1 Fundamental concepts

In this section we will present the basic results that will be needed in future sections. We shall start by introducing some terminology so we can conveniently translate arithmetic progressions into modular arithmetic. We will then define what a "Euclidean proof" is in light of the well-known theorems of Euclid and Dirichlet. Also, some basic but relevant properties and definitions related to polynomials will be given. This chapter will conclude with a compendium of Galois and Algebraic Number Theory results, which form the core of the central results in this work.

1.1 Arithmetic progressions

Our main goal is to find a special type of proof of the fact that there exist infinitely many primes in some arithmetic progressions, which are sequences $\{a_n\}_{n=0}^{\infty} \subset \mathbb{R}$, where the nth term is given by the formula

$$a_n = kn + \ell,\ n \geqslant 0, \tag{1.1}$$

for some $k, \ell \in \mathbb{R}$.

Hereafter, unless otherwise specified, we will always assume k and ℓ to be a pair of non-zero positive integers, since we are only interested in integer values of the sequence $\{a_n\}$. Observe that these two integers univocally identify the arithmetic progression $kn + \ell$, $n \geqslant 0$. We may additionally suppose that $k > \ell$.

Remark 1.1. Observe that requiring $0 < \ell < k$ is not restrictive:

- The cases where $k = 0$ or $\ell = 0$ have obviously no interest, since there is no hope to find infinitely many primes in such progressions.
- If k and ℓ are negative, one can multiply by -1 and obtain the same progression, with positive terms instead. We consider positive progressions since we are looking for primes of a certain form, which are positive numbers.
- If $k > 0$ and $\ell < 0$, consider the canonical representative $\bar{\ell} := \ell \bmod k$, which will be positive and less than k. Note that the progression $kn + \ell$ will have the same terms as $kn + \bar{\ell}$ for $n \geqslant 1$. This is really just a choice of writing: if, say, $k = 5$ and $\ell = -3$, the progression $5n - 3$ has the same terms as $5n + 2$ (except for the first one). Therefore, in this thesis we choose to write our progressions in the latter form.
- If $k < 0$ and $\ell > 0$, consider the progression $-kn - \ell$, which will have the same terms (but positive) and apply the previous point since now $k > 0$ and $\ell < 0$.
- Finally, if $k, \ell > 0$ but $k < \ell$, consider again the progression $kn + \bar{\ell}$ and note that $kn + \ell$ and $kn + \bar{\ell}$ will have the same terms for $n \geqslant 1$.

Observe that, fixed k and ℓ, every term a_n in the sequence defined by Eq. (1.1) satisfies

$$a_n \equiv \ell \pmod{k},\ n \geqslant 0.$$

Therefore, any prime p we may find in the sequence $\{a_n\}$ will also satisfy $p \equiv \ell \pmod{k}$. Since the integers k and ℓ univocally define the arithmetic progression $a_n = kn + \ell$, we

will be interested in finding certain proofs of the infinitude of primes (in the arithmetic progression) $\equiv \ell \pmod{k}$ or, equivalently, proofs of the existence of infinitely many primes in the congruence class $\ell \bmod k$[1].

1.2 The Theorems of Euclid and Dirichlet

Euclid's theorem of the infinitude of primes [**Euclid**] plays a pivotal role in this thesis, as we are trying to mimic his proof and extend it to more cases. We should therefore state his Theorem and its proof.

Theorem 1.2 (Euclid). *There are infinitely many prime numbers.*

Proof. Suppose there are finitely many primes, say $p_1, p_2, \ldots, p_m$. Our goal is to show that there exists yet another prime not in our list to reach a contradiction. Thus, consider $Q := p_1 p_2 \cdots p_m + 1$. This number has at least one prime divisor, p, since $Q > 1$. If p was one of the p_i for $1 \leqslant i \leqslant m$, then p would divide $p_1 p_2 \cdots p_m$. Since p also divides Q, we deduce that p divides $Q - p_1 p_2 \cdots p_m = 1$, so p must equal 1, a contradiction (1 is not a prime). Therefore, p is a prime, and it cannot be in our list, which is a contradiction again. □

We are now interested in extending this model of proof to primes of a certain form. In particular, to primes that are $\equiv \ell \pmod{k}$. In other words, we want to prove *à la Euclid* that there exist infinitely many primes of the form $kn + \ell$, $n \geqslant 0$.

It is immediate to check that we need to impose some conditions over k and ℓ to have some possibility of success. For example, if $\gcd(k, \ell) = d > 1$, then $k = dk'$ and $\ell = d\ell'$, for some $k', \ell' \in \mathbb{Z}$. Suppose that p is a prime satisfying $p \equiv \ell \pmod{k}$. Then, $p \equiv \ell \pmod{d}$, but since d also divides ℓ, then $p \equiv 0 \pmod{d}$. Thus, d divides p, which necessarily means that $p = d$. Therefore, there is only one prime (if any) in the arithmetic progression $\equiv \ell \pmod{k}$ if $\gcd(k, \ell) > 1$. Imposing an extra constraint makes all the difference:

Theorem 1.3 (Dirichlet). *Suppose that k and ℓ are two fixed, non-zero integers. If $\gcd(k, \ell) = 1$, there exist infinitely many primes in the congruence class $\ell \bmod k$.*

As we said in the introduction, the proof of this theorem was first given by Dirichlet in terms of L-functions. Although some other proofs that minimize the prerequisites are available [**Selberg**; **ShapiroI**; **ShapiroII**], proving this theorem is still far from straightforward. Therefore, we shall not give the proof here, but [**Dirichlet**] is a good reference for it.

Remark 1.4. An even stronger result asserts that the density of primes in the congruence class $\ell \bmod k$ exists and equals $1/\varphi(k)$ (see [**StrongDirichlet**]), where φ is Euler's totient function (this function counts the number of positive integers less than k relatively prime to k). In this thesis, Dirichlet's Theorem will only refer to Theorem 1.3, not to the stronger assertion about the density of such primes.

Thanks to Dirichlet's Theorem 1.3 we must look for infinitely many primes in arithmetic progressions that satisfy $\gcd(k, \ell) = 1$, which sets an extra condition over k and ℓ. From

[1] If the context is clear, we will refer to the congruence class $\ell \bmod k$ as simply ℓ.

now on, we will always assume this condition to be true. In fact, for every $k > 2$, there are $\varphi(k) > 1$ congruence classes with infinitely many primes[2].

However, not every one of these $\varphi(k)$ progressions admits a proof that follows the spirit of Euclid's. In **??** we will establish that the condition $\gcd(k, \ell) = 1$ is not enough to find such proofs, the constraint $\ell^2 \equiv 1 \pmod{k}$ being also required. In fact, this last condition is stronger than the first one, since it implies that ℓ is an invertible element of $\mathbb{Z}/k\mathbb{Z}$, so ℓ belongs to $(\mathbb{Z}/k\mathbb{Z})^\times$, and thus $\gcd(k, \ell) = 1$.

Proving that a Euclidean proof can be found if and only if $\ell^2 \equiv 1 \pmod{k}$ will be the main technical achievement of this thesis. The progressions that satisfy this will obviously be a subset of those allowed by Dirichlet's Theorem 1.3. For any of this to make sense, however, we must precisely define what we mean by "Euclidean proof" of the infinitude of primes $\equiv \ell \pmod{k}$. We will first give an example of a proof that follows Euclid's idea in Theorem 1.2, so the definition we will give later is more natural.

Example 1.5. Suppose there are finitely many primes $\equiv 1 \pmod 3$, say $p_1, p_2, \ldots, p_m$. Our goal is to show that there exists yet another prime $\equiv 1 \pmod 3$ not in our list. For this goal, consider $Q := p_1 p_2 \cdots p_m$ and the polynomial $f(x) := x^2+3$. Now, $f(Q) = Q^2+3$ has at least one prime divisor, p, since it is greater than one. We then have that p divides $Q^2 + 3$.

Observe that $p \neq p_i$, $1 \leqslant i \leqslant m$: if $p = p_i$ for some i, then p would divide Q^2. Since p also divides $Q^2 + 3$, we get that p divides 3, so $p = p_i = 3$, which is a contradiction (3 is not $\equiv 1 \pmod 3$). Therefore, p is a prime not in our list. We just need to show that $p \equiv 1 \pmod 3$ to reach a contradiction and conclude the proof.

If p divides $Q^2 + 3$, then $Q^2 \equiv -3 \pmod p$. By the Legendre symbol, this means that $\left(\frac{-3}{p}\right) = 1$. Since $\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)$, we deduce that $\left(\frac{p}{3}\right) = 1$, which happens if and only if $p \equiv 1 \pmod 3$ (see **??** in **??** in the Appendix). This gives us an infinitude of primes $\equiv 1 \pmod 3$ provided we have one. Since 7 is a prime $\equiv 1 \pmod 3$, the desired result is finally settled.

Observe that in the case of Theorem 1.2 we supposed there are finitely many primes, considered their product, Q, and also implicitly considered the polynomial $f(x) = x + 1$. We then developed a contradiction argument based on the value $f(Q)$. Similarly, for the previous example, we also considered the product Q and used the irreducible polynomial $f(x) = x^2+3$. We then showed that every prime divisor of $f(Q)$ is $\equiv 1 \pmod 3$ and again reached a contradiction. To end the proof, we needed to find one prime $\equiv 1 \pmod 3$.

To construct the proof in the general case, we first define the following concept. Let $f \in \mathbb{Z}[x]$ be a polynomial. We say that a prime number p is a *prime divisor* of f (or simply that p *divides* f) if there exists $m \in \mathbb{Z}$ such that p divides $f(m)$. The set of prime divisors of f is denoted by $\mathrm{Spl}_1(f)$. Now, in the general case, we will see that it is enough to find an irreducible polynomial such that all its prime divisors are $\equiv 1$ or $\ell \pmod k$ (except maybe *finitely* many)[3]. Therefore, we define:

Definition 1.6. The arithmetic progression $\equiv \ell \pmod k$ admits a *Euclidean polynomial* if there exists an irreducible polynomial $f \in \mathbb{Z}[x]$ such that all its prime divisors (except

[2]In the cases $k = 1, 2$ the only congruence class with infinitely many primes is $\ell = 1$.

[3]Observe that the polynomial $f(x) = x^2 + 3$ we considered in the case $\equiv 1 \pmod 3$ satisfies this condition.

for finitely many) are either $\equiv 1$ or $\ell \pmod{k}$, with infinitely many of the latter kind occurring. We may also suppose that f is monic.

We shall then say that there exists a *Euclidean proof* for the arithmetic progression $\equiv \ell \pmod{k}$ if the proof uses a Euclidean polynomial and the shape of its prime divisors to conclude there are infinitely many primes of this type. The procedure to reach this will be fully developed in **??**.

There are other possible and interesting ways of proving specific examples of Dirichlet Theorem that also avoid its complexity and are not necessarily Euclidean. In [**GueronTessler**; **XianzuLin**; **Selberg**; **Mestrovic**] many examples of such proofs can be found. We could call these other proofs *elementary*[4], rather than Euclidean. For instance, in [**Shanks**] infinitely many primes $\equiv 1 \pmod{p^n}$ are found (p is a prime and $n$lies in $\mathbb{N}$), but the scheme of the proof has nothing to do with our Definition 1.6. Instead, it uses the form of the prime divisors of $(2^{mp}-1)/(2^m-1)$ for some integer m.

Although Dirichlet's complexity can be overcome by many elemental methods for specific cases, in this thesis we are looking for a *general*, *elementary* and *Euclidean* method to obtain infinitely many primes $\equiv \ell \pmod{k}$.

1.3 Essential results

Some basic notation should be recalled before tackling the main results that will pave the way for those in **??**. Let $k \geqslant 1$ be a fixed integer. We shall start by remembering that the multiplicative group of units of $\mathbb{Z}/k\mathbb{Z}$ is

$$G := (\mathbb{Z}/k\mathbb{Z})^\times = \{a \in \mathbb{Z}/k\mathbb{Z} : \gcd(k,a) = 1\},$$

and that the number of elements in G equals $\varphi(k)$. Since polynomials are at the core of Euclidean proofs, we will also outline some results and concepts regarding their prime divisors and roots, which will be later on important. The definiton of G enables us to define:

Definition 1.7. The *kth cyclotomic polynomial*, Φ_k, is defined by the formula

$$\Phi_k(x) := \prod_{a \in G} \left(x - e^{\frac{2\pi i a}{k}}\right) = \prod_{a \in G} (x - \zeta^a), \tag{1.2}$$

where we set $\zeta := e^{2\pi i/k}$. Observe that Φ_k is a monic polynomial.

It is obvious from Eq. (1.2) that the roots of Φ_k are all the kth primitive roots of unity and that $\deg(\Phi_k) = \varphi(k)$. Cyclotomic polynomials satisfy the following important relation, which is proved in [**StevenRoman**].

Lemma 1.8. *The following equality of polynomials holds:*

$$\prod_{d|k} \Phi_d(x) = x^k - 1. \tag{1.3}$$

Some results regarding the prime divisors of polynomials can already be established.

[4]By *elementary* we refer to techniques that do not require advanced mathematics such as L-functions, but rather use undergraduate-level results.

Lemma 1.9. *Let $f, r \in \mathbb{Z}[x]$. Then,* $\mathrm{Spl}_1(f \circ r) \subseteq \mathrm{Spl}_1(f)$.

Proof. Let p be a prime such that p belongs to $\mathrm{Spl}_1(f \circ r)$. This implies that there exists $a \in \mathbb{Z}$ such that p divides $f(r(a))$. Since $r(a)$ lies in $\mathbb{Z}$ because r belongs to $\mathbb{Z}[x]$, we have that p divides $f(b)$ with $b := r(a) \in \mathbb{Z}$, so p belongs to $\mathrm{Spl}_1(f)$. □

This enables us to prove the following result.

Proposition 1.10. *If $f \in \mathbb{Z}[x]$ is non-constant, the set* $\mathrm{Spl}_1(f)$ *is infinite.*

Proof. We can suppose that $f(0) = c \neq 0$. If $f(0) = 0$, exchange the polynomial f for $f \circ r$ with a suitable polynomial $r \in \mathbb{Z}[x]$ such that $f(r(0)) \neq 0$. Proving that $f \circ r$ has infinitely many prime divisors will automatically imply that f has infinitely many prime divisors since $\mathrm{Spl}_1(f \circ r) \subseteq \mathrm{Spl}_1(f)$ (see Lemma 1.9).

To begin with, there is obviously at least one prime divisor of f, since the case $f(x) = \pm 1$ only happens for a finite number of integer values of x. Next, suppose f has only a finite number of prime divisors, say $p_1, p_2, \ldots, p_t$, and let $Q := p_1 p_2 \cdots p_t$.

Since $f(0) = c \neq 0$ (changing f for $f \circ r$ if necessary), we have $f(Qx) = g(x)$ for some $g \in \mathbb{Z}[x]$ of the form $1 + c_1 x + c_2 x^2 + \cdots + c_d x^d$ (where $c_i \in \mathbb{Z}$ for every $1 \leqslant i \leqslant d$, and $d = \deg(f)$). Note that Q divides every c_i. This polynomial g must also have at least one prime divisor, say p, for the same reason as before. Therefore, p divides $g(m)$ for some $m \in \mathbb{Z}$, and this implies that p divides $f(Qm)$. Since $m' := Qm$ lies in $\mathbb{Z}$, it follows that p is a prime divisor of f. But p does not divide Q, since p dividing Q would mean that p divides c_i, for every $1 \leqslant i \leqslant d$ (recall that Q divides every c_i). This, together with the fact that p divides $g(m)$, would imply that p divides $g(m) - \sum_{i=1}^{d} c_i m^i = 1$, which means $p = 1$, a contradiction.

Now, p is a prime divisor of f, but p is not any of the primes $p_1, p_2, \ldots, p_t$, since we just proved that p does not divide $p_1 p_2 \cdots p_t = Q$. Thus, we found a new prime divisor of f not in our list, so one concludes that f has infinitely many prime divisors. □

The above proof is a detailed version of that in [**Murty**].

Remark 1.11. In **??** we will prove that every prime divisor of Φ_k is $\equiv 1 \pmod{k}$, except for finitely many, so, from Proposition 1.10, we deduce that Φ_k has infinitely many prime divisors $\equiv 1 \pmod{k}$. There is a result due to Trygve Nagell [**Murty**] that ensures that for any pair of non-constant polynomials f and g in $\mathbb{Z}[x]$, the set $\mathrm{Spl}_1(f) \cap \mathrm{Spl}_1(g)$ is infinite. This tells us that every non-constant polynomial has infinitely many prime divisors $\equiv 1 \pmod{k}$.

The following result also holds.

Proposition 1.12. *Consider a field $\mathbb{F}$. A polynomial $f \in \mathbb{Z}[x]$ has (at least) a double root $\alpha \in \mathbb{F}$ if and only if $f(\alpha) = f'(\alpha) = 0$.*

Proof. We will start with the direct implication. We may write $f(x) = (x - \alpha)^r g(x)$, for some integer $r \geqslant 2$, and some $g \in \mathbb{Z}[x]$ satisfying $g(\alpha) \neq 0$. Now, $f'(x) = r(x - \alpha)^{r-1} g(x) + (x - \alpha)^r g'(x)$, so $f(\alpha) = f'(\alpha) = 0$.

Conversely, if $f(\alpha) = f'(\alpha) = 0$ we may write, using a Taylor expansion around α,

$$f(x) = f(\alpha) + (x-\alpha) f'(\alpha) + (x-\alpha)^2 \frac{f''(\alpha)}{2!} + O\Big((x-\alpha)^3\Big) = (x-\alpha)^2 \frac{f''(\alpha)}{2!} + O\Big((x-\alpha)^3\Big).$$

Thus, $f(x) = (x-\alpha)^r j(x)$ for some $j \in \mathbb{Z}[x]$ and $r \geqslant 2$. Therefore, f has (at least) a double root $\alpha \in \mathbb{F}$. □

Finally, we also need to give an expression for the *discriminant* of a monic polynomial $f \in \mathbb{Z}[x]$, which we denote by $\Delta(f)$. Let $\deg(f) = d$ and let $\{r_1, r_2, \ldots, r_d\} \subset \mathbb{C}$ be the roots of f (not necessarily distinct). Then,

$$\Delta(f) = \prod_{i<j} (r_i - r_j)^2, \quad 1 \leqslant i, j \leqslant d. \tag{1.4}$$

1.4 Some Galois Theory

Galois Theory results will also be needed. Since our definition of Euclidean polynomial requires it to be irreducible (see Definition 1.6), we will find the following theorem particularly useful. The proofs of the next two results can be found in [**GaloisCox**].

Theorem 1.13. *Let F be a field and let $f \in F[x]$ be a separable polynomial. Also let L be the splitting field of f. Then, the group $\mathrm{Gal}(L/F)$ is transitive on the roots of f if and only if f is irreducible over F.*

Consider now an arbitrary tower of field extensions $K/L/F$. Recall that if K/F is Galois, then K/L is automatically a Galois extension. A condition can be given so that L/F is also Galois.

Theorem 1.14. *Let $K/L/F$ be a tower of extensions where K/F is Galois. Suppose L is the fixed field of a subgroup H of $\mathrm{Gal}(K/F)$. Then, L/F is Galois if and only if H is normal on $\mathrm{Gal}(K/F)$.*

There is one particular field which will be relevant in this thesis. Again, fix an integer $k \geqslant 1$ and let ζ be a kth primitive root of unity (from now on, ζ will always denote a root of Φ_k). The field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is called the *kth cyclotomic field*. It is the smallest subfield of $\mathbb{C}$ containing ζ.

This extension is generated by the cyclotomic polynomial Φ_k. Indeed, since the cyclotomic polynomials are irreducible over $\mathbb{Q}$ (see [**GaloisCox**]), we have that the cyclotomic field is generated via $\mathbb{Q}[x]/(\Phi_k)$, so $\mathbb{Q}(\zeta)$ is a finite field extension over $\mathbb{Q}$, with $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg(\Phi_k) = \varphi(k)$.

Now, since every kth root of unity is of the form ζ^j for some $j \in \mathbb{Z}$, it follows that $\mathbb{Q}(\zeta)$ contains every root of Φ_k (see Definition 1.7). Since we are working in characteristic 0, it follows that $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension. The Galois group of this extension can be easily described thanks to the following proposition, proved in [**GaloisCox**].

Proposition 1.15. *The group $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is canonically isomorphic to $(\mathbb{Z}/k\mathbb{Z})^\times$ via sending the morphism $\sigma_a : \zeta \mapsto \zeta^a$ of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ to the residue class $a \bmod k$, for every $a \in (\mathbb{Z}/k\mathbb{Z})^\times$.*

In future sections we will extensively use this canonical isomorphism to identify some subgroup of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ with the corresponding subgroup of $(\mathbb{Z}/k\mathbb{Z})^\times$.

1.5 Some Algebraic Number Theory

As we said in the introduction, Euclidean methods to show that the congruence class $\equiv \ell \pmod{k}$ contains infinitely many primes can only be found when $\ell^2 \equiv 1 \pmod{k}$. This requires proving two implications. Imagine we somehow have a Euclidean polynomial for the congruence class $\equiv \ell \pmod{k}$. In this situation, showing that $\ell^2 \equiv 1 \pmod{k}$ will be the hardest implication to settle. By "hard" we mean that some algebraic number theory will be needed. Therefore, we shall introduce some technical parlance and results, which we will take from Chapter 3 of [**Marcus**].

We say that a field extension K over $\mathbb{Q}$ is a *number field* if $[K : \mathbb{Q}]$ is finite. Now, fix a number field K with $[K : \mathbb{Q}] = n$. The set of all algebraic integers in K is denoted by $\mathcal{O}_K$. That is,

$$\mathcal{O}_K := \{\alpha \in K : \text{ exists a monic polynomial } h \in \mathbb{Z}[x], h \neq 0 \text{ and } h(\alpha) = 0\} \subseteq K.$$

This set is actually a ring, called the *ring of integers* of K. Moreover, $\mathcal{O}_K$ is a Dedekind domain, so every non-zero proper ideal factors uniquely (up to the order of the factors) into a product of prime ideals.

If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$, then the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is called a $\mathbb{Z}$-*power basis* of $\mathcal{O}_K$. In this case, the number field K is called a *monogenic* number field.

If $n = 2$ or K is a cyclotomic field, then $\mathcal{O}_K$ always admits a $\mathbb{Z}$-power basis. However, this is not always the case. There is an example due to Dedekind that shows that such a basis cannot always be found. For this purpose, Dedekind considered the number field $K := \mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^3 - x^2 - 2x - 8$ and showed that K is not monogenic (see page 30 of Dedekind's original article [**Dedekind1878**]).

Now, given a prime p of $\mathbb{Z}$, consider the ideal of $\mathcal{O}_K$ defined by $p\mathcal{O}_K := \{px : x \in \mathcal{O}_K\}$. This ideal is not prime in general, but it breaks down uniquely as a product of prime ideals (up to the order of the factors). Precisely, suppose that the ideal $p\mathcal{O}_K$ factors in $\mathcal{O}_K$ like

$$p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}, \tag{1.5}$$

where every $\mathfrak{p}_i$, $1 \leqslant i \leqslant g$, is a prime ideal of $\mathcal{O}_K$. The number $e_i \in \mathbb{N}$ is called the *ramification index* of $\mathfrak{p}_\mathfrak{i}$ over p. If $e_i > 1$ for any i, we say p is *ramified* in K. If every e_i equals 1, we say p is *unramified* in K. We also say that $\mathfrak{p}_i$ *divides* or *contains*[5] $p\mathcal{O}_K$.

We now have the following situation:

$$\begin{array}{ccccc} K & \supseteq & \mathcal{O}_K & \supseteq & p\mathcal{O}_K \\ | & & | & & | \\ \mathbb{Q} & \supseteq & \mathbb{Z} & \ni & p \end{array}$$

Observe that $\mathfrak{p}_i \cap \mathbb{Z} = p\mathbb{Z}$, since $\mathfrak{p}_i$ contains $p\mathcal{O}_K \supseteq \mathbb{Z}$, so it contains every multiple of p. Now, remember that in Dedekind domains, prime ideals are also maximal ideals. Therefore, for every $1 \leqslant i \leqslant g$, $\mathcal{O}_K/\mathfrak{p}_i$ is a field with characteristic p (for a proof of this fact, again see [**Marcus**]), which is called the *residue field* of $\mathfrak{p}_i$. Since it is a field of characteristic p, it must be isomorphic to $\mathbb{F}_{p^n}$ for some integer $n \geqslant 1$. This integer is

[5] This makes sense since the product of two ideals I and J in a general ring R always satisfies $IJ \subseteq I$ and $IJ \subseteq J$.

called the *inertia degree* of $\mathfrak{p}_i$ over p, and it is denoted by $f_{K/\mathbb{Q}}(\mathfrak{p}_i|p)$ (or simply $f(\mathfrak{p}_i|p)$ or f_i if there is no ambiguity).

Therefore, $f(\mathfrak{p}_i|p) := [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{F}_p]$, and, in view of this, one can define the *absolute norm* of the nonzero ideal $\mathfrak{p}_\mathfrak{i}$ by $\mathrm{N}(\mathfrak{p}_\mathfrak{i}) := p^{f_i}$. In the specific case where $K/\mathbb{Q}$ is a normal extension (thus automatically Galois), we have the following result:

Proposition 1.16. *If $K/\mathbb{Q}$ is a normal extension, then there exists a unique $e \in \mathbb{N}$ such that $p\mathcal{O}_K = \prod_{i=1}^{g} \mathfrak{p}_i^e$, and every inertia degree f_i is the same for $1 \leqslant i \leqslant g$ (we then simply write the inertia degree as f). Moreover, $e \cdot f \cdot g = [K : \mathbb{Q}]$.*

In all, when we express $p\mathcal{O}_K$ as in Eq. (1.5), we refer to the data provided by the ramification indices, the inertia degrees and the natural number g as the "shape" of the factorization of $p\mathcal{O}_K$.

There are some quantities attached to every number field that describe it. One of these quantities is called the *discriminant* of K, and it regulates which primes ramify in K. Let $b_1, \ldots, b_n$ be an integral basis of $\mathcal{O}_K$, and let $\{\sigma_1, \ldots, \sigma_n\}$ be the set of injective ring homomorphisms from K to $\mathbb{C}$. The *discriminant* of a number field K, $\Delta(K)$, is defined by $\Delta(K) := (\det(\sigma_i(b_j)_{i,j}))^2$, for $1 \leqslant i, j \leqslant n$.

The notion of discriminant can be extended to $\mathcal{O}_K$. In this case, $\Delta(\mathcal{O}_K)$ is defined to be the discriminant of K. Also, if $K = \mathbb{Q}(\alpha)$ for some α in $\mathcal{O}_K$, and we let h denote the minimal polynomial of α, we then have that $\Delta(\mathbb{Z}[\alpha])$ coincides with the discriminant of h. If K is monogenic with $\mathcal{O}_K = \mathbb{Z}[\beta]$ for some $\beta \in \mathcal{O}_K$, then $\Delta(K)$ also coincides with the discriminant of the minimal polynomial of β.

Remark. We have so far worked with field extensions over $\mathbb{Q}$. The same results hold for *relative extensions* over a fixed, arbitrary number field. This requires replacing $\mathbb{Q}$ with a number field F and $\mathbb{Z}$ with $\mathcal{O}_F$. Also, p would now be a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$.

In the same lines, one can also define the *relative discriminant* of an extension K/F, which is denoted by $\Delta(K/F)$. It is an ideal of $\mathcal{O}_F$ and controls what primes of F ramify in K.

We will now learn that the shape of $p\mathcal{O}_K$ can be studied via the factorization of a certain polynomial. Suppose a monic polynomial $\overline{h} \in \mathbb{F}_p[x]$ factors into monic irreducible factors $\overline{h_i} \in \mathbb{F}_p[x]$ like

$$\overline{h} = \overline{h_1}^{e_1} \overline{h_2}^{e_2} \cdots \overline{h_g}^{e_g},$$

for some natural numbers g and e_i. We also refer to the quantity g, the exponents e_i and the degrees of each $\overline{h_i}$ as the "shape" of the factorization of the polynomial $\overline{h}$ in $\mathbb{F}_p[x]$. There exists a criterion by Dedekind that allows to work out the shape of the factorization of $p\mathcal{O}_K$ via the shape of the factorization in $\mathbb{F}_p[x]$ of a certain polynomial with integer coefficients. The criterion holds for all but finitely many primes, and is proved in detail in [**Marcus**]. It reads:

Theorem 1.17 (Dedekind Criterion). *Let α belong to $\mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$. Let $h \in \mathbb{Z}[x]$ be the minimal polynomial of α over $\mathbb{Q}$. Also, let p be a prime not dividing $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, and let $\overline{h}$ be the reduction of $h \bmod p$. Then, there exists an integer $g \geqslant 1$, some prime ideals $\mathfrak{p}_i \subseteq \mathcal{O}_K$ and some ramification indices e_i such that*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_g^{e_g} \quad \textit{if and only if} \quad h \equiv \overline{h_1}^{e_1} \overline{h_2}^{e_2} \cdots \overline{h_g}^{e_g} \pmod{p},$$

where every $\overline{h_i}$ is a distinct monic irreducible factor of h in $\mathbb{F}_p[x]$. Moreover, there is an isomorphism of residue fields $\mathbb{F}_p[x]/\overline{h_i} \cong \mathcal{O}_K/\mathfrak{p}_i$ defined by sending $x \mapsto \alpha \pmod{\mathfrak{p}_i}$, for every $1 \leqslant i \leqslant g$.

The above theorem tells us that $f(\mathfrak{p}_i|p) = \deg(\overline{h_i})$, and that there is a bijection between every prime ideal $\mathfrak{p}_i$ and each irreducible factor $\overline{h_i}$ such that $\mathrm{N}(\mathfrak{p}_\mathfrak{i}) = p^{\deg(\overline{h_i})}$. Moreover, since $\Delta(\mathbb{Z}[\alpha]) = \Delta(h) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]^2\Delta(\mathcal{O}_K)$ holds, it is enough to check that p^2 does not divide $\Delta(h)$ for Dedekind Criterion to work for p. The following result can be deduced from the previous theorem.

Corollary 1.18. *Consider the field extension K/F. A prime ideal $\mathfrak{p}$ of F ramifies in K if and only if $\mathfrak{p}$ divides $\Delta(K/F)$.*

Remark 1.19. Since $\Delta(K/F) \neq 0$, only finitely many prime ideals of F ramify in K.

For the following two results we temporarily write the kth cyclotomic field as $\mathbb{Q}(\zeta_k)$, and we let p be a prime and n a positive integer. The proof of the upcoming two results can be found in [**Washington**].

Proposition 1.20. *The discriminant of the number field $\mathbb{Q}(\zeta_{p^n})$ is $\pm p^{p^{n-1}(pn-n-1)}$, where the sign is negative if $p = 2$ and $n = 2$ or if $p \equiv 3 \pmod 4$. The sign is otherwise positive.*

For the next result, first observe that $\Delta(\Phi_k) = \Delta(\mathbb{Q}(\zeta_k))$, because $\mathbb{Q}(\zeta_k)$ is monogenic since its ring of integers is $\mathbb{Z}[\zeta_k]$.

Proposition 1.21. *If p divides $\Delta(\Phi_k)$, then p also divides k.*

Proof. A prime number p divides $\Delta(\Phi_k) = \Delta(\mathbb{Q}(\zeta_k))$ if and only if p ramifies in $\mathbb{Q}(\zeta_k)$ (see Corollary 1.18). Thus, we are reduced to prove that the fact that p ramifies in $\mathbb{Q}(\zeta_k)$ implies that p divides k. Equivalently, we will show that if p does not divide k, then p does not ramify in $\mathbb{Q}(\zeta_k)$.

Set $k = \prod_i q_i^{n_i}$, for some primes q_i and some integer exponents $n_i > 0$ and note that $\mathbb{Q}(\zeta_k)$ is the compositum of the fields $\mathbb{Q}(\zeta_{q_i^{n_i}})$. Suppose p does not divide k, so $p \neq q_i$ for every i. Then p is unramified in each $\mathbb{Q}(\zeta_{q_i^{n_i}})$, since p does not divide the discriminant of $\mathbb{Q}(\zeta_{q_i^{n_i}})$ (see Proposition 1.20). Therefore, p does not ramify in the compositum, which is $\mathbb{Q}(\zeta_k)$. □

If $p \neq 2$, then the converse of the previous proposition is also true: if p divides k, then $\mathbb{Q}(\zeta_p) \subseteq \mathbb{Q}(\zeta_k)$. Since $p \neq 2$, p ramifies in $\mathbb{Q}(\zeta_p) \supsetneq \mathbb{Q}$ (because it divides $\Delta(\mathbb{Q}(\zeta_p))$), so we deduce that p ramifies in $\mathbb{Q}(\zeta_k)$. Thus, p divides $\Delta(\mathbb{Q}(\zeta_k)) = \Delta(\Phi_k)$. However, if we take $p = 2$ and $k = 6$, then p divides k, but p does not divide $\Delta(\Phi_6) = -3$.

1.6 Notation for Murty Theorem

With the definitions and results we have given so far we can introduce some notation that will easen the proof of Murty Theorem [**Murty**]. The notation we follow here is due to Keith Conrad, who gives a detailed version of Murty's theorem in [**Conrad**].

Let $h \in \mathbb{Z}[x]$ be a monic polynomial and let p be a prime divisor of h. Recall that in Section 1.2 we set

$$\mathrm{Spl}_1(h) := \{p : p \text{ is a prime divisor of } h\} = \{p : h \bmod p \text{ has a linear factor in } \mathbb{Z}/p\mathbb{Z}[x]\}.$$

Giving a rule to determine which primes belong to $\mathrm{Spl}_1(h)$ is the so-called "reciprocity problem", and any possible answer to it is a "reciprocity law". A helpful reference regarding this topic is [**Chebotarev2**].

These reciprocity laws exist for generating polynomials of quadratic extensions and cyclotomic extensions. For example, the well-known *Quadratic Reciprocity Law* (see **??** in **??** in the Appendix) determines when an irreducible monic polynomial $h(x) = x^2 + b$ with b in $\mathbb{Z}$ splits into linear factors when reduced mod p. That is, this law determines $\mathrm{Spl}_1(h)$ when $\deg(h) = 2$. For example, the QRL enables us to give an easy description of the set $\mathrm{Spl}_1(\Phi_4) = \mathrm{Spl}_1(x^2 + 1)$. Indeed, let p be a prime divisor of Φ_4, so $n^2 + 1 \equiv 0 \pmod{p}$, for some $n \in \mathbb{Z}$. This tells us that -1 is a quadratic residue mod p, for every prime divisor of Φ_4 different from 2, so $\left(\frac{-1}{p}\right) = 1$ for $p \neq 2$. By the supplemental laws of the QRL (again, see **??**), we deduce that $p \equiv 1 \pmod{4}$, so finally $\mathrm{Spl}_1(\Phi_4) = \{p : p \equiv 1 \pmod{4}\} \cup \{2\}$.

However, $\mathrm{Spl}_1(h)$ for $h(x) = x^5 - x + 1$ has no easy description. Nevertheless, in this thesis —taking advantage of the results that lead to Euclidean proofs— we will give an explicit reciprocity law for a special type of polynomials, which had not been previously considered in the literature. Suppose $L := \mathbb{Q}(\eta)$ for some $\eta \in \mathbb{Q}(\zeta)$ and $[\mathbb{Q}(\zeta) : L] \leqslant 2$. We will effectively give a characterisation of $\mathrm{Spl}_1(h)$, where h is the minimal polynomial of η over $\mathbb{Q}$. In fact, the reciprocity law for the cyclotomic case $[\mathbb{Q}(\zeta) : L] = 1$ is already known [**Chebotarev2**].

Now fix an arbitrary number field K over $\mathbb{Q}$. Similarly to the set $\mathrm{Spl}_1(h)$, one may define the set $\mathrm{Spl}_1(K)$ as

$$\mathrm{Spl}_1(K) := \{p : \text{some } \mathfrak{p} \text{ dividing } p\mathcal{O}_K \text{ in } K \text{ has } f_{K/\mathbb{Q}}(\mathfrak{p}|p) = 1\}.$$

Thus, in the notation of Eq. (1.5), $\mathrm{Spl}_1(K)$ is the set of primes such that the corresponding factorization in prime ideals of $\mathcal{O}_K$ includes a prime ideal $\mathfrak{p}_i$ with $\mathrm{N}(\mathfrak{p}_i) = p$, for some $1 \leqslant i \leqslant g$. As Keith Conrad summarises in [**Conrad**], "p lies in $\mathrm{Spl}_1(h)$ when h has a root mod p, while p lies in $\mathrm{Spl}_1(K)$ when p has a prime ideal factor in K whose residue field is $\mathbb{Z}/p\mathbb{Z}$".

Again, any rule that determines what primes lie in $\mathrm{Spl}_1(K)$ is called a reciprocity law. For instance, $\mathrm{Spl}_1(\mathbb{Q}(i))$ can be easily calculated using Dedekind Criterion (Theorem 1.17) with $\alpha = i$ and $h = \Phi_4$, which is the minimal polynomial of the algebraic element i. Observe that $\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$, so Dedekind Criterion holds for every prime. Thus, to calculate $\mathrm{Spl}_1(\mathbb{Q}(i))$ we need to work out for what primes p the reduction of $\Phi_4(x) = x^2 + 1 \bmod p$ produces a linear factor in $\mathbb{F}_p[x]$ (since the degrees of the irreducible factors correspond to the inertia degrees)[6]. But this will happen exactly when p lies in $\mathrm{Spl}_1(h)$, so finally $\mathrm{Spl}_1(\mathbb{Q}(i)) = \{p : p \equiv 1 \pmod{4}\} \cup \{2\}$.

Following this idea, in this thesis we will also give a characterisation of $\mathrm{Spl}_1(L)$, for L lying below $\mathbb{Q}(\zeta)$ of degree at most 2.

Now that we have a better understanding of the sets $\mathrm{Spl}_1(h)$ and $\mathrm{Spl}_1(K)$, we can introduce two more sets, which will play a crucial role in the proof of Murty's theorem. As usual, fix an integer $k \geqslant 1$. We define

$$S_1(k, h) := \{b \bmod k : p \equiv b \pmod{k} \text{ for infinitely many } p \in \mathrm{Spl}_1(h)\}$$

[6]In fact, since $\mathbb{Q}(i)/\mathbb{Q}$ is Galois, if Φ_4 has a linear factor (mod p), every factor of $\Phi_4 \bmod p$ will be linear.

and

$$S_1(k,K) := \{b \bmod k : p \equiv b \pmod{k} \text{ for infinitely many } p \in \mathrm{Spl}_1(K)\}.$$

Observe that the elements of the above (finite) sets are congruence classes mod k. Moreover, they are subsets of $(\mathbb{Z}/k\mathbb{Z})^\times$, since $\gcd(k,b) = 1$, for otherwise the condition of existing infinitely many primes $\equiv b \pmod{k}$ would not be met.

Remark 1.22. These sets are of particular interest since they give a simple description of Euclidean polynomials. Using again Dedekind Criterion, if h is irreducible over $\mathbb{Q}$, and θ is a root of h, $\mathrm{Spl}_1(h)$ and $\mathrm{Spl}_1(\mathbb{Q}(\theta))$ are the same, except maybe in a finite number of cases arising if $\mathbb{Z}(\theta)$ is not the ring of integers of $\mathbb{Q}(\theta)$. However, $S_1(k,h)$ and $S_1(k,\mathbb{Q}(\theta))$ do coincide without exceptions.

Thus, observing Definition 1.6 and Remark 1.11, a Euclidean polynomial for the progression $\equiv \ell \pmod{k}$ is any monic, irreducible polynomial $h \in \mathbb{Z}[x]$ such that $S_1(k,h) = \{1,\ell\}$ (writing ℓ instead of $\ell \bmod k$). Equivalently, h will be a Euclidean polynomial for the progression $\equiv \ell \pmod{k}$ if, for any root $\theta \in \mathbb{C}$ of h, we have that $S_1(k,\mathbb{Q}(\theta)) = \{1,\ell\}$.

1.7 Chebotarev Density Theorem

The key step to prove Murty's theorem will be Chebotarev Density Theorem. This result is even deeper than Dirichlet Theorem, and it constitutes a cornerstone in modern algebraic number theory. In order to understand its statement, we must first introduce some concepts and results (proved in detail in [**Marcus**]).

Let K and F be number fields, and assume K is an abelian extension. Also assume that K/F is a normal extension of F, so K/F is automatically Galois. Now set $G := \mathrm{Gal}(K/F)$ and let $\mathcal{O}_K$ and $\mathcal{O}_F$ denote the corresponding rings of integers. Also, denote by $\mathrm{Cl}(\sigma) = \{\tau\sigma\tau^{-1} : \tau \in G\}$ the conjugacy class of $\sigma \in G$.

Now, fix a prime $\mathfrak{p}$ of $\mathcal{O}_F$, so that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, for some prime p. For each prime $\mathfrak{q}$ of $\mathcal{O}_K$ lying over[7] $\mathfrak{p}$, we define the following two subgroups of G:

Definition 1.23. The *decomposition group* is defined by:

$$\begin{aligned} D_\mathfrak{q} &:= \{\sigma \in G : \sigma(\mathfrak{q}) = \mathfrak{q}\} \\ &= \{\sigma \in G : \sigma(\alpha) \equiv 0 \pmod{\mathfrak{q}} \text{ if and only if } \alpha \equiv 0 \pmod{\mathfrak{q}}, \forall \alpha \in \mathcal{O}_K\}. \end{aligned}$$

The *inertia group* is defined by:

$$I_\mathfrak{q} := \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{q}}, \forall \alpha \in \mathcal{O}_K\}.$$

From the definition, $I_\mathfrak{q}$ lies in $D_\mathfrak{q}$. In principle, $D_\mathfrak{q}$ and $I_\mathfrak{q}$ depend on $\mathfrak{p}$ and on the choice of $\mathfrak{q}$ lying over $\mathfrak{p}$. If $\mathfrak{q}'$ is another prime ideal of $\mathcal{O}_K$ lying over $\mathfrak{p}$, then $D_\mathfrak{q}$ and $D_{\mathfrak{q}'}$ (resp. $I_\mathfrak{q}$ and $I_{\mathfrak{q}'}$) are conjugate in G via any $\sigma \in G$ sending $\mathfrak{q}$ to $\mathfrak{q}'$. However, since K/F is abelian, every conjugacy class only contains one element, so $D_\mathfrak{q}$ and $I_\mathfrak{q}$ do not depend on the choice of $\mathfrak{q}$[8].

[7] By this we mean any prime ideal $\mathfrak{q} \subseteq \mathcal{O}_K$ such that $\mathfrak{q} \cap \mathcal{O}_F = \mathfrak{p}$.

[8] We will however not drop the subscript for clarity.

Any $\sigma \in G$ is an automorphism of the field K, so $\sigma(\mathcal{O}_K) \subseteq \mathcal{O}_K$. Now, if we additionally suppose that σ lies in $D_\mathfrak{q} \subseteq G$, then σ fixes $\mathfrak{q}$ and hence induces a well-defined automorphism σ^* of the field $\kappa(\mathfrak{q}) := \mathcal{O}_K/\mathfrak{q}$. Indeed, for each $\sigma \in D_\mathfrak{q}$, we define

$$\begin{aligned} \sigma^* : \kappa(\mathfrak{q}) &\longrightarrow \kappa(\mathfrak{q}) \\ [\alpha] &\longmapsto [\sigma(\alpha)] \\ [\alpha + t] &\longmapsto [\sigma(\alpha) + \sigma(t)] = [\sigma(\alpha)] + t \end{aligned}$$

for $\alpha \in \mathcal{O}_K$ and $t \in \mathfrak{q}$. Also write $\kappa(\mathfrak{p}) := \mathcal{O}_F/\mathfrak{p}$. Since σ also fixes $\mathcal{O}_F$ (because σ lies in G), it can be proved that σ^* belongs to $G^* := \mathrm{Gal}(\kappa(\mathfrak{q})/\kappa(\mathfrak{p}))$, so we have a group homomorphism π between $D_\mathfrak{q}$ and G^*. Moreover, this homomorphism is surjective, and its kernel is:

$$\ker(\pi) = \{\sigma \in D_\mathfrak{q} : \sigma^* = \mathrm{id}\} = \{\sigma \in D_\mathfrak{q} : \sigma(\alpha+\mathfrak{q}) = \sigma(\alpha)+\sigma(\mathfrak{q}) = \alpha+\mathfrak{q},\ \forall \alpha \in \mathcal{O}_K\} = I_\mathfrak{q}, \tag{1.6}$$

from which we deduce that $I_\mathfrak{q}$ is a normal subgroup of G. Therefore, we have the following exact[9] sequence in $I_\mathfrak{q}$, $D_\mathfrak{q}$ and G^*:

$$\{1\} \longrightarrow I_\mathfrak{q} \hookrightarrow D_\mathfrak{q} \overset{\pi}{\twoheadrightarrow} G^* \longrightarrow \{1\}.$$

Assume now that $\mathfrak{p}$ is unramified in K (equivalently, $\mathfrak{p}$ does not divide $\Delta(K/F)$ because of Corollary 1.18). One can show that $\mathfrak{p}$ ramifies in K if and only if $I_\mathfrak{q} \neq \{1\}$. Therefore, if $\mathfrak{p}$ is unramified in K, $I_\mathfrak{q}$ is trivial, and we have that π is in fact an isomorphism from Eq. (1.6). Observe that $\kappa(\mathfrak{q})$ is a finite field extension of $\kappa(\mathfrak{p})$ with characteristic p. Therefore, the group G^* is cyclic, with a special generator descending from $D_\mathfrak{q}$:

Definition 1.24. The generator of G^* is denoted by $\mathrm{Frob}_\mathfrak{p}^*$, so $\langle \mathrm{Frob}_\mathfrak{p}^* \rangle = G^*$. If $\mathfrak{p}$ is unramified in K, the automorphism $\pi^{-1}(\mathrm{Frob}_\mathfrak{p}^*) \in D_\mathfrak{q}$ is well-defined, and we call it the *Frobenius automorphism* of $\mathfrak{q}$ over $\mathfrak{p}$ and we denote it by $\mathrm{Frob}_\mathfrak{p}$.

By noting that the finite group G^* is generated by the automorphism $x \mapsto x^{\mathrm{N}(\mathfrak{p})}$, $x \in \kappa(\mathfrak{q})$, one deduces that $\mathrm{Frob}_\mathfrak{p}$ is the unique automorphism of G with the following defining property for every $\alpha \in \mathcal{O}_K$:

$$\mathrm{Frob}_\mathfrak{p}(\alpha) \equiv \alpha^{\mathrm{N}(\mathfrak{p})} \pmod{\mathfrak{q}}.$$

Remark 1.25. In principle, $\mathrm{Frob}_\mathfrak{p}$ would also depend on the prime ideal $\mathfrak{q}$ lying above $\mathfrak{p}$, so we would instead write $\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}}$. In general, if we consider a different $\mathfrak{q}'$ lying above $\mathfrak{p}$, the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}'}$ attached to it would be conjugate to $\mathrm{Frob}_{\mathfrak{p},\mathfrak{q}}$. Therefore, the Frobenius element is not well-defined as an element but rather as a conjugacy class. However, since we chose K/F to be abelian, the conjugacy classes only contain one element and $\mathrm{Frob}_\mathfrak{p}$ is a unique, well-defined element of $D_\mathfrak{q} \subseteq G$, which does not depend on the choice of $\mathfrak{q}$.

Before tackling Chebotarev Density Theorem, we first need to introduce a numerical measure of sets of prime ideals called the *Dirichlet density*.

[9] A sequence of maps $\cdots \to A \xrightarrow{f} B \xrightarrow{g} C \to \cdots$ is *exact* in B if $\mathrm{Im}(f) = \ker(g)$.

A set of prime ideals S in a number field K has *Dirichlet density* $d(S)$ if the limit

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s}}{-\log(s-1)} = d(S) \tag{1.7}$$

exists. If it does not exist, we may always define the *lower Dirichlet density* (resp. *upper Dirichlet density*) using the limit inferior (resp. limit superior).

The Dirichlet density is a finitely additive measure and, from Eq. (1.7), one has that $0 \leqslant d \leqslant 1$. The definition of this density is different from the more usual *natural density*. See **??** in the Appendix to understand where Eq. (1.7) comes from and the relation between the natural and Dirichlet density. To advance towards Chebotarev's theorem, we need the following result.

Lemma 1.26. *Let S be the set of primes $\mathfrak{p}$ lying above some prime p with $f_{F/\mathbb{Q}}(\mathfrak{p}|p) \geqslant 2$. Then, the Dirichlet density $d(S)$ is zero.*

Proof. For $d(S)$ to be zero, it is enough to prove that $\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-s}$ converges (absolutely) at $s = 1$, since $\lim_{s\to 1^+} \log(s-1) = \infty$ (observe Eq. (1.7)). Let $f := f_{F/\mathbb{Q}}(\mathfrak{p}|p) \geqslant 2$, let T be the set of primes arising from $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for $\mathfrak{p} \in S$, and let Π be the set of all primes. Additionally, consider a normal closure M of F, which is a finite and normal extension of $\mathbb{Q}$. The number of prime ideals in the factorization of $p\mathcal{O}_M$ is bounded by some $g \leqslant [M:\mathbb{Q}]/2 < \infty$, for every p (because of Proposition 1.16). Since $\mathrm{N}(\mathfrak{p}) = p^f$, at $s = 1$ we have:

$$\sum_{\mathfrak{p}\in S} \mathrm{N}(\mathfrak{p})^{-1} = \sum_{\mathfrak{p}\in S} p^{-f} \leqslant \sum_{\mathfrak{p}\in S} p^{-2} \leqslant \frac{[M:\mathbb{Q}]}{2} \sum_{p\in\Pi} \frac{1}{p^2} \leqslant \frac{[M:\mathbb{Q}]}{2} \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty.$$

□

Remark 1.27. This tells us that the set of primes $\mathfrak{p}$ lying above a certain prime p with $f_{F/\mathbb{Q}}(\mathfrak{p}|p) = 1$ has Dirichlet density equal to one.

The Dirichlet density has the following property.

Lemma 1.28. *Let A be a set with $d(A) = 1$ and let B be a set with $d(B) = \delta > 0$. Then, $d(A \cap B) > 0$.*

Proof. Remember that the inclusion-exclusion principle holds for the Dirichlet density d since it is a finitely additive measure. A direct consequence of this fact is that $d(A \cup B) = d(A) + d(B) - d(A \cap B)$. Now, since always $d(A \cup B) \leqslant 1$, we have that

$$d(A) + d(B) - d(A \cap B) \leqslant 1,$$

which yields $d(A) + d(B) - 1 \leqslant d(A \cap B)$. Since $d(A) + d(B) = 1 + \delta > 1$, then $d(A \cap B) \geqslant d(A) + d(B) - 1 > 1 - 1 = 0$. □

Remark 1.29. From the above result we deduce that $A \cap B$ is infinite, observing Eq. (1.7).

Now that we have the notion of density, it is now natural to ask if a fixed element of G corresponds to a Frobenius automorphism over a prime ideal $\mathfrak{p}$. This question is answered using the Chebotarev Density Theorem, which is formulated in terms of Dirichlet density. In the general case where K/F is not necessarily abelian we have:

Theorem 1.30 (Chebotarev Density Theorem). *Let $C \subset G$ be a fixed conjugacy class. Then, the set*

$$S := \{\mathfrak{p} : \mathfrak{p} \text{ a prime ideal of } F, \mathfrak{p} \text{ unramified in } K,\ \mathrm{Cl}(\mathrm{Frob}_{\mathfrak{p}}) = C\}$$

has Dirichlet density $d(S) = \#C/\#G > 0$, so there exist infinitely many such prime ideals.

The proof of this theorem goes beyond the scope of this thesis, so it will be skipped here, but can be found in [**Chebotarev1**]. If the extension K/F is abelian, then each conjugacy class only contains one element, the automorphism $\mathrm{Frob}_{\mathfrak{p}}$ is well-defined and Theorem 1.30 reads:

Corollary 1.31. *Suppose that K/F is abelian, and fix $\sigma \in G$. Then, the set*

$$S := \{\mathfrak{p} : \mathfrak{p} \text{ a prime ideal of } F, \mathfrak{p} \text{ unramified in } K,\ \mathrm{Frob}_{\mathfrak{p}} = \sigma\}$$

has Dirichlet density $d(S) = 1/\#G > 0$, so there exist infinitely many such prime ideals.