PROVING THE TCHEBOTAREV DENSITY THEOREM

NICOLAS SIMARD

CONTENTS

INTRODUCTION

Dirichlet's theorem on primes in arithmetic progression tells us that

$$\lim_{N\to\infty} \frac{\#\{p \text{ prime} | p \leq N \text{ and } p \equiv a \pmod{q}\}}{\pi(N)} = \frac{1}{\phi(q)}$$

In these notes, we will explain and prove the following theorem, due to Tchebotarev:

Theorem 1 (Tchebotarev's Theorem)**.** *Let* L/K *be a Galois extension of number fields with Galois group* G *and let* c *be the conjugacy class in* G*. Then the set* $\mathcal{P}_{L/K}(c) = \left\{ \mathfrak{p} \text{ prime in } K \,\middle|\, \left(\frac{E/K}{\mathfrak{p}}\right) = c \right\}$ *has Dirichlet density* $\frac{|c|}{|G|}$.

To do so, we will proceed in three steps. First, we will reinterpret Dirichlet's theorem in terms of ideals. This will allows us to generalise his theorem to number fields. Then, using the main results of class field theory, we will obtain version of Tchebotarev's theorem valid for abelian extensions. Finally, we will prove Theorem 1 by using this abelian version of it and by carefully analysing the decomposition of primes in Galois extensions.

Along the way, we will recall the important concepts needed to understand and prove Tchebotarev's theorem. We assume that the reader is familiar with Galois theory, classical algebraic number theory (number fields, primes decomposition, ideal class group, etc.) and the theory of "classical" Dirichlet L-functions. The Artin map will be defined and the main results of class field theory will be stated

Date: September 26, 2016.

(without proof!). For an easy-to-read first contact with class field theory, Cox's book [Cox] is excellent!

1. From rational numbers to ideals

As we said in the introduction, our first objective is to generalise Dirichlet's theorem on primes in arithmetic progression to number fields. Unfortunately, we cannot do this directly for one good reason: the integers in number fields do not factor uniquely in general. In fact, it is known that the ring of integers in imaginary quadratic fields is a unique factorisation domain in only 9 cases. For real quadratic fields, the question is still open. Our first challenge will be to define Dirichlet L-series in number fields. But what is the correct analogue of a character of $(\mathbb{Z}/m\mathbb{Z})^\times$?

Let's start by reinterpreting the "classical" Dirichlet L-series, i.e. the series of the form

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

where s is a complex number and χ is a character of $(\mathbb{Z}/m\mathbb{Z})^\times$ extended to $\mathbb{Z}$ in the natural way. First, we want realise $(\mathbb{Z}/m\mathbb{Z})^\times$ as a quotient of a certain group of (fractional) ideals (recall that in number fields, we need to consider ideals to recover unique factorisation). Our first guess might be to look at a map like

$$\begin{aligned} \{a\mathbb{Z} | a \in \mathbb{Z}\} &\longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \\ a\mathbb{Z} &\longmapsto [a] \end{aligned}$$

but the set of ideals $\{a\mathbb{Z}|a \in \mathbb{Z}\}$ is not a group and the map is not well-defined if $(a,m) \neq 1$. This leads naturally to the consideration of the set $I_{\mathbb{Q}}^m = \{\frac{a}{b}\mathbb{Z} | a, b \in \mathbb{Z} \text{ and } (a,m) = (b,m) = 1\}$ and the map

$$\begin{aligned} I_{\mathbb{Q}}^m &\longrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \\ \frac{a}{b}\mathbb{Z} &\longmapsto [a][b]^{-1} \end{aligned}$$

where we choose the positive generator of $\frac{a}{b}\mathbb{Z}$ (i.e. $\frac{a}{b} > 0$). This map is well-defined and clearly surjective. The kernel is the set of ideals $\frac{a}{b}\mathbb{Z}$ where the positive generator $\frac{a}{b}$ is such that $ab^{-1} \equiv 1 \pmod m$ or equivalently $a \equiv b \pmod m$. If we define $\mathbb{Q}_m = \{\frac{a}{b} \in \mathbb{Q} | (a,m) = (b,m) = 1\}$, $\mathbb{Q}_{m\infty,1} = \{\frac{a}{b} \in \mathbb{Q}_m | a \equiv b \pmod m, \frac{a}{b} > 0\}$ and $\iota : \mathbb{Q}_{m\infty,1} \longrightarrow I_{\mathbb{Q}}^m$ to be the map sending a rational number to the principal ideal it generates, we proved that

$$I_{\mathbb{Q}}^m / \iota(\mathbb{Q}_{m\infty,1}) \simeq (\mathbb{Z}/q\mathbb{Z})^\times$$

The reason why we put the symbol ∞ in $\mathbb{Q}_{m\infty,1}$ will soon be apparent.

2. Ray class groups and generalised L-series

The above realisation of $(\mathbb{Z}/q\mathbb{Z})^\times$ as a quotient of a group of ideals may look sophisticated, but it has the advantage of being easy to generalise to other number fields. First, we define the analogue of m.

Definition 1. *Let K be a number field. A modulus $\mathfrak{m}$ is a formal product*

$$\mathfrak{m} = \prod_{\mathfrak{p} \text{ prime}} \mathfrak{p}^{n_\mathfrak{p}}$$

where

(1) $n_\mathfrak{p} \geq 0$ *for all primes and* $n_\mathfrak{p} > 0$ *for finitely many primes.*
(2) $n_\mathfrak{p} = 0$ *or* 1 *if* $\mathfrak{p}$ *is a real infinite prime.*
(3) $n_\mathfrak{p} = 0$ *if* $\mathfrak{p}$ *is a complex infinite prime.*

Recall that a finite prime of K is a prime ideal of $\mathcal{O}_K$, a real infinite prime is an embedding $\sigma : K \hookrightarrow \mathbb{R}$ and a complex infinite prime is a pair of complex conjugate embeddings $\sigma, \overline{\sigma} : K \hookrightarrow \mathbb{C}$, where $\sigma \neq \overline{\sigma}$. For example, a real quadratic field has two real infinite primes and no complex infinite primes, an imaginary quadratic field has no real infinite prime and one complex infinite prime and $\mathbb{Q}(\sqrt[3]{2})$ has one real infinite prime and one complex infinite prime.

Any modulus $\mathfrak{m}$ can be written uniquely as $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an integral ideal of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a formal product of distinct real infinite primes. Note that $\mathbb{Q}$ has only one real prime, namely the inclusion of $\mathbb{Q}$ in $\mathbb{R}$, which we denote ∞. With this notation, $m\infty$ is a modulus of $\mathbb{Q}$ for any integer m.

We will now define the analogue of $I_\mathbb{Q}^m$. Let $\mathfrak{m}$ be a modulus of K and let I_K be the group of fractional ideals of K, i.e. the free abelian group generated by the prime ideals of $\mathcal{O}_K$. We define

$$I_K^\mathfrak{m} = \{\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \dots \mathfrak{p}_n^{\alpha_n} | (\mathfrak{p}_i, \mathfrak{m}_0) = 1 \text{ for all } i\}$$

In other words, $I_K^\mathfrak{m}$ is the set of ideals prime to $\mathfrak{m}_0$. It is easy to see that $I_K^\mathfrak{m}$ is the subgroup of I_K generated by the primes that do not divide $\mathfrak{m}_0$. We also define

$$K_\mathfrak{m} = \left\{ \frac{a}{b} \in K^\times | (a\mathcal{O}_K, \mathfrak{m}_0) = (b\mathcal{O}_K, \mathfrak{m}_0) = 1 \right\}$$

and

$$K_{\mathfrak{m},1} = \{x \in K^\times | x \equiv 1 \pmod{\mathfrak{m}}\}$$

where $x \equiv 1 \pmod{\mathfrak{m}}$ has the following meaning. First, if σ is a real infinite prime dividing $\mathfrak{m}_\infty$, it means that $\sigma(x) > 0$. If $\mathfrak{p}$ divides $\mathfrak{m}_0$ to the exact power $n_\mathfrak{p}$, it means that $\mathrm{ord}_\mathfrak{p}(x-1) \geq n_\mathfrak{p}$, where $\mathrm{ord}_\mathfrak{p}$ is the normalised discrete valuation on $K^\times$ associated to $\mathfrak{p}$.

One can easily verify that $K_\mathfrak{m} \subseteq K_{\mathfrak{m},1}$. Taking $x = \frac{a}{b} \in K_\mathfrak{m}$ and using the properties of $\mathrm{ord}_\mathfrak{p}$, we see that $x \in K_{\mathfrak{m},1}$ is equivalent to $a - b \in \mathfrak{p}^{n_\mathfrak{p}}$ for all the finite primes $\mathfrak{p}$ dividing $\mathfrak{m}$ and $\sigma(a/b) > 0$ for all real infinite primes σ dividing $\mathfrak{m}$. This equivalent definition now coincides with the definition of $\mathbb{Q}_{m\infty,1}$ we gave above.

Now letting $\iota : K_\mathfrak{m} \longrightarrow I_K^\mathfrak{m}$ be the map sending x to $x\mathcal{O}_K$, we can define the ray class groups.

Definition 2. *Let* K *be a number field and* $\mathfrak{m}$ *a modulus of* K*. The ray class group mod* $\mathfrak{m}$*, denoted* $C_\mathfrak{m}$*, is defined as the quotient*

$$I_K^\mathfrak{m} / \iota(K_{\mathfrak{m},1})$$

The order of $C_\mathfrak{m}$ *is denoted* $h_\mathfrak{m}$*.*

The second part of this definition makes sense, as one can show that the ray class group mod $\mathfrak{m}$ is always finite. These objects may seem very abstract at first sight, but in fact they are familiar in many cases.

Example 1.

Take the field K to be $\mathbb{Q}$ and take the modulus $\mathfrak{m}$ to be $m\infty$ for some integer m. What we actually proved at the beginning of this section is that

$$C_{m\infty} \simeq (\mathbb{Z}/m\mathbb{Z})^\times$$

and so $h_{m\infty} = \varphi(m)$. Note that $I_{\mathbb{Q}}^{m} = I_{\mathbb{Q}}^{m\infty}$.

Example 2.

Let K be any field and let $\mathfrak{m} = 1$ be the trivial modulus. In this case $I_K^{\mathfrak{m}} = I_K$ and $K_{\mathfrak{m},1} = K^\times$, so $C_1 = \mathrm{Cl}(K)$ is the usual class group of K and $h_1 = h_K$ is just the class number of K. Therefore one should consider ray class groups as a natural generalisation of the usual class group of a field.

Example 3.

Let K be a real quadratic field and let ∞_0 and ∞_1 denote its two real infinite primes. Taking $\mathfrak{m} = \infty_0\infty_1$, we obtain the narrow-class group of K. Indeed, $I_K^{\mathfrak{m}} = I_K$ and so $C_{\mathfrak{m}}$ is the group of ideals modulo principal ideals generated by totally positive elements, i.e. elements that are positive under each embedding of K in $\mathbb{R}$. In this case, $h_{\mathfrak{m}}$ is denoted h_+ and is called the narrow-class number. One can show that $h_+ = 2h_K$ or h_K, depending on the sign of the norm of the fundamental unit.

Example 4.

Let K be an imaginary quadratic field. A well-known result says that the ideal class group of K is isomorphic to the group of binary quadratic forms of discriminant D_K, the discriminant of K. For a non-fundamental quadratic discriminant $D < 0$, things are slightly more complicated. Writing D as $D = f^2 D_0$, where D_0 is fundamental, one can show that the form class group of discriminant D is naturally isomorphic to the group of proper ideals of the order of conductor f in K. With more work, one can show that this group is in fact a quotient of the ray class group mod $f\mathcal{O}_K$. In this sense, the ray class groups of a quadratic imaginary field allows us to recover the correspondence between form class groups and ideal class groups in quadratic fields.

These ray class groups will play a role analogue to $(\mathbb{Z}/m\mathbb{Z})^\times$ in number fields other than $\mathbb{Q}$, as one can see in the following definition:

Definition 3. *Let K be a number field, $\mathfrak{m}$ be a modulus of K and χ be a character of $C_{\mathfrak{m}} = I_K^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1})$, the ray class group mod $\mathfrak{m}$. Then a Dirichlet L-series is a series of the form*

$$L_{\mathfrak{m}}(s,\chi) = \sum_{\mathfrak{a}\subseteq\mathcal{O}_K} \frac{\chi(\mathfrak{a})}{\mathbb{N}(\mathfrak{a})^s}$$

where $\mathbb{N}(\mathfrak{a}) = (\mathcal{O}_K : \mathfrak{a})$, $\chi(\mathfrak{a}) = 0$ if $(\mathfrak{a}, \mathfrak{m}_0) \neq 1$ and $\chi(\mathfrak{a}) = \chi(\mathfrak{a} \mod \iota(K_{\mathfrak{m},1}))$ if $(\mathfrak{a}, \mathfrak{m}_0) = 1$.

This definition is almost identical to the definition of the classical Dirichlet L-series. In fact, if we take $K = \mathbb{Q}$ and $\mathfrak{m} = m\infty$, we proved that the Dirichlet L-series defined above coincide with the classical Dirichlet L-series. Note also that for an arbitrary number K, the Dirichlet L-series associated to the trivial modulus $\mathfrak{m} = 1$

and the trivial character χ_0 coincides with the zeta function of K, i.e. $L_1(s,\chi_0) = \zeta_K(s)$.

These generalized Dirichlet L-series have many properties in common with the classical L-series, as can be seen in the next theorem.

Theorem 2. *Let K be a number field, $\mathfrak{m}$ a modulus and χ a character of $C_{\mathfrak{m}}$. Then*

(1) *For $Re(s) > 1$, $L_{\mathfrak{m}}(s,\chi)$ is analytic and has an Euler product expansion:*

$$L_{\mathfrak{m}}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}_0} (1-\chi(\mathfrak{p})\mathbb{N}(\mathfrak{p})^{-s})^{-1}$$

(2) *If $\chi \neq \chi_0$, $L_{\mathfrak{m}}(s,\chi)$ can be analytically continued to the region $Re(s) > 1 - 1/[K:\mathbb{Q}]$. Moreover, $L_{\mathfrak{m}}(1,\chi) \neq 0$ in this region.*

(3) *If $\chi = \chi_0$, $L_{\mathfrak{m}}(s,\chi_0)$ can be analytically continued to the region $Re(s) > 1 - 1/[K:\mathbb{Q}]$ except for a simple pole at $s = 1$. Moreover, if $\mathfrak{m} = 1$, the residue of $L_1(s,\chi_0) = \zeta_K(s)$ is*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}Reg(K)}{w_K\sqrt{|D_K|}}h_K$$

where

- *r_1 is the number of real infinite primes of K and r_2 is the number of complex infinite primes of K.*
- *$Reg(K)$ is the regulator of K.*
- *w_K, called the root number, is the number of roots of unity in K.*
- *D_K is the discriminant of K.*
- *h_K is the class number of K.*

Proof. We will not give a full proof of all these results here, but we will give precise references.

For the proof of (1), see [Neu] Chapter V, Theorem 2.2. Note that assuming the convergence of $L_{\mathfrak{m}}(s,\chi)$ for $\mathrm{Re}(s) > 1$, it is not hard to show the existence of the Euler product.

For a proof of the continuation of $L_{\mathfrak{m}}(s,\chi)$ for $\chi \neq \chi_0$, see [Neu] Chapter V, Theorem 3.2. The non-vanishing is much harder to prove. See for example [Jan], Chapter V, Proposition 10.2. For a proof using Artin L-functions, see [Neu], Chapter V, Lemma 6.3. Both proofs rely on the existence theorem of class field theory.

For a proof of (3), see [Neu] Chapter V, Theorem 2.2 and [Jan], Chapter IV, Theorem 2.14. □

Recall that the proof of Dirichlet's theorem on primes in arithmetic progressions relies crucially on the fact that $\zeta_{\mathbb{Q}}(s) = \zeta(s)$ has a simple pole at $s = 1$ and $L(s,\chi)$ is defined and non-vanishing at $s = 1$. This theorem generalises those results and will also play a very important role in the proof of Tchebotarev's theorem. It is worth noting that the formula giving the residue of $\zeta_K(s)$ at $s = 1$ is called the *class number formula*.

Example 5.

Using the class number formula for the field $\mathbb{Q}$, we see that $\zeta(s)$ has residue 1 at $s = 1$. This could be seen using much simpler methods!

Example 6.

Let K be a quadratic number field.

If K is imaginary, then we saw that $r_2 = 0$ and $r_1 = 1$. Since $\mathcal{O}_K^\times$ has rank $r_1 + r_2 - 1 = 0$ as a $\mathbb{Z}$-module, $\mathrm{Reg}(K) = 1$ and the class number formula tells us that the residue at $s = 1$ of $\zeta_K(s)$ is

$$\frac{2\pi}{w_K\sqrt{|D_K|}}h_K$$

Using the correspondence between quadratic forms and ideals, we see that this formula is essentially equivalent to Dirichlet's class number formula for imaginary quadratic fields.

If K is a real quadratic field, then $r_1 = 2$ and $r_2 = 0$. Moreover, $w_K = 2$ and $\mathrm{Reg}(K) = \log|\epsilon_K|$, where ϵ_K is a fundamental unit of K. Then the residue of $\zeta_K(s)$ at $s = 1$ is simply

$$\frac{2\log|\epsilon_K|}{2\sqrt{D_K}}h_K = \frac{\log|\epsilon_K|}{\sqrt{D_K}}h_K$$

Here the correspondence with Dirichlet's class number formula is slightly less trivial. This is because the form class group is isomorphic to the narrow-class group of K, so $h_K = h_+$ or $2h_+$, where h_+ is the narrow-class number of K. Thus the formula above essentially gives Dirichlet's class number formula, modulo a factor of 2, depending on the sign of the norm of the fundamental unit.

3. Dirichlet density

Before starting the proof of the Tchebotarev density theorem, we need to define the notion of Dirichlet density. First, we introduce some notation. Given functions f and g, we write $f \sim g$ if $f - g$ is analytic in some neighbourhood of $s = 1$.

Definition 4. *Let K be a number field and let $\mathcal{S}$ be a set of finite primes of K. The Dirichlet density of $\mathcal{S}$, denotes $\delta(\mathcal{S})$ is defined as*

$$\delta(\mathcal{S}) = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in\mathcal{S}} \mathbb{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathbb{N}(\mathfrak{p})^{-s}} = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in\mathcal{S}} \mathbb{N}(\mathfrak{p})^{-s}}{-\log(s-1)}$$

provided that the limit exists.

Note that the second equality in the definition follows from the fact that

$$\log(\zeta_K(s)) = \sum_{\mathfrak{p}}\sum_{m=1}^{\infty} \frac{1}{m\mathbb{N}(\mathfrak{p})^{sm}} = \sum_{\mathfrak{p}} \mathbb{N}(\mathfrak{p})^{-s} + \sum_{\mathfrak{p}}\sum_{m=2}^{\infty} \frac{1}{m\mathbb{N}(\mathfrak{p})^{sm}} \sim \sum_{\mathfrak{p}} \mathbb{N}(\mathfrak{p})^{-s}$$

and

$$\log(\zeta_K(s)) \sim -\log(s-1)$$

where we used the fact that if $\mathfrak{p}$ is a prime of K lying over the rational prime p (i.e. $\mathfrak{p}\cap\mathbb{Z} = p\mathbb{Z}$), then $\mathbb{N}(\mathfrak{p}) = p^{f(\mathfrak{p}/p)}$, where $f(\mathfrak{p}/p)$ is the inertial degree of $\mathfrak{p}$.

The Dirichlet density has many properties. Here are a few of them:

Proposition 1. *Let $\mathcal{S}$ and $\mathcal{T}$ be sets of finite primes of a number field K and let $\mathcal{P}_K$ be the set of all finite primes of K. Then*

1. $\delta(\mathcal{P}_K) = 1$.
2. *If $\mathcal{S}$ is finite, then $\delta(\mathcal{S}) = 0$.*
3. *If $\mathcal{S}\subseteq\mathcal{T}$, then $\delta(\mathcal{S}) \le \delta(\mathcal{T})$ whenever both densities exist.*
4. *If $\delta(\mathcal{S})$ exists, $0 \le \delta(\mathcal{S}) \le 1$.*

(5) *If $\mathcal{S}$ and $\mathcal{T}$ are disjoint, then $\delta(\mathcal{S} \cup \mathcal{T}) = \delta(\mathcal{S}) + \delta(\mathcal{T})$ whenever both densities exist.*
(6) *Let $\mathcal{R} = \{\mathfrak{p} \in \mathcal{P}_K | f(\mathfrak{p}/\mathbb{Z}) = 1\}$ be the set of primes of relative degree 1 over $\mathbb{Q}$. Then $\delta(\mathcal{S}) = \delta(\mathcal{S} \cap \mathcal{R})$, whenever the density of $\mathcal{S}$ exists.*

Proof. The proof of $(1) - (5)$ follows directly from the definition. For the last property, first note that if $\mathfrak{p} \in \mathcal{R}$ and $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, then $\mathbb{N}(\mathfrak{p}) = p$. If $\mathfrak{p} \notin \mathcal{R}$, then $\mathbb{N}(\mathfrak{p}) \geq p^2$ and there are at most $[K : \mathbb{Q}]$ primes of K lying over a fixed prime of $\mathbb{Q}$. It follows that

$$\sum_{\mathfrak{p} \in \mathcal{S}} \frac{1}{\mathbb{N}(\mathfrak{p})^s} = \sum_{\mathfrak{p} \in \mathcal{S} \cap \mathcal{R}} \frac{1}{p^s} + \sum_{\mathfrak{p} \in \mathcal{S} \setminus \mathcal{R}} \frac{1}{\mathbb{N}(\mathfrak{p})^s} \sim \sum_{\mathfrak{p} \in \mathcal{S} \cap \mathcal{R}} \frac{1}{p^s}$$

since the second sum is

$$\left| \sum_{\mathfrak{p} \in \mathcal{S} \setminus \mathcal{R}} \frac{1}{\mathbb{N}(\mathfrak{p})^s} \right| \leq [K : \mathbb{Q}] \sum_{p \in \mathbb{Q}} \frac{1}{p^{2\sigma}} < \infty$$

for any $\sigma > 1$. □

The last property of the density tells us that when we compute the density of a set of primes, we may suppose that our primes are of relative degree one over $\mathbb{Q}$. The fourth and the fifth property, together with the fact that only finitely many primes of $\mathbb{Q}$ ramify in K, tells us that we may also suppose that our primes are unramified.

To conclude this section about densities, note that one can define a more natural density for a set $\mathcal{S}$ of primes of K as follows:

$$\delta_{\text{nat}}(\mathcal{S}) = \lim_{N \to \infty} \frac{\{\mathfrak{p} \in \mathcal{S} | \mathbb{N}(\mathfrak{p}) \leq N\}}{\{\mathfrak{p} \text{ prime} | \mathbb{N}(\mathfrak{p}) \leq N\}}$$

provided that this limit exists. This density is called the *natural density* of $\mathcal{S}$. One can show that if $\delta_{\text{nat}}(\mathcal{S})$ exists, $\delta(\mathcal{S})$ exists and $\delta_{\text{nat}}(\mathcal{S}) = \delta(\mathcal{S})$. However, the natural density may fail to exist even if the Dirichlet density exists.

4. Dirichlet's theorem revisited

We are now ready to prove a generalized version of Dirichlet's theorem on primes in arithmetic progressions.

Theorem 3. *Let K be a number field, let $\mathfrak{m}$ be a modulus of K and let $\mathfrak{h}_0$ be a fixed class in $C_{\mathfrak{m}}$, the ray class group mod $\mathfrak{m}$. If $\mathcal{P}(\mathfrak{h}_0)$ denotes the set of primes of K that are prime to $\mathfrak{m}_0$ and congruent to $\mathfrak{h}_0 \mod \iota(K_{\mathfrak{m},1})$, then*

$$\delta(\mathcal{P}(\mathfrak{h}_0)) = \frac{1}{|C_{\mathfrak{m}}|}$$

Before proving this theorem, recall that if $\hat{G}$ denotes the group of characters of a finite abelian group G, i.e. $\hat{G} = \{\text{homomorphism } \chi : G \longrightarrow \mathbb{C}^\times\}$, then

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} |G| & \text{if } g = 1 \\ 0 & \text{if } g \neq 1 \end{cases}$$

for any $g \in G$.

Proof. The proof is identical to the proof of Dirichlet's theorem. First, we see that for $\mathrm{Re}(s) > 1$

$$\log L_m(s,\chi) = \sum_{\mathfrak{p}\nmid \mathfrak{m}_0} \sum_{m=1}^{\infty} \frac{\chi(\mathfrak{p})^m}{m\mathbb{N}(\mathfrak{p})^{ms}} \sim \sum_{\mathfrak{p}\nmid \mathfrak{m}_0} \frac{\chi(\mathfrak{p})}{\mathbb{N}(\mathfrak{p})^s} = \sum_{\mathfrak{p}} \frac{\chi(\mathfrak{p})}{\mathbb{N}(\mathfrak{p})^s}$$

It follows that

$$\sum_{\chi \bmod \mathfrak{m}} \chi^{-1}(\mathfrak{h}_0) \log L_m(s,\chi) \sim \sum_{\mathfrak{p}} \frac{\sum_{\chi \bmod \mathfrak{m}} \chi^{-1}(\mathfrak{h}_0)\chi(\mathfrak{p})}{\mathbb{N}(\mathfrak{p})^s} = |C_m| \sum_{\mathfrak{p}\in\mathcal{P}(\mathfrak{h}_0)} \frac{1}{\mathbb{N}(\mathfrak{p})^s}$$

where the sum $\sum_{\chi \bmod \mathfrak{m}}$ runs over all characters of C_m. Using the first part of theorem 2, we see that for $\mathrm{Re}(s) > 1$,

$$L_m(s,\chi_0) = \prod_{\mathfrak{p}\nmid \mathfrak{m}_0} (1-\mathbb{N}(\mathfrak{p})^{-s})^{-1} = \zeta_K(s) \prod_{\mathfrak{p}\mid \mathfrak{m}_0} (1-\mathbb{N}(\mathfrak{p})^{-s})$$

and so $\log L_m(s,\chi_0) \sim \log \zeta_K(s) \sim -\log(s-1)$. Using this and theorem 2 again, we see that

$$\log L_m(s,\chi_0) + \sum_{\chi\neq\chi_0} \chi^{-1}(\mathfrak{h}_0) \log L_m(s,\chi) \sim -\log(s-1)$$

This proves that

$$|C_m| \sum_{\mathfrak{p}\in\mathcal{P}(\mathfrak{h}_0)} \frac{1}{\mathbb{N}(\mathfrak{p})^s} \sim -\log(s-1)$$

and completes the proof. □

If we take K to be $\mathbb{Q}$ and $\mathfrak{m}$ to be $m\infty$, we obtain directly Dirichlet's theorem. Note the importance of theorem 2 in the proof: the two main ingredients were the simple pole of $L_m(s,\chi_0)$ at $s = 1$ and the non-vanishing of $L_m(s,\chi)$ at $s = 1$ for $\chi \neq \chi_0$.

5. Class field theory

In the previous section, we completed the first step of our three step proof of the Tchebotarev theorem. In order to complete the second one, we will need to translate our result about the density of primes lying in certain residue classes into a result involving the Galois group of certain extensions. We will do so with the help of class field theory.

Class field theory is one of the most elegant part of algebraic number theory. The main results are easy to state and relatively simple to understand. However, the proofs are long and use many tools. In this section, we will start by briefly recalling the construction of the Artin map. Then we will state (without proof), the two main results of class field theory, namely the *Artin Reciprocity Law* and the *Existence Theorem*.

Let L/K be an extension of number fields. Then $\mathcal{O}_K$ is a Dedekind domain and so the ideals of K factor uniquely into a product of primes ideals (if not explicitly mentioned, we suppose that our primes are finite). If $\mathfrak{p}$ be a prime of K, we also know that

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

where the $\mathfrak{P}_i$ are primes of $\mathcal{O}_L$ and $e_i \geq 1$. Moreover, $\mathcal{O}_L/\mathfrak{P}_i$ is a finite extension of $\mathcal{O}_K/\mathfrak{p}$ and we let f_i denote the degree of this extension. This f_i is called the *relative*

degree of $\mathfrak{P}_i$ over $\mathfrak{p}$ (or K). If L/K is a Galois extension, then the e_i are all equal to some e and the f_i are all equal to f. This gives the very useful relation $[L : K] = efg$. Recall also that only finitely many primes of K are ramified in L. If $\mathfrak{P}$ is a prime of L and $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$, so that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^e \dots$, we denote e by $e(\mathfrak{P}/K)$ and the relative degree of $\mathfrak{P}$ by $f(\mathfrak{P}/K)$.

Proposition 2. *Let $E/L/K$ be extensions of number fields. Let $\mathfrak{p}_E$ be a prime of E and let $\mathfrak{p}_L = \mathfrak{p}_E \cap \mathcal{O}_L$ and $\mathfrak{p}_K = \mathfrak{p}_E \cap \mathcal{O}_K$. Then*

(1) $f(\mathfrak{p}_E/K) = f(\mathfrak{p}_E/L)f(\mathfrak{p}_L/K)$.
(2) $e(\mathfrak{p}_E/K) = e(\mathfrak{p}_E/L)e(\mathfrak{p}_L/K)$.

Proof. The proof of the second point is seen by looking at the decomposition of $\mathfrak{p}_K$ in L and of $\mathfrak{p}_L$ in E. The first point follows from the multiplicativity of the degree of field extensions. □

This proposition can be used to analyse the decomposition of primes in multiple extensions. For example, if a prime in a number field K is unramified in L, it is unramified in any field F such that $L \supseteq F \supseteq K$. If a prime in a number field K has relative degree one over $\mathbb{Q}$, it must have relative degree one over any field contained in K.

Now suppose that L/K is a Galois extension with Galois group G and let $\mathfrak{P}$ be a prime of L. Any automorphism $\sigma : L \longrightarrow L$ induces a map $\sigma : \mathcal{O}_L \longrightarrow \mathcal{O}_L/\mathfrak{P}$, which factors through $\mathfrak{P}$ if and only if $\sigma(\mathfrak{P}) = \mathfrak{P}$. The subgroup of G formed by the automorphisms that preserve $\mathfrak{P}$ (i.e. such that $\sigma(\mathfrak{P}) = \mathfrak{P}$) is called the *decomposition group* of $\mathfrak{P}$ and is denoted $D(\mathfrak{P})$. Let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$ and let $k_{\mathfrak{P}} = \mathcal{O}_L/\mathfrak{P}$ and $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$ denote the residue fields of $\mathfrak{P}$ and $\mathfrak{p}$. Then the reasoning above shows that we have a well defined map

$$\tilde{\cdot} : D(\mathfrak{P}) \longrightarrow \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$$

sending σ to $\tilde{\sigma}$, where $\tilde{\sigma}(\alpha+\mathfrak{P}) = \sigma(\alpha)+\mathfrak{P}$. The map $\tilde{\cdot}$ is clearly a homomorphism and one can show that it is also surjective. The kernel of this map, called the *inertia subgroup*, is $I(\mathfrak{P}) = \{\sigma \in G | \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}\}$. Since $D(\mathfrak{P})$ has order $e(\mathfrak{P}/K)f(\mathfrak{P}/K)$, $I(\mathfrak{P})$ has order $e(\mathfrak{P}/K)$.

Now take a prime $\mathfrak{p}$ in K that is unramified in L and fix a $\mathfrak{P}$ of L that divides $\mathfrak{p}$. Since $\mathfrak{p}$ is unramified, $e(\mathfrak{P}/\mathfrak{p}) = 1$ and it follows by what we mentioned above that $D(\mathfrak{P}) \simeq \mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$. We know that $\mathrm{Gal}(k_{\mathfrak{P}}/k_{\mathfrak{p}})$ is cyclic and generated by the Frobenius element and so there exists a unique element of $D(\mathfrak{P})$ that maps to it. We denote this element by

$$\left(\frac{L/K}{\mathfrak{P}}\right) \in D(\mathfrak{P})$$

The symbol $\left(\frac{L/K}{\bullet}\right)$ is called the *Artin symbol*.

If we choose another prime of L that divides $\mathfrak{p}$, say $\mathfrak{P}'$, then $\mathfrak{P}' = \tau(\mathfrak{P})$ for some $\tau \in G$ (recall that such a τ always exists, as G acts transitively on the set of primes of L dividing $\mathfrak{p}\mathcal{O}_L$). We then see that $D(\mathfrak{P}') = D(\tau(\mathfrak{P})) = \tau D(\mathfrak{P})\tau^{-1}$ and similarly

$$\left(\frac{L/K}{\mathfrak{P}'}\right) = \left(\frac{L/K}{\tau(\mathfrak{P})}\right) = \tau\left(\frac{L/K}{\mathfrak{P}}\right)\tau^{-1}$$

This relation shows that in general the Artin symbol depends on the choice of prime of L dividing $\mathfrak{p}$. However, the symbol is independant of this choice in the

case where L/K is abelian. Thus the symbol

$$\left(\frac{L/K}{\mathfrak{p}}\right)$$

is well-defined. If we let $\mathfrak{m}$ be a modulus divisible by all the (finitely many) ramified primes of K, we obtain the so-called *Artin map*

$$\left(\frac{L/K}{\bullet}\right) : I_K^{\mathfrak{m}} \longrightarrow \mathrm{Gal}(L/K)$$

by defining

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{\mathfrak{p}\subseteq K \text{ prime}} \left(\frac{L/K}{\mathfrak{p}}\right)^{\alpha_{\mathfrak{p}}}$$

if $\mathfrak{a} = \prod_{\mathfrak{p}\subseteq K \text{ prime}} \mathfrak{p}^{\alpha_{\mathfrak{p}}}$, as we would do for the Jacobi symbol. The condition on $\mathfrak{m}$ is there to ensure that the Artin symbol is well defined (if $\mathfrak{p}$ is ramified in L, there is more than one element of $\mathrm{Gal}(L/K)$ mapping to the Frobenius).

If L/K is not abelian, we define

$$\left(\frac{L/K}{\mathfrak{p}}\right) = \left\{ \left(\frac{L/K}{\mathfrak{P}}\right) | \mathfrak{P} \text{ divides } \mathfrak{p} \right\}$$

In other words, since the Artin symbol depends on the prime we choose above $\mathfrak{P}$, we take all of them. By what we saw above, this is a conjugacy class in $\mathrm{Gal}(L/K)$. We will need this more general point of view to state Tchebotarev's theorem.

We can now state the first main theorem of class field theory.

Theorem 4 (Artin Reciprocity Theorem)**.** *Let L/K be an abelian extension of number fields. Then there exists a modulus $\mathfrak{m}$ of K divisible by all ramified primes of K, finite or infinite, such that the Artin map*

$$\left(\frac{L/K}{\bullet}\right) : I_K^{\mathfrak{m}} \longrightarrow \mathit{Gal}(L/K)$$

is surjective. Moreover, the kernel $H^{\mathfrak{m}}$ of this map contains $\iota(K_{\mathfrak{m},1})$. Consequently,

$$\mathit{Gal}(L/K) \simeq I_K^{\mathfrak{m}}/H^{\mathfrak{m}}$$

A ramified infinite prime is a real infinite prime σ of K such that there exists a complex infinite prime τ of L that restricts to σ on K, i.e. $\tau|K = \sigma$. By definition, a complex infinite prime of K cannot ramify in L.

If L/K is an extension of number fields and $\mathfrak{m}$ is a modulus of K, a subgroup $H^{\mathfrak{m}} \subseteq I_K^{\mathfrak{m}}$ containing $\iota(K_{\mathfrak{m},1})$ is called a *congruence subgroup* for $\mathfrak{m}$. These congruence subgroups naturally correspond to the subgroups of the ray class group mod $\mathfrak{m}$. Thus the Artin Recitpocity Theorem states that the Galois group of any abelian extension of K can be realised as a quotient of a ray class group mod $\mathfrak{m}$ for some modulus $\mathfrak{m}$. This theorem is beautiful because it tells us that the abelian extensions of K, which live "outside of K", have something to do with the "internal" structure of K.

A natural question is to ask if a certain converse of this theorem is true. The answer is yes.

Theorem 5 (Existence Theorem)**.** *Let K be a number field, $\mathfrak{m}$ be a modulus of K and $H^{\mathfrak{m}}$ be a congruence subgroup for $\mathfrak{m}$, i.e. $\iota(K_{\mathfrak{m},1}) \subseteq H^{\mathfrak{m}} \subseteq I_K^{\mathfrak{m}}$. Then there exists a unique*

abelian extension L *of* K*, all of whose ramified primes, finite or infinite, divide* $\mathfrak{m}$*, such that the Artin map*

$$\left(\frac{L/K}{\bullet}\right) : I_K^{\mathfrak{m}} \longrightarrow Gal(L/K)$$

has kernel $H^{\mathfrak{m}}$*. Consequently,*

$$Gal(L/K) \simeq I_K^{\mathfrak{m}}/H^{\mathfrak{m}}$$

This Existence Theorem will be the main ingredient in the second step of the proof of Tchebotarev's theorem.

To conclude this section on class field theory, one may ask if the correspondence between abelian extensions of K and congruence subgroups is bijective. The answer is no. The problem is that many congruence subgroups can correspond to a given abelian extension of K, by playing with the exponents of the modulus, for example. This problem can be solved by introducing a certain equivalence relation on the congruence subgroups. Then the abelian extensions correspond in a bijective way to these equivalence classes. To learn more about this, a good reference is [Jan], Chapter V, section 6.

6. Dirichlet's theorem revisited again

In this section, we will reinterpret Dirichlet's theorem in the language of Galois groups of abelian extensions, using class field theory. We introduce some notation. Let L/K be an abelian extension with Galois group G and let σ be any automorphism in G. Then we define

$$\mathcal{P}_{L/K}(\sigma) = \left\{ \mathfrak{p} \text{ unramified prime of } K \,\middle|\, \left(\frac{L/K}{\mathfrak{p}}\right) = \sigma \right\}$$

We can now restate Dirichlet's theorem in terms of Galois groups.

Theorem 6. *Using the same notation as above, we have*

$$\delta(\mathcal{P}_{L/K}(\sigma)) = \frac{1}{|G|} = \frac{1}{[L:K]}$$

Proof. By the Existence Theorem, there exists a modulus $\mathfrak{m}$ of K and a congruence subgroup $H^{\mathfrak{m}}$ for $\mathfrak{m}$ such that the Artin map induces an isomorphism $I_K^{\mathfrak{m}}/H^{\mathfrak{m}} \simeq G$. Since excluding a finite number of primes does not affect the density, we may suppose that no prime of $\mathcal{P}_{L/K}(\sigma)$ divides $\mathfrak{m}_0$. Let $\overline{H}^{\mathfrak{m}}$ denote the image of $H^{\mathfrak{m}}$ in $C_{\mathfrak{m}}$, that is $\overline{H}^{\mathfrak{m}} = H^{\mathfrak{m}}/\iota(K_{\mathfrak{m},1})$. Then one sees that

$$\mathcal{P}_{L/K}(\sigma) = \left\{ \mathfrak{p} \text{ unramified prime of } K \,\middle|\, \mathfrak{p} \nmid \mathfrak{m}_0, \mathfrak{p} \in \mathfrak{a}\overline{H}^{\mathfrak{m}} \right\}$$

for a certain class $\mathfrak{a}$ in $C_{\mathfrak{m}}$ (we used the isomorphism $I_K^{\mathfrak{m}}/H^{\mathfrak{m}} \simeq G$ and $I_K^{\mathfrak{m}}/H^{\mathfrak{m}} \simeq C_{\mathfrak{m}}/\overline{H}^{\mathfrak{m}}$). Now $\overline{H}^{\mathfrak{m}}$ is itself a union of classes of $C_{\mathfrak{m}}$, say $\overline{H}^{\mathfrak{m}} = \{\mathfrak{h}_1, \ldots, \mathfrak{h}_n\}$, where $n = (H^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1}))$. We can now use Dirichlet's theorem 3 to say that $\delta(\mathcal{P}(\mathfrak{h}_i)) = 1/|C_{\mathfrak{m}}|$ for all i. Since $\mathcal{P}_{L/K}(\sigma) = \mathcal{P}(\mathfrak{h}_1) \cup \cdots \cup \mathcal{P}(\mathfrak{h}_n)$ and $\mathcal{P}(\mathfrak{h}_i) \cap \mathcal{P}(\mathfrak{h}_j) = \emptyset$ for $i \neq j$, we see that

$$\delta(\mathcal{P}_{L/K}(\sigma)) = \delta(\mathcal{P}(\mathfrak{h}_1)) + \cdots + \delta(\mathcal{P}(\mathfrak{h}_n)) = \frac{(H^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1}))}{|C_{\mathfrak{m}}|} = \frac{(H^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1}))}{(I_K^{\mathfrak{m}} : \iota(K_{\mathfrak{m},1}))} = \frac{1}{|G|}$$

□

This theorem is in fact the abelian version of Tchebotarev's theorem.

7. Proof of Tchebotarev's theorem

We are finally ready to prove the main theorem of the notes. Before, we introduce a bit more notation. As we said above, if L/K is a non-abelian Galois extension of number fields and $\mathfrak{p}$ is a prime of K, then $\left(\frac{L/K}{\mathfrak{p}}\right)$ is a conjugacy class c in $\mathrm{Gal}(L/K)$. In this case, we define

$$\mathcal{P}_{L/K}(c) = \left\{ \mathfrak{p} \text{ unramified prime of } K \,\middle|\, \left(\frac{L/K}{\mathfrak{p}}\right) = c \right\}$$

Note that this definition makes sense for abelian extensions also, since any conjugacy class contains a single element in an abelian group. Therefore $\mathcal{P}_{L/K}(\sigma) = \mathcal{P}_{L/K}(c)$, where $c = \{\sigma\}$ is the conjugacy class of σ. We can now state and prove

Theorem 7 (Tchebotarev's Theorem)**.** *Let L/K be a Galois extension of number fields with Galois group G and let c be a conjugacy class in G. Then*

$$\delta(\mathcal{P}_{L/K}(c)) = \frac{|c|}{|G|}$$

Proof. Choose $\sigma \in c$, so that c is the conjugacy class of σ. Note that we know that the result is true if G is abelian, as in this case $c = \{\sigma\}$ and the result follows from the previous theorem. The idea is to use this information and analyse the decomposition of primes to deduce the general case. Let E be the fixed field of $H = \langle\sigma\rangle \leq G$ in L, so that L/E is a cyclic extension with Galois group H. By the abelian case of the theorem, we know that $\delta(\mathcal{P}_{L/E}(\sigma)) = \frac{1}{|H|}$. Let $\mathcal{S} \subseteq \mathcal{P}_{L/E}(\sigma)$ be the subset of primes of E of relative degree one over K. By the properties of the Dirichlet densities, we know that $\delta(\mathcal{S}) = \delta(\mathcal{P}_{L/E}(\sigma)) = 1/|H|$.

Now note that $\mathcal{P}_{L/K}(c) = \left\{ \mathfrak{p} \text{ prime of } K \,\middle|\, \left(\frac{L/K}{\mathfrak{P}}\right) = \sigma \text{ for some prime } \mathfrak{P} \text{ of } L \text{ lying over } \mathfrak{p} \right\}$. Our goal now is to relate $\mathcal{S}$ to $\mathcal{P}_{L/K}(c)$ and then use this relation to find the density of $\mathcal{P}_{L/K}(c)$. Let $\mathfrak{P}$ be a prime of $\mathcal{S}$ and let $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_K$. We need to know how many primes divisors of $\mathfrak{p}$ in E are in $\mathcal{S}$. Fix a prime $\wp$ of L that divides $\mathfrak{P}$ and recall that $\left(\frac{L/E}{\mathfrak{P}}\right) = \sigma$. If we let $G/H = \{H\tau_1, \ldots, H\tau_{[G:H]}\}$ be a system of coset representatives of H in G, then the $\tau_i(\wp)$ are the distinct prime divisors of $\mathfrak{p}$ in L. To see this, first note that

$$\sigma = \left(\frac{L/E}{\wp}\right) = \left(\frac{L/K}{\wp}\right)^{f(\mathfrak{P}/K)} = \left(\frac{L/K}{\wp}\right)$$

because $\mathfrak{P} \in \mathcal{S}$ implies $f(\mathfrak{P}/K) = 1$ by definition. Then $D_{E/K}(\wp) = \left\langle \left(\frac{L/K}{\wp}\right) \right\rangle = \langle\sigma\rangle = H$, so $f(\wp/K) = |H|$ and $g(\wp/K) = [G : H]$. It follows that the $\tau_i(\wp)$ are all distinct, which proves the claim. This also proves that the $\mathfrak{P}_i = \tau_i(\wp) \cap \mathcal{O}_E$ are the divisors of $\mathfrak{p}$ in E. Now that we found a description of these divisors, we need to know which of these $\mathfrak{P}_i$ have relative degree one over K, i.e. which $\mathfrak{P}_i$ belong to $\mathcal{S}$. We claim that this is the case if and only if $\tau_i^{-1}\sigma\tau_i = \sigma$, i.e. if and only if τ_i belongs to $C_G(\sigma)$, the centralizer of σ in G. To see this, note that

$$|H| = f(\wp/\mathfrak{p}) = f(\wp/\mathfrak{P}_i) f(\mathfrak{P}_i/\mathfrak{p})$$

and

$$D_{L/E}(\tau_i(\wp)) = \{\gamma \in H | \gamma\tau_i(\wp) = \tau_i(\wp)\} = \tau_i^{-1} H \tau_i \cap H$$

The claim now follows directly form the fact that $H = \langle\sigma\rangle$ and $|D_{L/E}(\tau_i(\wp))| = f(\wp/\mathfrak{P}_i)$.

Finally, we can say that there are exactly $|C_G(\sigma)|/|H|$ primes in $\mathcal{S}$ that divide $\mathfrak{p}$. Therefore we have

$$\frac{|C_G(\sigma)|}{|H|}\delta(\mathcal{P}_{L/K}(c)) = \delta(\mathcal{S}) = \frac{1}{|H|}$$

and so

$$\delta(\mathcal{P}_{L/K}(c)) = \frac{1}{|C_G(\sigma)|}$$

It is an easy exercise in group theory to prove that $|C_G(\sigma)| = |G|/|c|$ (just let G act on H by conjugation). This completes the proof. □

8. A FEW APPLICATIONS OF TCHEBOTAREV'S THEOREM

As the reader may guess, Tchebotarev's theorem has a lot of applications. Here we will only give a few results that follow easily from the theorem and that have nice consequences.

Corollary 1. *Let* L/K *be a Galois extension of number fields. Then the density of the primes of* K *that split completely in* L *is* $\frac{1}{[L:K]}$.

Proof. Take the conjugacy class of 1 in $\mathrm{Gal}(L/K)$. By Tchebotarev's theorem

$$\mathcal{P}_{L/K}(1) = \left\{ \mathfrak{p} \text{ unramified prime of } K \;\middle|\; \left(\frac{L/K}{\mathfrak{p}}\right) = 1 \right\}$$

has density $1/[L:K]$. But we know that if $\mathfrak{P}$ divides $\mathfrak{p}$ in L, $\left(\frac{L/K}{\mathfrak{P}}\right)$ has order exactly $f(\mathfrak{P}/\mathfrak{p})$. We deduce that if $\mathfrak{p} \in \mathcal{P}_{L/K}(1)$, then $f(\mathfrak{P}/\mathfrak{p}) = 1$ for any $\mathfrak{P}$ in L dividing $\mathfrak{p}$. □

We can now easily prove the following theorem:

Theorem 8. *Let* L *and* M *be finite Galois extensions of a number fields* K. *Then*

$$L \subseteq M \Leftrightarrow \mathit{Spl}(L/K) \supseteq \mathit{Spl}(M/K)$$

In particular,

$$L = M \Leftrightarrow \mathit{Spl}(L/K) = \mathit{Spl}(M/K)$$

Proof. $\Rightarrow$) Obvious from the properties of the inertial degree.

$\Leftarrow$) First, we claim that

$$\mathrm{Spl}(LM/K) = \mathrm{Spl}(L/K) \cap \mathrm{Spl}(M/K)$$

To see this, first recall that there is a natural injection

$$\mathrm{Gal}(LM/K) \hookrightarrow \mathrm{Gal}(L/K) \times \mathrm{Gal}(M/K)$$

defined as $\sigma \mapsto (\sigma|L, \sigma|M)$. Therefore

$$\begin{aligned}
\mathfrak{p} \in \mathrm{Spl}(LM/K) &\Leftrightarrow \left(\frac{LM/K}{\mathfrak{p}}\right) = 1 \\
&\Leftrightarrow \left(\frac{LM/K}{\mathfrak{p}}\right)|K = 1 \text{ and } \left(\frac{LM/K}{\mathfrak{p}}\right)|L = 1 \\
&\Leftrightarrow \left(\frac{L/K}{\mathfrak{p}}\right) = 1 \text{ and } \left(\frac{M/K}{\mathfrak{p}}\right) = 1 \\
&\Leftrightarrow \mathfrak{p} \in \mathrm{Spl}(L/K) \cap \mathrm{Spl}(M/K)
\end{aligned}$$

Using the hypothesis, we get

$$\mathrm{Spl}(LM/K) = \mathrm{Spl}(M/K)$$

and so by the previous theorem,

$$\frac{1}{[LM : K]} = \frac{1}{[M : K]}$$

which is equivalent to $L \subseteq M$. □

Example 7.

Using the basic properties of quadratic fields, we can see that

$$\mathrm{Spl}(\mathbb{Q}(i)/\mathbb{Q}) = \{p \text{ prime of } \mathbb{Q} | (-1/p) = 1\} = \{p \equiv 1 \pmod 4\}$$

where $(-1/p)$ is the Legendre symbol. Then the theorem above tells us that $\mathbb{Q}(i)$ is uniquely determined, as an extension of $\mathbb{Q}$, by this set $\mathrm{Spl}(\mathbb{Q}(i)/\mathbb{Q})$. In other words, if we find a Galois extension $K/\mathbb{Q}$ such that $\mathrm{Spl}(K/\mathbb{Q})$ is the set of primes congruent to $1 \mod 4$ (up to a finite number of exceptions, since this doesn't affect the density), then $K = \mathbb{Q}(i)$.

This idea that extensions of K are classified in terms of some information coming from K is the basic idea of class field theory. In particular, we see that in order to determine all the possible Galois extensions of K, one has to determine the sets $\mathrm{Spl}(K/\mathbb{Q}) \subseteq \mathbb{Q}$ that can occur. For abelian extensions, class field theory does that. For arbitrary Galois extensions, characterising those sets is still an open question.

REFERENCES

[Cox] COX, D. A., *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts, Wiley, 1989.

[Jan] JANUSZ, G. J., *Algebraic Number Fields*, Advances in the Mathematical Sciences, American Mathematical Society, 1996.

[Mil] MILNE, J. S., *Algebraic Number Theory*, Available at www.jmilne.org/math/, 2012.

[Mil] MILNE, J. S., *Class Field Theory*, Available at www.jmilne.org/math/, 2013.

[Neu] NEUKIRCK, J., *Class Field Theory*, Grundlehren Der Mathematischen Wissenschaften, Springer-Verlag Berlin Heidelberg, 1986.