007.

[9] Oliver H. King. The subgroup structure of finite classical groups in terms of geometric configurations. In Bridget S. Webb, editor, *Surveys in Combinatorics 2005*, volume 327 of *London Mathematical Society Lecture Note Series*, pages 29–56. Cambridge University Press, 2005.

[10] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[11] Hyunsuk Moon. Finiteness results on certain mod p galois representations. *Journal of Number Theory*, 84(1):156–165, 2000.

[12] Hyunsuk Moon and Yuichiro Taguchi. Refinement of tate's discriminant bound and non-existence theorems for mod p galois representations. *Documenta Mathematica*, Extra Volume: Kazuya Kato's Fiftieth Birthday:641–654, 2003.

[13] Hyunsuk Moon and Yuichiro Taguchi. On the finiteness and non-existence of certain mod 2 galois representations of quadratic fields. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 84(5):63–67, 2008.

[14] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1999.

[15] Andrew M. Odlyzko. Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. *Séminaire de Théorie des Nombres de Bordeaux*, pages 1–15, 1976.

[16] Andrew M. Odlyzko. Discriminant bounds table (table 2). `https://www-users.cse.umn.edu/~odlyzko/unpublished/discr.bound.table2`, Accessed May 2025. Unpublished data on discriminant bounds.

[17] Jean-Pierre Serre. *Corps Locaux*. Hermann, 1968.

[18] Jean-Pierre Serre. Valeurs propres des opérateurs de hecke modulo l. *Astérisque*, 24–25:109–117, 1975.

[19] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de gal(q/q). *Duke Mathematical Journal*, 54(1):179–230, 1987.

[20] Jean-Pierre Serre. *Oeuvres – Collected Papers III: 1972–1984*. Collected Works in Mathematics. Springer-Verlag, Berlin, Heidelberg, 2003. Reprint of the 2003 edition, published in 2013.

[21] Andrew V. Sutherland. Class field theory: Ray class groups and ray class fields. `http://math.mit.edu/classes/18.785/2017fa/`, 2017. Lecture #21, 18.785 Number Theory I, Fall 2017, Massachusetts Institute of Technology.

[22] John Tate. The non-existence of certain galois extensions of $\mathbb{Q}$ unramified outside 2. In Gary Cornell and Joseph H. Silverman, editors, *Arithmetic Geometry*, volume 174 of *Contemporary Mathematics*, pages 153–156. American Mathematical Society, Providence, RI, 1994.

[23] The LMFDB Collaboration. The l-functions and modular forms database. `https://www.lmfdb.org`. Accessed: 2025-06-07.

[24] Mehmet Haluk Şengün. The nonexistence of certain representations of the absolute galois group of quadratic fields. *Proceedings of the American Mathematical Society*, 137(1):27–35, 2009.