CHEBOTAREV'S DENSITY THEOREM

Matthew Di Meglio

Supervisor: Associate Professor David Harvey

School of Mathematics and Statistics
UNSW Sydney

November 2019

Submitted in partial fulfillment of the requirements of the degree of
Bachelor of Advanced Mathematics with Honours

Acknowledgements

I would like to thank my supervisor, David Harvey, for his guidance and support throughout the course of my honours year. From providing comprehensive and constructive feedback on all of the many drafts of the various sections of this thesis, to meeting with me weekly (and often allowing me to overstay my allocated hour) to help clarify concepts and remove barriers to my progress, David has gone above and beyond his role, and for that, I am very grateful.

My family also deserve many thanks for their love, patience and support throughout the year.

Abstract

In this thesis, we provide a comprehensive introduction to and a detailed proof of *Chebotarev's density theorem* (for extensions of number fields). Our proof is unlike typical modern proofs of Chebotarev's theorem, which assume familiarity with class field theory and, in particular, rely on *Artin reciprocity*. Instead, our proof is closer in spirit to Chebotarev's original proof. We begin by proving that Chebotarev's theorem holds for cyclotomic extensions of number fields, detouring into the realm of analytic number theory with our study of the *Weber L-functions*. We then use a method similar to Chebotarev's field "crossing" technique to deduce the case of Chebotarev's theorem for abelian extensions of number fields from the case for cyclotomic extensions. Finally, Deuring's counting argument allows us to conclude, from the case of Chebotarev's theorem for cyclic (abelian) extensions of number fields, that Chebotarev's theorem does indeed hold in general.

Throughout this work, our aim is to present Chebotarev's theorem in a manner that is more accessible for students than standard treatments of this subject matter. With this goal in mind, we provide motivation, in the form of several concrete examples supported with numerical data, for the study of Chebotarev's theorem — these examples include particular instances of *Dirichlet's theorem on prime numbers in arithmetic progressions* and the *Frobenius density theorem*. Our thorough introduction to the concepts from algebraic and analytic number theory that we use, such as the notion of *Frobenius elements*, serves the same purpose. In addition, and for this same reason, we include more detail in our proofs than is normally provided in the texts that we follow.

Symbols

$\mathbb{Z}^+$	Positive integers
$\mathbb{N}$	Non-negative integers
$\psi\|_S$	Restriction of ψ to S
$\mathbb{L}^H$	Subfield of $\mathbb{L}$ fixed by H
$\varphi(n)$	Euler totient function
χ_1	Trivial character
$\widehat{G}$	Character group of G
$\mathcal{O}_\mathbb{K}$	Ring of integers of $\mathbb{K}$
$N_\mathbb{K}^\mathbb{L}(\alpha)$	Norm of $\alpha \in \mathbb{L}$ relative to $\mathbb{K}$
$N(\mathfrak{a})$	Absolute ideal norm of $\mathfrak{a}$
$\mathrm{disc}(\mathbb{K})$	Discriminant of the number field $\mathbb{K}$
$P(\mathbb{K})$	Non-zero prime ideals of $\mathcal{O}_\mathbb{K}$
$e(\mathfrak{P}\|\mathfrak{p})$	Ramification index of $\mathfrak{P}$ over $\mathfrak{p}$
$f(\mathfrak{P}\|\mathfrak{p})$	Inertial degree of $\mathfrak{P}$ over $\mathfrak{p}$
$\mathbb{F}_\mathfrak{p}$	Residue field $\mathcal{O}_\mathbb{K}/\mathfrak{p}$
$D(\mathfrak{P}\|\mathfrak{p})$	Decomposition group (Definition 2.19)
$I(\mathfrak{P}\|\mathfrak{p})$	Inertia group (Definition 2.22)
$\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$	Frobenius element (Definition 2.25)
$\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right)$	Frobenius class (Definition 2.28)
$\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]$	The single element in $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right)$ when $\mathbb{L}/\mathbb{K}$ is abelian (Remark 2.30)
$\delta(A)$	Dirichlet density of A (Definition 2.34)
$\delta_{\sup}(A)$	Upper Dirichlet density of A (Definition 2.44)
$\delta_{\inf}(A)$	Lower Dirichlet density of A (Definition 2.44)
$\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_\mathfrak{m}$	Artin map (Definition 3.20)
$\mathcal{I}_\mathbb{K}$	Group of fractional ideals of $\mathbb{K}$
$\mathrm{Cl}_\mathbb{K}$	Ideal class group of $\mathbb{K}$
$\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$	Modulus (Definition 3.27)
$\mathcal{I}_\mathbb{K}^\mathfrak{m}$	Group of fractional ideals of $\mathbb{K}$ coprime to $\mathfrak{m}$ (Definition/Proposition 3.28)
$\mathrm{Cl}_\mathbb{K}^\mathfrak{m}$	Ray class group of $\mathbb{K}$ for the modulus $\mathfrak{m}$ (Definition/Proposition 3.28)
$h_\mathbb{K}^\mathfrak{m}$	Ray class number (Proposition 3.36)
$\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_\mathfrak{m}}$	See Corollary 3.39
$L_\mathbb{K}^\mathfrak{m}(s,\chi)$	Weber L-function (Definition/Proposition 4.4)
$\ell_\mathbb{K}^\mathfrak{m}(s,\chi)$	Logarithm of Weber L-function (Definition 4.25)

Contents

Chapter 1

Introduction

In 1837, Peter Gustav Lejeune Dirichlet (1805–1859) presented his paper *Proof of the theorem that any infinite arithmetic progression whose first term and difference are integers without a common factor contains infinitely many primes*[1] [25, 26] to the Akademie der Wissenschaften in Berlin. Using the analytic properties of his L-series, today referred to as *Dirichlet L-series* or *Dirichlet L-functions*, Dirichlet showed that the sum $\sum \frac{1}{p^\sigma}$, taken over the primes p in the arithmetic progression

$$a, a+m, a+2m, \cdots$$

where a and m are coprime, is unbounded as $\sigma \to 1^+$, implying that the sum has infinitely many terms and thus that there are infinitely many such prime numbers [26, p. 421]. This paper is widely recognised as the genesis of analytic number theory — the application of analytic techniques to problems of number theoretic nature.

In November 1880, Ferdinand Georg Frobenius (1849–1917) communicated to Ludwig Stickelberger and Richard Dedekind the results of his paper *On relationships between the prime ideals of an algebraic field and the permutations of its group* [14], which he published in 1896, after Dedekind published his theory of ideals in 1894. In this paper, Frobenius made several contributions to number theory. Given a polynomial with rational coefficients, to each prime number he associated a conjugacy class of the Galois group of this polynomial. Today, we call the conjugacy class associated to a prime number p the *Frobenius class* of p, and the elements of the class *Frobenius elements* or *Frobenius substitutions*. Frobenius conjectured that the density of prime numbers belonging to a given conjugacy class of the Galois group is proportional to the number of elements in the class [14, p. 702]; yet he could only prove the corresponding weaker result for primes belonging to a given *division* (see Remark 2.54) of the Galois group, where the partition of a group into divisions is in general less fine than its partition into conjugacy classes.

Nikolai Grigor'evich Chebotarev[2] (1894–1947) is a Russian mathematician who made his name with his proof of Frobenius' conjecture, a result better known today as *Chebotarev's density theorem*. This result is the main focus of this thesis. First published in 1923 in Russian in the paper *Determining the density of a collection of primes belonging to a given class of permutations* [37], and claimed by Chebotarev

[1] In this thesis, all titles written in italics are translations. See the reference list for the original untranslated titles.

[2] The name Чеботарева will be transliterated from Cyrillic as *Chebotarev* throughout this text. Other transliterations commonly used today include *Chebotarëv* and *Čebotarev*. In the German adaptation of his paper [31], Чеботарева was transliterated as *Tschebotareff*. Chebotarev signed his letters to Hasse with *Tschebotaröw* [12, p. 82].

in his autobiography to have been proved as early as 1922 [12, p. 98], Chebotarev's result became widely known after the German adaptation [31] of his Russian paper was published in volume 95 of the Mathematische Annalen in 1925. The following translated extract from his paper [31, p. 192] indicates that Dirichlet and Frobenius laid the foundations for Chebotarev's work:

> *The notion of density comes from Lejeune-Dirichlet*[1]*, who has proved that the primes are equally distributed among the congruence classes relatively prime to k for any modulus k, i.e. that the density of each prime of this type is equal to $\frac{1}{\varphi(k)}$. The investigations of Kummer link this result to the determination of the density of a set of primes belonging to each of the permutations of a cyclotomic field. [...] Frobenius has determined the density of divisions. By a division he means the collection of all permutations TS^iT^{-1}, where i runs through all of the values not exceeding the order f of S and relatively prime to f. However, he has failed to determine the same for classes of permutations. This is the subject of this study.*

Chebotarev's manuscript was received by the Mathematische Annalen on September 5, 1924. According to Chebotarev, Emmy Noether told him when they met in 1925 that although she had been appointed as referee for his article, she had declined and the job had been passed on to Emil Artin[2] (1898–1962) [12, p. 97].

The *Artin L-functions* (or *Artin L-series*) and *Artin's reciprocity law*, as they are known today, both introduced by Artin in his article *On a new kind of L-series* [4] in 1923, are arguably Artin's two greatest contributions to number theory [27, p. 44]. In a letter to Hasse, dated July 9, 1923, Artin describes his L-series as *general L-series attached to Frobenius group characters which accomplish for general fields exactly what the usual L-series* (Weber's L-series, see Section 4.1) *accomplish for abelian fields*[3]. If $\mathbb{K}$ is a number field and $\mathbb{L}$ is a *ray class field* corresponding to some *ray class group* of $\mathbb{K}$, then Artin's reciprocity law establishes a canonical isomorphism from the ray class group to the Galois group of the extension $\mathbb{L}/\mathbb{K}$ (see Remark 3.37). Artin reciprocity is considered by many to be *the* centerpiece of class field theory [29, p. 35], a branch of mathematics which describes all abelian extensions of a given algebraic number field[4]. In his 1923 paper [4], Artin boldly stated his reciprocity law as a theorem [4, Satz 2, p. 98], and proceeded to explain how his theorem implies that his new L-functions are generalisations of the *ordinary* L-functions (those of Weber, see Section 4.1) and how his theorem coincides with

[1] Here, the German adaptation of Chebotarev's paper cites [24, p. 13] and, for further information, Dirichlet's *Lectures on Number Theory* [10, pp. 342–359]. The page number 13 in the first citation is a miscopy from the the original Russian paper which references pages 307 and 313 — the starting pages of two of Dirichlet's works, originally from 1837, the second being his paper on primes in arithmetic progression. Here Chebotarev is crediting Dirichlet for a notion that we know today as the *Dirichlet density*.

[2] This seems to contradict Artin's remark to Hasse in a letter [12, p. 82] dated February 10, 1926, that he was unable to understand the article.

[3] A full translation of this letter [12, p. 74] and other letters from Artin to Hasse may be found in "Emil Artin and Helmut Hasse: The Correspondence 1923–1958" [12].

[4] Modern formulations are concerned more generally with abelian extensions of local and global fields.

the previously known *general law of reciprocity* in the case of cyclic extensions; after which he admitted that he had as yet no proof of the general result, and thus it could only be taken as true *in those cases in which the general reciprocity law is accessible to us, that is, for fields* $\mathbb{L}$ *of prime degree* (over $\mathbb{K}$) *and the fields composed of them.* Nonetheless, later in the same article [4, Section 7, p. 105], Artin used his as yet unproven reciprocity law, to give a "proof" of Frobenius' conjecture (Chebotarev's density theorem).

Artin took particular interest in Chebotarev's article [31] for its ingenious reduction of the case of Chebotarev's density theorem for abelian extensions to the case for *cyclotomic extensions* (see Definition 3.1) — this involved "crossing"[1] the abelian extension of interest with a cyclotomic extension satisfying certain properties (see Chapter 6), an idea whose origin is perhaps Hilbert's proof of the Kronecker–Weber theorem (1896) [12, p. 127]. Chebotarev's method of "crossing" was, in Artin's own words, the *missing link* needed to prove his reciprocity law [12, p. 125]. Indeed in 1927, within a year and a half of the publication of Chebotarev's article, Artin published another, titled *Proof of the general reciprocity law* [3], in which he used a modification of Chebotarev's "crossing" method, together with ideas from the proof of Dirichlet's theorem on prime numbers in arithmetic progressions, to give a complete proof of reciprocity [12, p. 99].

According to Stevenhagen and Lenstra [29, p. 35]:

> *Chebotarev's technique is still a crucial ingredient of all known proofs of Artin's Reciprocity Law.*

On the other hand, today, Chebotarev's density theorem is typically encountered as a consequence of Artin reciprocity [29, p. 34], within the study of class field theory. Unfortunately, the modern presentation of class field theory (in terms of ideles and adeles) is less accessible than its more elementary formulations (in terms of ideals) at its conception in the early 1900s. It is interesting to note that Chebotarev's proof is independent from these contemporary formulations of class field theory [29, p. 34] (which, at the time, was under rapid development by the likes of Hilbert, Weber and Takagi), even though he was aware of some of its notions and their relevance to his results, such as Weber's *class field* and the *Kronecker–Weber theorem* (see the introduction to Chapter 4).

1.1 This thesis

The aim of this thesis is to present an elementary proof of Chebotarev's theorem for extensions of algebraic number fields, similar in vein to Chebotarev's original proof. We assume the reader is familiar with the basic definitions and results of

- *abstract algebra*: groups, rings and fields;
- *algebraic number theory*: rings of integers, and splitting of prime ideals;
- *Galois theory*: Galois extensions, Galois groups, and field compositums; and
- *complex analysis*: holomorphic and meromorphic functions, poles and residues, and infinite sums and infinite products;

[1] The German word is "Durchkreuzung", introduced by Hasse in Part II of his class field theory report [12, Footnote 20, p. 126].

although no more than would be covered in an introductory textbook or undergraduate course on these subjects.

In Chapter 2, our aim is to understand the statement of Chebotarev's density theorem. We begin with motivation, in the form of several concrete examples supported with numerical data, for the study of Chebotarev's theorem. These examples include particular instances of the already-mentioned theorems of Dirichlet and Frobenius. The notions of *Dirichlet density* from analysis, and of *Frobenius elements* and *Frobenius classes* from algebraic number theory, are central to the statement and proof of Chebotarev's theorem. For this reason, in this chapter we provide a comprehensive introduction to these concepts, including detailed proofs of all stated results.

In Chapters 3 and 4, we prove that Chebotarev's density theorem holds for a cyclotomic extension $\mathbb{L}/\mathbb{K}$ of number fields. If we further assume that the base field $\mathbb{K}$ is the field of rational numbers $\mathbb{Q}$, and indeed Chebotarev's general formulation of his theorem was for extensions of $\mathbb{Q}$ and not arbitrary extensions of number fields, then this case becomes equivalent to Dirichlet's theorem on prime numbers in arithmetic progressions. Our proof proceeds analogously, where Weber's ideal class groups modulo a non-zero ideal $\mathfrak{m}$ of the ring of integers $\mathcal{O}_{\mathbb{K}}$ (today known as the *narrow ray class group* of $\mathbb{K}$ for the modulus $\mathfrak{m}$, see Remark 3.33) are the appropriate generalisation of the congruence classes modulo an integer m, relatively prime to m; and Weber's L-functions are the appropriate generalisation of Dirichlet's L-functions. Although we do not assume any results from class field theory, we will, in the course of our proof of this case of Chebotarev's theorem, essentially prove a part of the cyclotomic case of Artin reciprocity. Here, we omit the proof of a technical result (Theorem 4.17) which gives an asymptotic estimate for the number of ideals of norm at most N in a given ray class as $N \to \infty$, as well as the proof that ray class groups are finite (Proposition 3.36). Such proofs would involve a long diversion in a direction somewhat orthogonal to the rest of this thesis. It is worth noting that, throughout our proof of Chebotarev's density theorem, these are the *only* non-elementary results which we do not prove.

In Chapter 5, we present a reduction, due to Deuring [9], of Chebotarev's density theorem for an arbitrary field extension $\mathbb{L}/\mathbb{K}$ to Chebotarev's density theorem for a certain intermediate cyclic extension $\mathbb{L}/\mathbb{M}$. This reduction has little analytic content — it is largely an application of properties of decomposition groups and Frobenius elements to the construction of a bijection between the sets of prime ideals of interest of $\mathbb{K}$ and $\mathbb{M}$. This reduction is used twice in the overall proof of Chebotarev's theorem — once to reduce the general case of Chebotarev's theorem to the abelian case (cyclic extensions are abelian), and once again in the reduction of the abelian case to the cyclotomic case, where the intermediate field extension $\mathbb{L}/\mathbb{M}$ turns out to be cyclotomic.

In Chapter 6, we present a simplified version of Chebotarev's field "crossing" argument mentioned earlier, thus reducing the abelian case of Chebotarev's theorem to the cyclotomic case, and completing our overall proof of the general result. The proof here, again, is mostly algebraic in nature — a combination of group theory, Galois theory, properties of cyclotomic extensions, and compositums of fields.

1.2 Source material

Our proof of Chebotarev's density theorem, distributed across Chapters 3, 4, 5 and 6, is an elaboration of the proof presented in Section 6.5 of Michael Fried and Moshe Jarden's "Field Arithmetic" [13, pp. 121–128][1]. Tom Apostol's "Introduction to Analytic Number Theory" [2] is a great resource for learning about the general theory of Dirichlet series, and is also the basis of our treatment of the characters of finite abelian groups (Appendix A). Much of the background material on algebraic number fields that we present in Chapter 2 is based on Chapters 3 and 4 of Daniel Marcus' "Number Fields" [28], whose treatment of the Dedekind zeta function and Dirichlet's L-functions in Chapter 7 was also a strong influence on our own treatment of the more general Weber L-functions (Section 4.1). Andrew Sutherland's lecture notes for MIT's graduate course *18.785 - Number Theory I* [30] were an invaluable resource for background knowledge in all aspects of this thesis, with lectures 7, 18, 19, 21 and 22 being particularly helpful. For the history presented in this chapter, the papers by Peter Stevenhagen and Hendrik Lenstra about Chebotarev [29] and Artin [27] were particularly helpful, as was the book "Emil Artin and Helmut Hasse: The Correspondence 1923–1958" [12] which provides commentary on translations of Artin's letters to Hasse. Photocopies of many of the original works referenced in this section [3, 4, 9, 10, 14, 24–26, 31, 37] may be found and downloaded for free from either the Internet Archive [17] or the Biodiversity Heritage Library [7].

[1] In Section 6.4, Fried and Jarden also prove Chebotarev's density theorem for function fields [13, pp. 115–120].

Chapter 2

Background

In this chapter, we aim to understand the following statement of Chebotarev's density theorem.

Theorem 2.1 (Chebotarev's density theorem)**.** *Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of number fields with Galois group G, and let C be a conjugacy class of G. Let*

$$P = \left\{\text{non-zero prime ideals } \mathfrak{p} \text{ of } \mathcal{O}_{\mathbb{K}} \text{ unramified in } \mathcal{O}_{\mathbb{L}} \text{ with } \left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = C\right\}.$$

Then the Dirichlet density $\delta(P)$ of P exists, and satisfies

$$\delta(P) = \frac{|C|}{|G|}.$$

To do so, apart from familiarity with basic concepts from Galois theory and algebraic number theory (summarised in Section 2.1 for the reader's convenience), we will need the notions of the *Frobenius class* (denoted above by the *Artin symbol* $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right)$) and *Dirichlet density*, both of which will be defined later in this chapter, in Section 2.3 and Section 2.2 respectively. For motivation, we provide here two examples of numerical observations, which, although seemingly unrelated, are both implied by Chebotarev's theorem. Later in this thesis, once we have the necessary background knowledge, we will return to explain and generalise these observations.

Example 2.2. It is clear why no prime numbers except 2 end in an even digit, and why no prime numbers except 5 have 5 as their last digit. In the following histogram, we see that approximately the same number of the the remaining prime numbers less than 100 end in each of the remaining possible last digits 1, 3, 7 and 9.

1	11	31	41	61	71		
3	3	13	23	43	53	73	83
7	7	17	37	47	67	97	
9	19	29	59	79	89		

Consider now the larger upper bound 10000. There are 1229 prime numbers less than 10000. Tallying the last digits of these primes (ignoring the special primes 2 and 5), we see in Table 2.1 that each of the final digits 1, 3, 5 and 9 still occurs about a quarter of the time.

In Theorem 3.14, applying Chebotarev's density theorem to a cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$, where ζ_m is a primitive m-th root of unity, we will deduce a stronger version of Dirichlet's theorem on prime numbers in arithmetic progressions than the one stated in Chapter 1. In particular, the equidistribution of primes across the

Table 2.1: Primes less than 10000 (excluding 2 and 5) by last digit.

Digit	Count	Fraction
1	306	24.9%
3	310	25.2%
7	308	25.1%
9	303	24.7%

last digits 1, 3, 7 and 9 may be deduced from Chebotarev's density theorem for the cyclotomic extension $\mathbb{Q}(\zeta_{10})/\mathbb{Q}$, where ζ_{10} is a primitive 10-th root of unity.

Remark 2.3. We would like to be able to write statements like

$$\delta\big(\{3, 13, 23, 43, 53, 73, 83, \ldots\}\big) = \frac{1}{4},$$

where the density $\delta(A)$ of a set of primes A should be a formalisation of the intuitive notion of the "frequency" of the elements of A amongst all prime numbers. In this thesis, we will mainly work with *Dirichlet density*, which we will define in Section 2.3. For now, it is easier to define the stronger notion of *natural density*, which, for a set of prime numbers A, is given by

$$d(A) = \lim_{n\to\infty} \frac{|\{p \in A : \ p \leqslant n\}|}{|\{p \text{ prime} : \ p \leqslant n\}|}.$$

If the natural density of A exists, then it coincides with the Dirichlet density of A.

Example 2.4. Consider the polynomial $f(X) = X^3 - 2$. Given a prime number p, we can reduce the coefficients of f modulo p, producing a polynomial $\overline{f} \in \mathbb{F}_p[X]$. Here, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the finite field of order p. Although f is irreducible in $\mathbb{Z}[X]$, $\overline{f}$ is not necessarily irreducible in $\mathbb{F}_p[X]$. For example, in $\mathbb{F}_5[X]$, $\overline{f}$ has two irreducible factors, namely $X + 2$ and $X^2 + 3X + 4$. The *decomposition type* of f modulo p is the unordered list of the degrees of the factors in the irreducible factorisation of $\overline{f}$ in $\mathbb{F}_p[X]$. For example, the decomposition type of f modulo 5 is $1, 2$. The decomposition types of f mod p for several small primes p are shown in Table 2.2. Tallying the decomposition types of f modulo p for all 1229 of the prime numbers p less than 10000, we see in Table 2.3 that the decomposition type $1, 2$ occurs for approximately half of these prime numbers, the decomposition type 3 occurs for approximately a third of these prime numbers, and the decomposition type $1, 1, 1$ occurs for approximately a sixth of these prime numbers.

It is well known that the Galois group G of the polynomial f over $\mathbb{Q}$ (i.e. the Galois group of $\mathbb{L}/\mathbb{Q}$ where $\mathbb{L}$ is the splitting field of f over $\mathbb{Q}$) is isomorphic, via its action on the roots of f, to the (entire) symmetric group

$$S_3 = \{(1)(2)(3), (1)(23), (2)(13), (3)(12), (123), (132)\}.$$

In general, the Galois group of an irreducible polynomial of degree n over $\mathbb{Q}$ is isomorphic to a *subgroup* of S_n via its action on the roots of the polynomial. The

Table 2.2: Decomposition type of f modulo p for small primes p.

p	Factorisation of $\overline{f}$ in $\mathbb{F}_p[X]$	Decomposition type
2	X^3	$1,1,1$
3	$(X+1)^3$	$1,1,1$
5	$(X+2)(X^2+3X+4)$	$1,2$
7	X^3+5	3
11	$(X+4)(X^2+7X+5)$	$1,2$
13	X^3+11	3
17	$(X+9)(X^2+8X+13)$	$1,2$
19	X^3+17	3
23	$(X+7)(X^2+16X+3)$	$1,2$
29	$(X+3)(X^2+26X+9)$	$1,2$
31	$(X+11)(X+24)(X+27)$	$1,1,1$

Table 2.3: Distribution of decomposition types of f modulo primes $p < 10000$, and of cycle types of elements $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$, compared.

	Primes $p < 10000$		$\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$	
Type	Count	Fraction	Count	Fraction
$1,1,1$	200	16.3%	1	$1/6$
$1,2$	616	50.1%	3	$1/2$
3	413	33.6%	2	$1/3$

cycle type of an element of such a Galois group is the unordered list of the lengths of the cycles in a disjoint cycle decomposition of its permutation action on the roots.

Curiously, G has three elements of cycle type $1,2$, two elements of cycle type 3, and one element of cycle type $1,1,1$, approximately matching the distribution of the primes less than 10000 across the possible decomposition types, as shown in Table 2.3. From the data, one might conjecture that

$$\delta\big(\{p \text{ of decomposition type } 1,2\}\big) = \frac{1}{2} = \frac{|\{\sigma \in G \text{ of cycle type } 1,2\}|}{|G|}$$
$$\delta\big(\{p \text{ of decomposition type } 3\}\big) = \frac{1}{3} = \frac{|\{\sigma \in G \text{ of cycle type } 3\}|}{|G|}$$
$$\delta\big(\{p \text{ of decomposition type } 1,1,1\}\big) = \frac{1}{6} = \frac{|\{\sigma \in G \text{ of cycle type } 1,1,1\}|}{|G|}$$

Later in this chapter, we will see that this is a specific instance of the *Frobenius density theorem* (Theorem 2.49) for the polynomial f. In Proposition 2.51, we will see that the Frobenius classes provide the connection between the decomposition types of f and the cycle types of the elements of G — for most primes p, the decomposition type of f modulo p is the same as the cycle type of all elements in the Frobenius class $\left(\frac{\mathbb{L}/\mathbb{Q}}{p\mathbb{Z}}\right)$ associated to p. It is this connection which will allow us to deduce the Frobenius density theorem from Chebotarev's density theorem.

2.1 Algebraic number theory

In this thesis, it is assumed that the reader is familiar with the basic definitions and results from algebraic number theory. For the convenience of the reader and to introduce our own notation, we summarise here the ones that we will use. Proofs of almost all of these results can be found in Chapters 2 and 3 of Marcus [28].

2.1.1 Algebraic number fields

An *algebraic number field* (or just *number field*) is a subfield $\mathbb{K}$ of $\mathbb{C}$ which is a finite degree extension of the field of rational numbers $\mathbb{Q}$. The *degree* of a field extension $\mathbb{L}/\mathbb{K}$ (this notation means $\mathbb{K} \subseteq \mathbb{L}$) is the dimension of the field $\mathbb{L}$ when considered as a vector space over $\mathbb{K}$, and is denoted $[\mathbb{L} : \mathbb{K}]$.

Let $\mathbb{L}/\mathbb{K}$ be an extension of number fields. The *primitive element theorem* says that we may write $\mathbb{L} = \mathbb{K}(\alpha)$ for some $\alpha \in \mathbb{L}$, where $\mathbb{K}(\alpha)$ denotes the smallest subfield of $\mathbb{C}$ containing both $\mathbb{K}$ and α. The element α is called a *primitive element* for $\mathbb{L}$ over $\mathbb{K}$. Algebraically, the ring $\mathbb{L}$ is isomorphic to the quotient ring $\mathbb{K}[X]/\langle f \rangle$ where $f \in \mathbb{K}[X]$ is the minimal polynomial of α over $\mathbb{K}$, that is, f is the smallest degree polynomial in $\mathbb{K}[X]$ of which α is a root, and such a polynomial is irreducible. If $n = \deg(f)$, that is, n is the degree of the polynomial f, then the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $\mathbb{L}$ as a vector space over $\mathbb{K}$, and thus $[\mathbb{L} : \mathbb{K}] = n$. In particular, taking $\mathbb{K} = \mathbb{Q}$, all number fields are of the form $\mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/\langle f \rangle$.

An *embedding* of a ring R into a ring S is an injective ring homomorphism from R to S. If $\mathbb{L}/\mathbb{K}$ is an extension of number fields, then the number of $\mathbb{K}$-embeddings of $\mathbb{L}$ (embeddings of $\mathbb{L}$ into $\mathbb{C}$ which fix $\mathbb{K}$ pointwise) is $[\mathbb{L} : \mathbb{K}]$. Indeed, writing $\mathbb{L} = \mathbb{K}(\alpha)$ for some primitive element $\alpha \in \mathbb{L}$, each $\mathbb{K}$-embedding of $\mathbb{L}$ is uniquely determined by sending α to one of the $[\mathbb{L} : \mathbb{K}]$ distinct roots of the minimal polynomial of α over $\mathbb{K}$. If $\mathbb{L}/\mathbb{K}$ is a *Galois* extension, that is, the splitting field of an irreducible polynomial in $\mathbb{K}[X]$, then each of the $\mathbb{K}$-embeddings of $\mathbb{L}$ is actually an automorphism of $\mathbb{L}$. Regardless of whether the extension $\mathbb{L}/\mathbb{K}$ is Galois[1], the $\mathbb{K}$-automorphisms of $\mathbb{L}$ form a group under composition called the *Galois group* of the extension $\mathbb{L}/\mathbb{K}$, and denoted $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$.

2.1.2 Rings of integers

An *algebraic integer* is a root (in $\mathbb{C}$) of a monic polynomial with integer coefficients. The set of algebraic integers forms a subring of $\mathbb{C}$. The intersection of this ring with any number field $\mathbb{K}$ is a subring of $\mathbb{K}$ called the *ring of integers* of $\mathbb{K}$, and denoted $\mathcal{O}_\mathbb{K}$. We have that $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$, and in general, a number field $\mathbb{K}$ is the field of fractions of its ring of integers $\mathcal{O}_\mathbb{K}$. If $\mathbb{L}/\mathbb{K}$ is an extension of number fields, then $\mathbb{Z} \subseteq \mathcal{O}_\mathbb{K} \subseteq \mathcal{O}_\mathbb{L}$. The ring $\mathcal{O}_\mathbb{L}$ is the *integral closure* of $\mathcal{O}_\mathbb{K}$ in $\mathbb{L}$ — this means that for each $\alpha \in \mathbb{L}$, we have that $\alpha \in \mathcal{O}_\mathbb{L}$ if and only if α is the root of a monic polynomial in $\mathcal{O}_\mathbb{K}[X]$. If $\beta \in \mathbb{K}$, then there is an integer n such that $n\beta$ is an algebraic integer. Hence, when applying the primitive element theorem to extensions of number fields, we may take the primitive element to be an algebraic integer.

Recall that a *fractional ideal* of $\mathcal{O}_\mathbb{K}$ is an $\mathcal{O}_\mathbb{K}$-submodule $\mathfrak{a}$ of $\mathbb{K}$ such that $\alpha\mathfrak{a} \subseteq \mathcal{O}_\mathbb{K}$ for some nonzero $\alpha \in \mathcal{O}_\mathbb{K}$. Equivalently, $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_\mathbb{K}$ if and only if $\mathfrak{a} = \alpha^{-1}\mathfrak{b}$ for some ideal $\mathfrak{b}$ of $\mathcal{O}_\mathbb{K}$ and some non-zero $\alpha \in \mathcal{O}_\mathbb{K}$. The

[1] Some authors use the notation $\mathrm{Aut}(\mathbb{L}/\mathbb{K})$ for the group of $\mathbb{K}$-automorphisms of $\mathbb{L}$ when the extension $\mathbb{L}/\mathbb{K}$ is not Galois.

non-zero fractional ideals of $\mathcal{O}_\mathbb{K}$ form a group, denoted $\mathcal{I}_\mathbb{K}$. The group operation is multiplication of fractional ideals — if $\mathfrak{a}$ and $\mathfrak{b}$ are fractional ideals, then $\mathfrak{ab}$ is the set of all finite sums whose terms are of the form $\alpha\beta$ where $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{b}$. The identity element is the ideal $\mathcal{O}_\mathbb{K}$. If $\mathfrak{a}$ is a fractional ideal of $\mathcal{O}_\mathbb{K}$, then

$$\mathfrak{a}^{-1} = \{\beta \in \mathbb{K} : \ \beta\mathfrak{a} \subseteq \mathcal{O}_\mathbb{K}\}.$$

Let $P(\mathbb{K})$ denote the set of *non-zero* prime ideals of $\mathcal{O}_\mathbb{K}$. Every non-zero fractional ideal $\mathfrak{a}$ of $\mathcal{O}_\mathbb{K}$ may be written uniquely (up to ordering) as a product of integer powers of non-zero prime ideals, that is,

$$\mathfrak{a} = \prod_{\mathfrak{p} \in P(\mathbb{K})} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$$

for some integers $v_\mathfrak{p}(\mathfrak{a})$ uniquely determined by $\mathfrak{a}$, where only finitely many $v_\mathfrak{p}(\mathfrak{a})$ are non-zero. The integer $v_\mathfrak{p}(\mathfrak{a})$ is called the $\mathfrak{p}$-*adic valuation of* $\mathfrak{a}$. The fractional ideal $\mathfrak{a}$ is an (ordinary) ideal of $\mathcal{O}_\mathbb{K}$ if and only if all of the integers $v_\mathfrak{p}(\mathfrak{a})$ are non-negative.

Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals of $\mathcal{O}_\mathbb{K}$. We say that $\mathfrak{b}$ *divides* $\mathfrak{a}$, and write $\mathfrak{b} \mid \mathfrak{a}$, if there is an (ordinary) ideal $\mathfrak{c}$ of $\mathcal{O}_\mathbb{K}$ such that $\mathfrak{a} = \mathfrak{bc}$. The *greatest common divisor* and *lowest common multiple* are defined respectively by

$$\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b} \qquad \text{and} \qquad \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}.$$

We say that $\mathfrak{a}$ and $\mathfrak{b}$ are *coprime* if $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathcal{O}_\mathbb{K}$. If $\mathfrak{a}$ and $\mathfrak{b}$ are coprime, then $\operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{ab}$. If $\mathfrak{a}$ and $\mathfrak{b}$ are non-zero, then we have

$$\begin{aligned} \mathfrak{d} = \gcd(\mathfrak{a}, \mathfrak{b}) \qquad &\iff \qquad \forall \mathfrak{p} \in P(\mathbb{K}). \qquad v_\mathfrak{p}(\mathfrak{d}) = \min\big(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b})\big), \\ \mathfrak{m} = \operatorname{lcm}(\mathfrak{a}, \mathfrak{b}) \qquad &\iff \qquad \forall \mathfrak{p} \in P(\mathbb{K}). \qquad v_\mathfrak{p}(\mathfrak{m}) = \max\big(v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b})\big). \end{aligned}$$

This means that distinct non-zero prime ideals of $\mathcal{O}_\mathbb{K}$ are coprime.

2.1.3 Norms of elements and ideals

Let $\mathbb{L}/\mathbb{K}$ be an extension of number fields of degree n, and let $\sigma_1, \ldots, \sigma_n$ be the $\mathbb{K}$-embeddings of $\mathbb{L}$. For each $\beta \in \mathbb{L}$, the *relative norm* $N_\mathbb{K}^\mathbb{L}(\beta)$ is defined by

$$N_\mathbb{K}^\mathbb{L}(\beta) = \sigma_1(\beta)\sigma_2(\beta)\cdots\sigma_n(\beta).$$

If $\beta \in \mathbb{L}$, then $N_\mathbb{K}^\mathbb{L}(\beta) \in \mathbb{K}$. If $\beta \in \mathcal{O}_\mathbb{L}$, then $N_\mathbb{K}^\mathbb{L}(\beta) \in \mathcal{O}_\mathbb{K}$. The relative norm is multiplicative. This means that for all β and γ in $\mathbb{L}$ we have

$$N_\mathbb{K}^\mathbb{L}(\beta\gamma) = N_\mathbb{K}^\mathbb{L}(\beta)N_\mathbb{K}^\mathbb{L}(\gamma).$$

If $\mathfrak{a}$ is a non-zero ideal of $\mathcal{O}_\mathbb{K}$, then the *absolute ideal norm* of $\mathfrak{a}$, denoted $N(\mathfrak{a})$, is the size of the quotient ring $\mathcal{O}_\mathbb{K}/\mathfrak{a}$. The absolute ideal norm is multiplicative, that is, $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$ whenever $\mathfrak{a}$ and $\mathfrak{b}$ are non-zero ideals of $\mathcal{O}_\mathbb{K}$. Also, if $\beta \in \mathcal{O}_\mathbb{K}$ is non-zero, then the principal ideal $\langle\beta\rangle$ has norm

$$N(\langle\beta\rangle) = |N_\mathbb{Q}^\mathbb{K}(\beta)|.$$

2.1.4 Splitting of prime ideals

Let $\mathbb{L}/\mathbb{K}$ be an extension of number fields, and let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_\mathbb{K}$. The ideal $\mathfrak{p}\mathcal{O}_\mathbb{L}$ of $\mathcal{O}_\mathbb{L}$ is not necessarily prime. We say that a prime ideal $\mathfrak{P}$ of $\mathcal{O}_\mathbb{L}$ *lies over* $\mathfrak{p}$ (and also that $\mathfrak{p}$ *lies under* $\mathfrak{P}$) if any of the following equivalent statements are true:

- $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}_\mathbb{L}$,
- $\mathfrak{p}\mathcal{O}_\mathbb{L} \subseteq \mathfrak{P}$,
- $\mathfrak{p} \subseteq \mathfrak{P}$,
- $\mathfrak{P} \cap \mathcal{O}_\mathbb{K} = \mathfrak{p}$,
- $\mathfrak{P} \cap \mathbb{K} = \mathfrak{p}$.

Note here that if $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_\mathbb{L}$, then $\mathfrak{P} \cap \mathbb{K}$ is a prime ideal of $\mathcal{O}_\mathbb{K}$. Every non-zero prime ideal of $\mathcal{O}_\mathbb{L}$ lies over exactly one prime ideal of $\mathcal{O}_\mathbb{K}$, and every non-zero prime ideal of $\mathcal{O}_\mathbb{K}$ lies under at least one prime ideal of $\mathcal{O}_\mathbb{L}$.

The *ramification index* $e(\mathfrak{P}|\mathfrak{p})$ of a prime ideal $\mathfrak{P}$ over $\mathfrak{p}$ is given by the $\mathfrak{P}$-adic valuation:

$$e(\mathfrak{P}|\mathfrak{p}) = v_\mathfrak{P}(\mathfrak{p}\mathcal{O}_\mathbb{L}).$$

As $\mathfrak{P}$ lies over $\mathfrak{p}$, clearly $e(\mathfrak{P}|\mathfrak{p}) \geqslant 1$. We say that $\mathfrak{P}$ is *ramified* over $\mathfrak{p}$ if $e(\mathfrak{P}|\mathfrak{p}) > 1$, and otherwise, we say that $\mathfrak{P}$ is *unramified* over $\mathfrak{p}$. If $e(\mathfrak{P}|\mathfrak{p}) = 1$ for all prime ideals $\mathfrak{P}$ of $\mathcal{O}_\mathbb{L}$ lying over $\mathfrak{p}$, then we say that $\mathfrak{p}$ is *unramified* in $\mathcal{O}_\mathbb{L}$.

For each prime ideal $\mathfrak{P}$ of $\mathcal{O}_\mathbb{L}$ above $\mathfrak{p}$, the quotient ring $\mathcal{O}_\mathbb{L}/\mathfrak{P}$ is a finite field, called the *residue field* of $\mathfrak{P}$ and denoted by $\mathbb{F}_\mathfrak{P}$. If $\iota\colon \mathcal{O}_\mathbb{K} \hookrightarrow \mathcal{O}_\mathbb{L}$ is the inclusion map, and $\pi_\mathfrak{P}\colon \mathcal{O}_\mathbb{L} \to \mathbb{F}_\mathfrak{P}$ is the quotient morphism, then $\ker(\pi_\mathfrak{P} \circ \iota) = \mathfrak{P} \cap \mathcal{O}_\mathbb{K} = \mathfrak{p}$. By the first isomorphism theorem, there is a unique map $\bar{\iota}\colon \mathbb{F}_\mathfrak{p} \hookrightarrow \mathbb{F}_\mathfrak{P}$ which satisfies

$$\bar{\iota}(\alpha + \mathfrak{p}) = \alpha + \mathfrak{P} \qquad \forall \alpha \in \mathcal{O}_\mathbb{K},$$

and it is an embedding. The degree of the extension $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$, denoted $f(\mathfrak{P}|\mathfrak{p})$, is called the *inertial degree* of $\mathfrak{P}$ over $\mathfrak{p}$. The inertial degree $f(\mathfrak{P}|\mathfrak{p})$ is finite because $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$ is an extension of finite fields.

The ramification indices and inertial degrees behave nicely in towers, as is shown in the following proposition.

Proposition 2.5 ([28, Chapter 3, Exercise 10])**.** *Let $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ be a tower of number fields. Let $\mathfrak{P}$, $\mathfrak{q}$ and $\mathfrak{p}$ be non-zero prime ideals of $\mathcal{O}_\mathbb{L}$, $\mathcal{O}_\mathbb{M}$ and $\mathcal{O}_\mathbb{K}$ respectively, with $\mathfrak{P}$ lying over $\mathfrak{q}$ and $\mathfrak{q}$ lying over $\mathfrak{p}$. Then*

$$e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{q})e(\mathfrak{q}|\mathfrak{p}),$$
$$f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{q})f(\mathfrak{q}|\mathfrak{p}).$$

Proof. The equation for the ramification indices follows from the uniqueness of the prime ideal factorisation of $\mathfrak{p}\mathcal{O}_\mathbb{L}$ in $\mathcal{O}_\mathbb{L}$. The equation for the inertial degrees is the tower law applied to the tower $\mathbb{F}_\mathfrak{p} \subseteq \mathbb{F}_\mathfrak{q} \subseteq \mathbb{F}_\mathfrak{P}$. □

The ramification indices, inertial degrees and the degree of an extension are related by the following equation.

Proposition 2.6 ([28, Theorem 21]). *Let $\mathbb{L}/\mathbb{K}$ be an extension of number fields, let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_\mathbb{K}$, and let P be the set of prime ideals of $\mathcal{O}_\mathbb{L}$ above $\mathfrak{p}$. Then*

$$[\mathbb{L} : \mathbb{K}] = \sum_{\mathfrak{P} \in P} e(\mathfrak{P}|\mathfrak{p}) f(\mathfrak{P}|\mathfrak{p}).$$

2.1.5 Discriminants and ramified primes

Let $\mathbb{L}$ be a number field of degree n over $\mathbb{Q}$, and let $\sigma_1, \ldots, \sigma_n$ be the $\mathbb{Q}$-embeddings of $\mathbb{L}$. The *discriminant* $\mathrm{disc}_\mathbb{L}(\beta_1, \ldots, \beta_n)$ of an n-tuple $\beta_1, \ldots, \beta_n$ of elements of $\mathbb{L}$ is defined to be the square of the determinant of the matrix whose entry in the i-th row and j-th column is $\sigma_i(\beta_j)$. Swapping two rows or columns of a matrix negates its determinant, so the discriminant is independent of the ordering of the σ_i and the β_j. The tuple $\beta_1, \ldots, \beta_n$ is a $\mathbb{Q}$-basis of $\mathbb{L}$ if and only if $\mathrm{disc}_\mathbb{L}(\beta_1, \ldots, \beta_n) \neq 0$. If $\beta_1, \ldots, \beta_n \in \mathcal{O}_\mathbb{L}$, then $\mathrm{disc}_\mathbb{L}(\beta_1, \ldots, \beta_n) \in \mathbb{Z}$. If $\beta \in \mathbb{L}$, then

$$\mathrm{disc}_\mathbb{L}(1, \beta, \ldots, \beta^{n-1}) = \prod_{1 \leqslant i < j \leqslant n} \big(\sigma_i(\beta) - \sigma_j(\beta)\big)^2 \tag{2.1.1}$$

as this discriminant is the square of a Vandermonde matrix.

The ring $\mathcal{O}_\mathbb{L}$ is a finitely generated free $\mathbb{Z}$-module of rank $[\mathbb{L} : \mathbb{Q}]$. A $\mathbb{Z}$-basis of $\mathcal{O}_\mathbb{L}$ is called an *integral basis* of $\mathcal{O}_\mathbb{L}$. All integral bases of $\mathcal{O}_\mathbb{L}$ are also $\mathbb{Q}$-bases of $\mathbb{L}$. If $\gamma_1, \ldots, \gamma_n$ is an integral basis of $\mathcal{O}_\mathbb{L}$ and $\beta_1, \ldots, \beta_n \in \mathcal{O}_\mathbb{L}$, then there is an $n \times n$ integer matrix A such that $(\beta_1, \ldots, \beta_n) = (\gamma_1, \ldots, \gamma_n)A$, and so

$$\mathrm{disc}_\mathbb{L}(\beta_1, \ldots, \beta_n) = \det(A)^2 \, \mathrm{disc}_\mathbb{L}(\gamma_1, \ldots, \gamma_n). \tag{2.1.2}$$

In particular, if $\gamma_1, \ldots, \gamma_n$ and $\beta_1, \ldots, \beta_n$ are both integral bases of $\mathcal{O}_\mathbb{L}$, then A is invertible, so $\det(A) = \pm 1$, and thus $\mathrm{disc}_\mathbb{L}(\beta_1, \ldots, \beta_n) = \mathrm{disc}_\mathbb{L}(\gamma_1, \ldots, \gamma_n)$. Hence, we may define the *discriminant* of $\mathbb{L}$, denoted $\mathrm{disc}(\mathbb{L})$, by

$$\mathrm{disc}(\mathbb{L}) = \mathrm{disc}_\mathbb{L}(\gamma_1, \ldots, \gamma_n)$$

where $\gamma_1, \ldots, \gamma_n$ is *any* integral basis of $\mathcal{O}_\mathbb{L}$.

The discriminant of a number field $\mathbb{L}$ tells us which prime numbers ramify in $\mathcal{O}_\mathbb{L}$, as is explained in the following proposition.

Proposition 2.7 ([28, Theorem 24 and Theorem 34]). *Let p be a prime number, and let $\mathbb{L}$ be a number field. Then $p\mathbb{Z}$ is ramified in $\mathcal{O}_\mathbb{L}$ if and only if $p \mid \mathrm{disc}(\mathbb{L})$.*

Corollary 2.8 ([28, Corollary 3 to Theorem 24]). *If $\mathbb{L}/\mathbb{K}$ is an extension of number fields, only finitely many non-zero prime ideals of $\mathcal{O}_\mathbb{K}$ are ramified in $\mathcal{O}_\mathbb{L}$.*

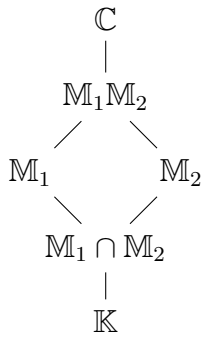
2.1.6 Galois theory of field compositums

Given number fields $\mathbb{M}_1$ and $\mathbb{M}_2$, their *compositum*, denoted $\mathbb{M}_1\mathbb{M}_2$, is the smallest subfield of $\mathbb{C}$ containing both $\mathbb{M}_1$ and $\mathbb{M}_2$. It is the set of all finite sums of products of the form $m_1 m_2$ where $m_1 \in \mathbb{M}_1$ and $m_2 \in \mathbb{M}_2$. We will need the following well-known results from Galois theory about compositums of fields.

Proposition 2.9 ([28, Theorem 56]). *Let $\mathbb{M}_1$ and $\mathbb{M}_2$ be number fields with a common subfield $\mathbb{K}$. If $\mathbb{M}_1/\mathbb{K}$ is Galois, then so is $\mathbb{M}_1\mathbb{M}_2/\mathbb{M}_2$, and the function*

$$\phi\colon \operatorname{Gal}(\mathbb{M}_1\mathbb{M}_2/\mathbb{M}_2) \to \operatorname{Gal}(\mathbb{M}_1/\mathbb{K}), \text{ given by } \sigma \mapsto \sigma|_{\mathbb{M}_1},$$

is an embedding of groups. Also, ϕ is an isomorphism if and only if $\mathbb{M}_1 \cap \mathbb{M}_2 = \mathbb{K}$.



Corollary 2.10. *Let $\mathbb{M}_1$ and $\mathbb{M}_2$ be number fields with a common subfield $\mathbb{K}$, and suppose that $\mathbb{M}_1/\mathbb{K}$ is Galois. Then $\mathbb{M}_1 \cap \mathbb{M}_2 = \mathbb{K}$ if and only if*

$$[\mathbb{M}_1\mathbb{M}_2 : \mathbb{K}] = [\mathbb{M}_1 : \mathbb{K}]\,[\mathbb{M}_2 : \mathbb{K}]\,.$$

Proposition 2.11 ([20, VI, §1, Theorem 1.14]). *Let $\mathbb{M}_1, \mathbb{M}_2$ be number fields which are both Galois over a common subfield $\mathbb{K}$. Then $\mathbb{M}_1\mathbb{M}_2/\mathbb{K}$ is also Galois, and*

$$\phi\colon \operatorname{Gal}(\mathbb{M}_1\mathbb{M}_2/\mathbb{K}) \to \operatorname{Gal}(\mathbb{M}_1/\mathbb{K}) \times \operatorname{Gal}(\mathbb{M}_2/\mathbb{K}), \text{ given by } \sigma \mapsto (\sigma|_{\mathbb{M}_1}, \sigma|_{\mathbb{M}_2}),$$

is an embedding of groups. Also, ϕ is an isomorphism if and only if $\mathbb{M}_1 \cap \mathbb{M}_2 = \mathbb{K}$.

Corollary 2.12. *Using the same notation as Proposition 2.11, if $\mathbb{M}_1/\mathbb{K}$ and $\mathbb{M}_2/\mathbb{K}$ are abelian extensions (i.e. are Galois extensions with abelian Galois groups), then so is $\mathbb{M}_1\mathbb{M}_2/\mathbb{K}$.*

2.2 Decomposition groups and Frobenius elements

Central to the statement and proof of Chebotarev's density theorem is the *Frobenius class* or *Artin symbol* of each unramified non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ in a Galois extension $\mathbb{L}/\mathbb{K}$ of number fields. The aim of this section is to introduce the theory surrounding these concepts. Our treatment is roughly a combination of Chapter 4 of Marcus' "Number Fields" [28] and the lecture notes for Lecture 7 of Andrew Sutherland's MIT graduate course *18.785 - Number Theory I* [30]. As the results that we state here are very important to the rest of the thesis, we provide proofs of all of the results in this section.

2.2.1 Splitting of prime ideals and Galois theory

In this section, we investigate the splitting of prime ideals in *Galois* extensions of number fields.

Lemma 2.13. *Suppose that σ is an automorphism of a number field $\mathbb{L}$. Then the restriction $\sigma|_{\mathcal{O}_{\mathbb{L}}}$ is an automorphism of $\mathcal{O}_{\mathbb{L}}$. Additionally, if σ fixes pointwise a subfield $\mathbb{K}$ of $\mathbb{L}$, then $\sigma|_{\mathcal{O}_{\mathbb{L}}}$ fixes pointwise the subring $\mathcal{O}_{\mathbb{K}}$ of $\mathcal{O}_{\mathbb{L}}$.*

Proof. Let $\beta' \in \sigma(\mathcal{O}_\mathbb{L})$. Then $\beta' = \sigma(\beta)$ for some $\beta \in \mathcal{O}_\mathbb{L}$. As $\mathcal{O}_\mathbb{L}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{L}$, β is the root of a monic polynomial $f \in \mathbb{Z}[X]$. As $\sigma(1) = 1$, and σ is additive, σ fixes $\mathbb{Z}$ pointwise, and thus it fixes the coefficients of f. Hence

$$f\big(\sigma(\beta)\big) = \sigma\big(f(\beta)\big) = \sigma(0) = 0.$$

As $\beta' = \sigma(\beta)$ is a root of the monic polynomial $f \in \mathbb{Z}[X]$, and $\mathcal{O}_\mathbb{L}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{L}$, we have $\beta' \in \mathcal{O}_\mathbb{L}$. So $\sigma(\mathcal{O}_\mathbb{L}) \subseteq \mathcal{O}_\mathbb{L}$. Replacing σ with σ^{-1} in the above argument implies that $\sigma^{-1}(\mathcal{O}_\mathbb{L}) \subseteq \mathcal{O}_\mathbb{L}$, and thus $\mathcal{O}_\mathbb{L} \subseteq \sigma(\mathcal{O}_\mathbb{L})$ because σ is surjective. Hence $\sigma(\mathcal{O}_\mathbb{L}) = \mathcal{O}_\mathbb{L}$, and since σ is injective, this means that it restricts to an automorphism of $\mathcal{O}_\mathbb{L}$. If σ fixes $\mathbb{K}$ pointwise, then $\sigma|_{\mathcal{O}_\mathbb{L}}$ fixes pointwise the elements of $\mathbb{K}$ which are in $\mathcal{O}_\mathbb{L}$, that is, the elements of $\mathcal{O}_\mathbb{K}$. □

Proposition 2.14. *Let $\mathbb{L}/\mathbb{K}$ be an extension of number fields with Galois group G. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_\mathbb{K}$, and let P denote the set of prime ideals $\mathfrak{P}$ of $\mathcal{O}_\mathbb{L}$ lying above $\mathfrak{p}$. Then P is a left G-set with the action given by $\sigma \cdot \mathfrak{P} = \sigma(\mathfrak{P})$ for all $\sigma \in G$ and all $\mathfrak{P} \in P$.*

Proof. We begin by showing that $(-)\cdot(-)\colon G \times P \to P$ does indeed map into P. Let $\sigma \in G$ and $\mathfrak{P} \in P$. By Lemma 2.13, σ restricts to an automorphism of $\mathcal{O}_\mathbb{L}$ which fixes $\mathcal{O}_\mathbb{K}$ pointwise. As all ring isomorphisms send prime ideals to prime ideals, $\sigma(\mathfrak{P})$ is a prime ideal of $\mathcal{O}_\mathbb{L}$. Also, as σ fixes $\mathcal{O}_\mathbb{K}$ pointwise, $\sigma(\mathfrak{p}) = \mathfrak{p}$. As $\mathfrak{P}$ lies above $\mathfrak{p}$, we have $\mathfrak{p} \subseteq \mathfrak{P}$, and so $\mathfrak{p} = \sigma(\mathfrak{p}) \subseteq \sigma(\mathfrak{P})$, which means that $\sigma(\mathfrak{P})$ also lies above $\mathfrak{p}$. Hence $\sigma \cdot \mathfrak{P} = \sigma(\mathfrak{P}) \in P$. The map $(-)\cdot(-)\colon G \times P \to P$ defines a left group action on P because $1_G \cdot \mathfrak{P} = \mathrm{id}(\mathfrak{P}) = \mathfrak{P}$ and $\sigma \cdot (\tau \cdot \mathfrak{P}) = \sigma(\tau(\mathfrak{P})) = (\sigma\tau)\cdot\mathfrak{P}$ for all $\sigma, \tau \in G$ and all $\mathfrak{P} \in P$. □

Proposition 2.15. *Suppose that σ is an automorphism of a number field $\mathbb{L}$, that $\mathfrak{P}$ is a non-zero prime ideal of $\mathcal{O}_\mathbb{L}$, and that $\mathfrak{P}' = \sigma(\mathfrak{P})$. Then there is a unique map $\overline{\sigma}\colon \mathbb{F}_\mathfrak{P} \to \mathbb{F}_{\mathfrak{P}'}$ which satisfies*

$$\overline{\sigma}(\alpha + \mathfrak{P}) = \sigma(\alpha) + \mathfrak{P}' \qquad \forall \alpha \in \mathcal{O}_\mathbb{L},$$

and it is a ring isomorphism. Additionally, if σ fixes a subfield $\mathbb{K}$ of $\mathbb{L}$ pointwise, and $\mathfrak{p}$ is the prime ideal of $\mathcal{O}_\mathbb{K}$ under $\mathfrak{P}$, then $\overline{\sigma}$ fixes $\mathbb{F}_\mathfrak{p}$ pointwise (i.e. with respect to the embeddings $\overline{\iota}_\mathfrak{P}\colon \mathbb{F}_\mathfrak{p} \hookrightarrow \mathbb{F}_\mathfrak{P}$ and $\overline{\iota}_{\mathfrak{P}'}\colon \mathbb{F}_\mathfrak{p} \hookrightarrow \mathbb{F}_{\mathfrak{P}'}$).

Proof. Let $\pi_{\mathfrak{P}'}\colon \mathcal{O}_\mathbb{L} \to \mathbb{F}_{\mathfrak{P}'}$ denote the quotient morphism. As $\sigma|_{\mathcal{O}_\mathbb{L}}$ is an automorphism of $\mathcal{O}_\mathbb{L}$ (Lemma 2.13), and $\pi_{\mathfrak{P}'}$ is surjective, their composition $\pi_{\mathfrak{P}'} \circ \big(\sigma|_{\mathcal{O}_\mathbb{L}}\big)$ is surjective. Also,

$$\ker\Big(\pi_{\mathfrak{P}'} \circ \big(\sigma|_{\mathcal{O}_\mathbb{L}}\big)\Big) = \sigma^{-1}(\mathfrak{P}') = \mathfrak{P}.$$

The existence of the map $\overline{\sigma}$ satisfying the properties in the proposition follows by the first isomorphism theorem.

Suppose now that $\mathbb{K}$ is a subfield of $\mathbb{L}$ which is fixed pointwise by σ, and let $\mathfrak{p}$ be the prime ideal of $\mathcal{O}_\mathbb{K}$ under $\mathfrak{P}$. For all $\beta \in \mathcal{O}_\mathbb{K}$, we have

$$\overline{\sigma}\big(\overline{\iota}_\mathfrak{P}(\beta + \mathfrak{p})\big) = \overline{\sigma}(\beta + \mathfrak{P}) = \sigma(\beta) + \mathfrak{P}' = \beta + \mathfrak{P}' = \overline{\iota}_{\mathfrak{P}'}(\beta + \mathfrak{p}).$$

Hence $\overline{\sigma}$ fixes $\mathbb{F}_\mathfrak{p}$ pointwise with respect to its embeddings into $\mathbb{F}_\mathfrak{P}$ and $\mathbb{F}_{\mathfrak{P}'}$. □

Proposition 2.16. *Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of number fields with Galois group G. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_\mathbb{K}$, and let P denote the set of prime ideals $\mathfrak{P}$ of $\mathcal{O}_\mathbb{L}$ lying above $\mathfrak{p}$. Then the action of G on P is transitive (i.e. it has a single orbit).*

Proof. Assume, for a contradiction, that there are prime ideals $\mathfrak{P}_1$ and $\mathfrak{P}_2$ above $\mathfrak{p}$ such that $\sigma(\mathfrak{P}_1) \neq \mathfrak{P}_2$ for all $\sigma \in G$. Number the remaining elements of P so that $P = \{\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_g\}$ where $g = |P|$. As the ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are pairwise coprime, by the Chinese remainder theorem, there is an $\alpha \in \mathcal{O}_\mathbb{L}$ which simultaneously satisfies the congruence equations

$$\alpha \equiv 0 \,(\mathrm{mod}\, \mathfrak{P}_1), \qquad \alpha \equiv 1 \,(\mathrm{mod}\, \mathfrak{P}_2), \qquad \ldots, \qquad \alpha \equiv 1 \,(\mathrm{mod}\, \mathfrak{P}_g).$$

As $\mathbb{L}/\mathbb{K}$ is Galois, the Galois group G is the set of all $\mathbb{K}$-embeddings of $\mathbb{L}$, and so $N_\mathbb{K}^\mathbb{L}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$. The factors of the product defining $N_\mathbb{K}^\mathbb{L}(\alpha)$ are all in $\mathcal{O}_\mathbb{L}$ because each $\sigma \in G$ restricts to an automorphism of $\mathcal{O}_\mathbb{L}$ and $\alpha \in \mathcal{O}_\mathbb{L}$. As α is one such factor, and α is an element of the ideal $\mathfrak{P}_1$ of $\mathcal{O}_\mathbb{L}$, we must have $N_\mathbb{K}^\mathbb{L}(\alpha) \in \mathfrak{P}_1$. But $N_\mathbb{K}^\mathbb{L}(\alpha) \in \mathcal{O}_\mathbb{K}$, so actually

$$N_\mathbb{K}^\mathbb{L}(\alpha) \in \mathcal{O}_\mathbb{K} \cap \mathfrak{P}_1 = \mathfrak{p} \subseteq \mathfrak{P}_2.$$

Now, let $\sigma \in G$. We know that $\sigma^{-1}(\mathfrak{P}_2)$ is an element of P, and by assumption it is not $\mathfrak{P}_1$, so $\alpha \equiv 1 \,(\mathrm{mod}\, \sigma^{-1}(\mathfrak{P}_2))$. In other words, we have

$$\alpha + \sigma^{-1}(\mathfrak{P}_2) = 1 + \sigma^{-1}(\mathfrak{P}_2),$$

and since σ is an automorphism, we may apply σ to get

$$\sigma(\alpha) + \mathfrak{P}_2 = \sigma(1) + \mathfrak{P}_2 = 1 + \mathfrak{P}_2.$$

So we have $\sigma(\alpha) \equiv 1 \,(\mathrm{mod}\, \mathfrak{P}_2)$, for all $\sigma \in G$. As the factors of the product defining $N_\mathbb{K}^\mathbb{L}(\alpha)$ are all congruent to 1 modulo $\mathfrak{P}_2$, so is $N_\mathbb{K}^\mathbb{L}(\alpha)$ itself. Hence $N_\mathbb{K}^\mathbb{L}(\alpha) \notin \mathfrak{P}_2$, which is a contradiction. □

Corollary 2.17. *Assuming the same notation as Proposition 2.16, the ramification indices $e(\mathfrak{P}|\mathfrak{p})$ and inertial degrees $f(\mathfrak{P}|\mathfrak{p})$ are the same for all $\mathfrak{P} \in P$.*

Proof. See Proposition 8.1 in Chapter II of Lang [23]. □

Proof. Let $\mathfrak{P}_1$ and $\mathfrak{P}_2$ be elements of P. As the action of G on P is transitive (Proposition 2.16), there is a $\sigma \in G$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_2$. By Proposition 2.15, $\mathbb{F}_{\mathfrak{P}_1}$ and $\mathbb{F}_{\mathfrak{P}_2}$ are isomorphic, and thus

$$f(\mathfrak{P}_1|\mathfrak{p}) = [\mathbb{F}_{\mathfrak{P}_1} : \mathbb{F}_\mathfrak{p}] = [\mathbb{F}_{\mathfrak{P}_2} : \mathbb{F}_\mathfrak{p}] = f(\mathfrak{P}_2|\mathfrak{p}).$$

It remains to show that $e(\mathfrak{P}_1|\mathfrak{p}) = e(\mathfrak{P}_2|\mathfrak{p})$. We have the prime ideal factorisation

$$\mathfrak{p}\mathcal{O}_\mathbb{L} = \prod_{\mathfrak{P} \in P} \mathfrak{P}^{e(\mathfrak{P}|\mathfrak{p})}.$$

By Lemma 2.13, σ^{-1} restricts to an automorphism of $\mathcal{O}_\mathbb{L}$ which fixes pointwise $\mathcal{O}_\mathbb{K}$ and thus also $\mathfrak{p}$. Hence

$$\mathfrak{p}\mathcal{O}_\mathbb{L} = \sigma^{-1}(\mathfrak{p})\sigma^{-1}(\mathcal{O}_\mathbb{L}) = \sigma^{-1}(\mathfrak{p}\mathcal{O}_\mathbb{L}) = \prod_{\mathfrak{P}\in P} \sigma^{-1}(\mathfrak{P})^{e(\mathfrak{P}|\mathfrak{p})} = \prod_{\mathfrak{P}\in P} \mathfrak{P}^{e(\sigma(\mathfrak{P})|\mathfrak{p})},$$

where the rightmost equality holds because σ^{-1} permutes the elements of P (Proposition 2.14). By the uniqueness of the prime ideal factorisation of $\mathfrak{p}\mathcal{O}_\mathbb{L}$, it follows that $e(\sigma(\mathfrak{P})|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p})$ for all $\mathfrak{P} \in P$. In particular, this means that

$$e(\mathfrak{P}_2|\mathfrak{p}) = e(\sigma(\mathfrak{P}_1)|\mathfrak{p}) = e(\mathfrak{P}_1|\mathfrak{p}). \qquad \square$$

Remark 2.18. From the corollary, if $\mathbb{L}/\mathbb{K}$ is a Galois extension of number fields, and $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_\mathbb{K}$, then the prime ideal factorisation of $\mathfrak{p}\mathcal{O}_\mathbb{L}$ is

$$\mathfrak{p}\mathcal{O}_\mathbb{L} = (\mathfrak{P}_1 \cdots \mathfrak{P}_{g_\mathfrak{p}})^{e_\mathfrak{p}}$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_{g_\mathfrak{p}}$ are the prime ideals of $\mathcal{O}_\mathbb{L}$ above $\mathfrak{p}$, and they have a common ramification index $e_\mathfrak{p}$ and inertial degree $f_\mathfrak{p}$. By Proposition 2.6, $e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p} = [\mathbb{L} : \mathbb{K}]$.

2.2.2 Decomposition and inertia groups

To construct the *Frobenius element* of a non-zero prime ideal $\mathfrak{P}$ of $\mathcal{O}_\mathbb{L}$ in a Galois extension of number fields $\mathbb{L}/\mathbb{K}$, we need to define the decomposition and inertia groups of $\mathfrak{P}$ over $\mathfrak{p}$, and understand how they are related to the Galois group $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ of the residue field extension, where $\mathfrak{p}$ is the prime ideal of $\mathcal{O}_\mathbb{K}$ under $\mathfrak{P}$.

Definition/Proposition 2.19 (Decomposition group)**.** Let $\mathbb{L}/\mathbb{K}$ be an extension of number fields with Galois group G, and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_\mathbb{L}$ lying above the non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_\mathbb{K}$. Then the set

$$D(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G : \ \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

is a subgroup of G, called the *decomposition group* of $\mathfrak{P}$ over $\mathfrak{p}$. If $\mathbb{L}/\mathbb{K}$ is Galois, then $|D(\mathfrak{P}|\mathfrak{p})| = e_\mathfrak{p} f_\mathfrak{p}$.

As we will use the *orbit-stabiliser theorem* several times throughout this thesis, including to compute the order of $D(\mathfrak{P}|\mathfrak{p})$ in the proof of the above proposition, we recall its statement here for the reader's convenience.

Theorem 2.20 (Orbit-stabiliser theorem)**.** *Let G be a group, and let S be a left G-set. Let $s \in S$, let H be the stabiliser of s in G, and let $G \cdot s$ denote the orbit of s in G. Then the map $\psi \colon G \cdot s \to G/H$, given by $g \cdot s \mapsto gH$ for all $g \in G$, is a G-set isomorphism. In particular, if $G \cdot s$ is finite, then $|G \cdot s| = [G : H]$.*

Proof. See Proposition 8.1 of Chapter II in Lang [23]. $\square$

Proof of Definition/Proposition 2.19. Let P be the set of prime ideals of $\mathcal{O}_\mathbb{L}$ above $\mathfrak{p}$. Then $D(\mathfrak{P}|\mathfrak{p})$ is the stabiliser of $\mathfrak{P}$ under the action of G on P, so it is a subgroup

of G. If $\mathbb{L}/\mathbb{K}$ is Galois, then P is the orbit of $\mathfrak{P}$ under this action (Proposition 2.16), so by the orbit-stabiliser theorem (Theorem 2.20) and Remark 2.18,

$$|D(\mathfrak{P}|\mathfrak{p})| = \frac{|G|}{|P|} = \frac{e_\mathfrak{p} f_\mathfrak{p} g_\mathfrak{p}}{g_\mathfrak{p}} = e_\mathfrak{p} f_\mathfrak{p}. \qquad \square$$

Let $\mathbb{L}$ be a number field and let $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}_\mathbb{L}$. In Proposition 2.15, we constructed a map $\sigma \mapsto \overline{\sigma}$, from the group of automorphisms of $\mathbb{L}$ which fix $\mathfrak{P}$, to the group of automorphisms of $\mathbb{F}_\mathfrak{P}$. Here, $\overline{\sigma}\colon \mathbb{F}_\mathfrak{P} \to \mathbb{F}_\mathfrak{P}$ is given by

$$\overline{\sigma}(\alpha + \mathfrak{P}) = \sigma(\alpha) + \mathfrak{P} \qquad \forall \alpha \in \mathcal{O}_\mathbb{L}.$$

Suppose additionally that $\mathbb{K}$ is a subfield of $\mathbb{L}$, and that $\mathfrak{p}$ is the prime ideal of $\mathcal{O}_\mathbb{K}$ lying under $\mathfrak{P}$. Let $\Psi_{\mathfrak{P}|\mathfrak{p}}$ denote the restriction of the above-mentioned map $\sigma \mapsto \overline{\sigma}$ to the subgroup $D(\mathfrak{P}|\mathfrak{p})$. Then, also in Proposition 2.15, we showed that the image of $\Psi_{\mathfrak{P}|\mathfrak{p}}$ is actually contained in $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$, so we may write

$$\Psi_{\mathfrak{P}|\mathfrak{p}}\colon D(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}).$$

Remark 2.21. Suppose now that $\mathbb{M}$ is an intermediate field of the extension $\mathbb{L}/\mathbb{K}$, and that $\mathfrak{q}$ is the prime ideal of $\mathcal{O}_\mathbb{M}$ lying above $\mathfrak{p}$ and below $\mathfrak{P}$. As $\mathbb{K} \subseteq \mathbb{M}$, any automorphism of $\mathbb{L}$ which fixes $\mathbb{M}$ pointwise also fixes $\mathbb{K}$ pointwise, and so $\mathrm{Gal}(\mathbb{L}/\mathbb{M}) \subseteq \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. In particular, any $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{M})$ which fixes $\mathfrak{P}$ is also in $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ and still fixes $\mathfrak{P}$. In other words, $D(\mathfrak{P}|\mathfrak{q}) \subseteq D(\mathfrak{P}|\mathfrak{p})$. As $\Psi_{\mathfrak{P}|\mathfrak{q}}$ and $\Psi_{\mathfrak{P}|\mathfrak{p}}$ are both restrictions of the same map $\sigma \mapsto \overline{\sigma}$, and their respective domains $D(\mathfrak{P}|\mathfrak{q})$ and $D(\mathfrak{P}|\mathfrak{p})$ satisfy the inclusion $D(\mathfrak{P}|\mathfrak{q}) \subseteq D(\mathfrak{P}|\mathfrak{p})$, clearly the restriction of $\Psi_{\mathfrak{P}|\mathfrak{p}}$ to $D(\mathfrak{P}|\mathfrak{q})$ is $\Psi_{\mathfrak{P}|\mathfrak{q}}$. When there is no confusion as to which field is the base field, we will just write $\Psi_\mathfrak{P}$, rather than $\Psi_{\mathfrak{P}|\mathfrak{p}}$.

In the rest of this section, our goal is to apply the first isomorphism theorem to the map $\Psi_\mathfrak{P}$, which we will see is a surjective group homomorphism.

Definition/Proposition 2.22. Let $\mathbb{L}/\mathbb{K}$ be an extension of number fields with Galois group G, and let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_\mathbb{L}$ lying above the non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_\mathbb{K}$. Then the map $\Psi_\mathfrak{P}\colon D(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ is a group homomorphism whose kernel is the set

$$I(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in G :\ \sigma(\alpha) \equiv \alpha \,(\mathrm{mod}\,\mathfrak{P}) \text{ for all } \alpha \in \mathcal{O}_\mathbb{L}\}.$$

We call $I(\mathfrak{P}|\mathfrak{p})$ the *inertia group* of $\mathfrak{P}$ over $\mathfrak{p}$.

Proof. Let $\sigma, \tau \in D(\mathfrak{P}|\mathfrak{p})$. For all $\alpha \in \mathcal{O}_\mathbb{L}$, we have

$$\begin{aligned}\Psi_\mathfrak{P}(\sigma\tau)(\alpha + \mathfrak{P}) = (\sigma\tau)(\alpha) + \mathfrak{P} = \sigma\big(\tau(\alpha)\big) + \mathfrak{P} = \Psi_\mathfrak{P}(\sigma)\big(\tau(\alpha) + \mathfrak{P}\big) \\ = \Psi_\mathfrak{P}(\sigma)\big(\Psi_\mathfrak{P}(\tau)(\alpha + \mathfrak{P})\big) = \big(\Psi_\mathfrak{P}(\sigma)\Psi_\mathfrak{P}(\tau)\big)(\alpha + \mathfrak{P}).\end{aligned}$$

Hence $\Psi_{\mathfrak{P}}(\sigma\tau) = \Psi_{\mathfrak{P}}(\sigma)\Psi_{\mathfrak{P}}(\tau)$, and so $\Psi_{\mathfrak{P}}$ is a group homomorphism. We also have

$$\begin{aligned}\ker(\Psi_{\mathfrak{P}}) &= \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) : \ \Psi_{\mathfrak{P}}(\sigma)(\alpha + \mathfrak{P}) = \alpha + \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_{\mathbb{L}}\} \\ &= \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) : \ \sigma(\alpha) + \mathfrak{P} = \alpha + \mathfrak{P} \text{ for all } \alpha \in \mathcal{O}_{\mathbb{L}}\} \\ &= \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) : \ \sigma(\alpha) \equiv \alpha \,(\mathrm{mod}\,\mathfrak{P}) \text{ for all } \alpha \in \mathcal{O}_{\mathbb{L}}\} \\ &= I(\mathfrak{P}|\mathfrak{p}).\end{aligned}$$

□

Proposition 2.23. *Assume the same notation as Definition/Proposition 2.22, and suppose additionally that the extension $\mathbb{L}/\mathbb{K}$ is Galois. Then $\Psi_{\mathfrak{P}}$ is surjective.*

Proof. As $\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}$ is an extension of finite fields, it is a finite and separable extension, and so $\mathbb{F}_{\mathfrak{P}} = \mathbb{F}_{\mathfrak{p}}(\overline{\alpha})$ for some $\overline{\alpha} \in \mathbb{F}_{\mathfrak{P}}^{\times}$ by the primitive element theorem.

Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ be the $g = g_{\mathfrak{p}}$ prime ideals of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{p}$, where $\mathfrak{P}_1 = \mathfrak{P}$. As the ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are pairwise coprime, by the Chinese remainder theorem, there is an $\alpha \in \mathcal{O}_{\mathbb{L}}$ which simultaneously satisfies the equations:

$$\alpha + \mathfrak{P}_1 = \overline{\alpha}, \qquad \alpha + \mathfrak{P}_2 = 0 + \mathfrak{P}_2, \qquad \ldots, \qquad \alpha + \mathfrak{P}_g = 0 + \mathfrak{P}_g.$$

Let

$$h = \prod_{\sigma \in G} \big(X - \sigma(\alpha)\big) \in \mathbb{L}[X].$$

We know that $\mathbb{K} = \mathbb{L}^G$ because the extension $\mathbb{L}/\mathbb{K}$ is Galois. Hence, if we can show that the coefficients of h are fixed by each element of G, then we may conclude that $h \in \mathbb{K}[X]$. Let $\tau \in G$. The induced map $\widetilde{\tau}\colon \mathbb{L}[X] \to \mathbb{L}[X]$ given by

$$\widetilde{\tau}\Big(\sum_{k=0}^{d} a_k X^k\Big) = \sum_{k=0}^{d} \tau(a_k) X^k$$

is a ring homomorphism. As the map $\sigma \mapsto \tau\sigma$ is a permutation of G, we have

$$\widetilde{\tau}(h) = \prod_{\sigma \in G} \widetilde{\tau}\big(X - \sigma(\alpha)\big) = \prod_{\sigma \in G} \big(X - (\tau\sigma)(\alpha)\big) = h.$$

This means that h and $\widetilde{\tau}(h)$ have the same coefficients, and thus τ fixes the coefficients of h. As α is an algebraic integer, all of the $\sigma(\alpha)$ are algebraic integers, and thus all of the coefficients of h are algebraic integers. Hence $h \in \mathcal{O}_{\mathbb{K}}[X]$.

Let $\overline{h} \in \mathbb{F}_{\mathfrak{p}}[X]$ be obtained by reducing the coefficients of h modulo $\mathfrak{p}$. Clearly

$$\overline{h} = \prod_{\sigma \in D(\mathfrak{P}|\mathfrak{p})} \Big(X - \big(\sigma(\alpha) + \mathfrak{P}\big)\Big) \prod_{\sigma \in G \backslash D(\mathfrak{P}|\mathfrak{p})} \Big(X - \big(\sigma(\alpha) + \mathfrak{P}\big)\Big)$$

in $\mathbb{F}_{\mathfrak{P}}[X]$. We claim that the roots of $\overline{h}$ coming from $G \backslash D(\mathfrak{P}|\mathfrak{p})$ are zero, and thus

$$\overline{h}/X^m = \prod_{\sigma \in D(\mathfrak{P}|\mathfrak{p})} \Big(X - \big(\sigma(\alpha) + \mathfrak{P}\big)\Big) \in \mathbb{F}_{\mathfrak{p}}[X],$$

where $m = |G \backslash D(\mathfrak{P}|\mathfrak{p})|$. Suppose that $\sigma \in G \backslash D(\mathfrak{P}_1|\mathfrak{p})$. Then $\sigma^{-1}(\mathfrak{P}_1)$ is a non-zero prime ideal of $\mathcal{O}_\mathbb{L}$ above $\mathfrak{p}$, but $\sigma^{-1}(\mathfrak{P}_1) \neq \mathfrak{P}_1$ as $\sigma \notin D(\mathfrak{P}_1|\mathfrak{p})$. Hence,

$$\alpha + \sigma^{-1}(\mathfrak{P}_1) = 0 + \sigma^{-1}(\mathfrak{P}_1),$$

and since σ is an automorphism, we may apply σ to both sides to get

$$\sigma(\alpha) + \mathfrak{P}_1 = 0 + \mathfrak{P}_1.$$

Let $\overline{\sigma} \in \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$. As $\overline{\sigma}$ fixes the coefficients of $\overline{h}/X^m$, it permutes its roots, and so $\overline{\sigma}(\overline{\alpha}) = \sigma(\alpha) + \mathfrak{P} = \Psi_\mathfrak{P}(\sigma)(\overline{\alpha})$ for some $\sigma \in D(\mathfrak{P}|\mathfrak{p})$. But as $\mathbb{F}_\mathfrak{P} = \mathbb{F}_\mathfrak{p}(\overline{\alpha})$, the elements of $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ are uniquely determined by where they send $\overline{\alpha}$, and so $\overline{\sigma} = \Psi_\mathfrak{P}(\sigma)$. Hence $\Psi_\mathfrak{P}$ is surjective. □

Recall that the Galois group of an extension of finite fields $\mathbb{F}_{q^k}/\mathbb{F}_q$ is cyclic of order k, and is generated by the Frobenius automorphism $x \mapsto x^q$. In our case, $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ is cyclic of order $f_\mathfrak{p}$, and is generated by the Frobenius automorphism $x \mapsto x^{N(\mathfrak{p})}$. Combining Definition/Proposition 2.22 and Proposition 2.23, we know that if $\mathbb{L}/\mathbb{K}$ is Galois, then $\Psi_\mathfrak{P} \colon D(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ is a surjective group homomorphism with kernel $I(\mathfrak{P}|\mathfrak{p})$. By the first isomorphism theorem for groups, $\Psi_\mathfrak{P}$ induces an isomorphism

$$\overline{\Psi}_\mathfrak{P} \colon D(\mathfrak{P}|\mathfrak{p})/I(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}),$$

and thus $D(\mathfrak{P}|\mathfrak{p})/I(\mathfrak{P}|\mathfrak{p})$ is also cyclic of order $f_\mathfrak{p}$, generated by some element sent by $\overline{\Psi}_\mathfrak{P}$ to the Frobenius automorphism. As $|D(\mathfrak{P}|\mathfrak{p})| = e_\mathfrak{p} f_\mathfrak{p}$, this also implies that $|I(\mathfrak{P}|\mathfrak{p})| = e_\mathfrak{p}$. Hence $I(\mathfrak{P}|\mathfrak{p})$ is the trivial group if and only if $\mathfrak{p}$ is unramified in $\mathcal{O}_\mathbb{L}$. In this case, $D(\mathfrak{P}|\mathfrak{p})$ is itself isomorphic to $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$.

From now on, we will only be concerned with the case that $\mathfrak{p}$ is unramified in $\mathcal{O}_\mathbb{L}$, that is, that $e_\mathfrak{p} = 1$. The following corollary of Definition/Proposition 2.22 and Proposition 2.23 summarises the discussion so far, in this particular case.

Corollary 2.24. *Assume the same notation as Proposition 2.23, and suppose additionally that $\mathfrak{p}$ is unramified in $\mathcal{O}_\mathbb{L}$. Then*

$$\Psi_\mathfrak{P} \colon D(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$$

is a group isomorphism. It follows that $D(\mathfrak{P}|\mathfrak{p})$ is a cyclic group of order $f_\mathfrak{p}$, generated by the element sent by $\Psi_\mathfrak{P}$ to the Frobenius automorphism $x \mapsto x^{N(\mathfrak{p})}$.

2.2.3 Frobenius elements and Frobenius classes

It is clear now what the *Frobenius element* associated to a prime ideal $\mathfrak{P}$ of $\mathcal{O}_\mathbb{L}$ in a Galois extension of number fields $\mathbb{L}/\mathbb{K}$ should be.

Definition 2.25 (Frobenius element)**.** Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of number fields with Galois group G. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_\mathbb{K}$ which is unramified in $\mathcal{O}_\mathbb{L}$, and let $\mathfrak{P}$ be one of the prime ideals of $\mathcal{O}_\mathbb{L}$ lying above $\mathfrak{p}$. The *Frobenius element* (or *Frobenius substitution*) of $\mathfrak{P}$ is the element of $D(\mathfrak{P}|\mathfrak{p})$ which is sent by

$\Psi_{\mathfrak{P}}$ to the Frobenius automorphism $x \mapsto x^{N(\mathfrak{p})}$ of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. It will be denoted by the *Frobenius symbol*[1] $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$.

Proposition 2.26. *Assume the same notation as Definition 2.25. Then* $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$ *is the* ***unique*** *element* $\sigma \in G$ *which satisfies the congruence equation*

$$\sigma(\alpha) \equiv \alpha^{N(\mathfrak{p})} \,(mod \mathfrak{P}) \qquad \forall \alpha \in \mathcal{O}_{\mathbb{L}}. \tag{2.2.1}$$

Proof. As $\Psi_{\mathfrak{P}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right])$ is the Frobenius automorphism $x \mapsto x^{N(\mathfrak{p})}$, clearly $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$ satisfies the congruence equation (2.2.1). For uniqueness, suppose that $\sigma \in G$ satisfies (2.2.1). In particular, if $\alpha \in \mathfrak{P}$, then $\alpha^{N(\mathfrak{p})} \in \mathfrak{P}$ and so

$$\sigma(\alpha) \equiv 0 \,(\mathrm{mod}\, \mathfrak{P}) \qquad \forall \alpha \in \mathfrak{P}.$$

Hence $\sigma(\mathfrak{P}) \subseteq \mathfrak{P}$, that is, $\mathfrak{P} \mid \sigma(\mathfrak{P})$. But $\sigma(\mathfrak{P})$ is a prime ideal of $\mathcal{O}_{\mathbb{L}}$, so actually $\sigma(\mathfrak{P}) = \mathfrak{P}$. Hence $\sigma \in D(\mathfrak{P}|\mathfrak{p})$. As σ satisfies (2.2.1), we have

$$\Psi_{\mathfrak{P}}(\sigma)(x) = x^{N(\mathfrak{p})} \qquad \forall x \in \mathbb{F}_{\mathfrak{P}},$$

and thus $\Psi_{\mathfrak{P}}(\sigma)$ is the Frobenius automorphism of $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. But $\Psi_{\mathfrak{P}}$ is injective and $\Psi_{\mathfrak{P}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right])$ is also the Frobenius automorphism, so actually $\sigma = \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$. □

Proposition 2.27. *Assume the same notation as Definition 2.25. For each* $\sigma \in G$,

$$\left[\frac{\mathbb{L}/\mathbb{K}}{\sigma(\mathfrak{P})}\right] = \sigma \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right] \sigma^{-1}.$$

Proof. Let $\sigma \in G$. Let $\alpha \in \mathcal{O}_{\mathbb{L}}$. As $\sigma^{-1}(\alpha) \in \mathcal{O}_{\mathbb{L}}$, we know that

$$\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\left(\sigma^{-1}(\alpha)\right) \equiv \left(\sigma^{-1}(\alpha)\right)^{N(\mathfrak{p})} (\mathrm{mod}\, \mathfrak{P})$$

from Proposition 2.26. In other words, we have

$$\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\left(\sigma^{-1}(\alpha)\right) - \left(\sigma^{-1}(\alpha)\right)^{N(\mathfrak{p})} \in \mathfrak{P},$$

and applying the isomorphism σ, we get

$$\begin{aligned}\sigma(\mathfrak{P}) \ni \sigma\left(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\left(\sigma^{-1}(\alpha)\right) - \left(\sigma^{-1}(\alpha)\right)^{N(\mathfrak{p})}\right) \\ = \sigma\left(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\left(\sigma^{-1}(\alpha)\right)\right) - \left(\sigma\left(\sigma^{-1}(\alpha)\right)\right)^{N(\mathfrak{p})} = \left(\sigma\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\sigma^{-1}\right)(\alpha) - \alpha^{N(\mathfrak{p})}.\end{aligned}$$

Hence

$$\left(\sigma\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\sigma^{-1}\right)(\alpha) \equiv \alpha^{N(\mathfrak{p})} \,(\mathrm{mod}\, \sigma(\mathfrak{P})) \qquad \forall \alpha \in \mathcal{O}_{\mathbb{L}},$$

and by the *uniqueness* part of Proposition 2.26, the result follows. □

Definition 2.28 (Frobenius class and Artin symbol)**.** Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of number fields, and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$ which is unramified in $\mathcal{O}_{\mathbb{L}}$.

[1] This symbol was introduced by Hasse (see [12, pp. 280, Footnote 12]), but is not standard. Some texts use $\sigma_{\mathfrak{P}}$ or $\mathrm{Frob}_{\mathfrak{P}}$.

Let P denote the set of all prime ideals of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{p}$. The set of Frobenius elements of all of the prime ideals in P is called the *Frobenius class* of $\mathfrak{p}$ in the extension $\mathbb{L}/\mathbb{K}$, and is denoted by the *Artin symbol*[1]

$$\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = \left\{\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right] : \mathfrak{P} \in P\right\}.$$

Proposition 2.29. *Assume the same notation as Definition 2.28. Then for each $\mathfrak{P} \in P$, the Frobenius class $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right)$ is the conjugacy class of $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$ in G.*

Proof. As G acts transitively on P (Proposition 2.16), we may write

$$\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = \left\{\left[\frac{\mathbb{L}/\mathbb{K}}{\sigma(\mathfrak{P})}\right] : \sigma \in G\right\},$$

and by Proposition 2.27, this becomes

$$\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = \left\{\sigma\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\sigma^{-1} : \sigma \in G\right\},$$

which is, by definition, the conjugacy class of $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$ in G. □

Remark 2.30. If G is abelian, then each conjugacy class of G contains a single element. In particular, this implies that each Frobenius class $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right)$ contains a single element, which we will denote by $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]$. To help remember the notation, a symbol with square brackets always refers to a single element of G (including the symbol for the Artin map, which will be introduced in Definition 3.20), whilst the Artin symbol (which is written with parentheses) refers to a conjugacy class of G.

Proposition 2.31. *Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of number fields, and let $\mathbb{M}$ be an intermediate field of this extension. Let $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{P}$ be non-zero prime ideals of $\mathcal{O}_{\mathbb{K}}$, $\mathcal{O}_{\mathbb{M}}$, and $\mathcal{O}_{\mathbb{L}}$ respectively, with $\mathfrak{P}$ above $\mathfrak{q}$, and $\mathfrak{q}$ above $\mathfrak{p}$. Then*

$$\left[\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{P}}\right] = \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]^{f(\mathfrak{q}|\mathfrak{p})}.$$

If $\mathbb{M}/\mathbb{K}$ is also Galois, then

$$\left[\frac{\mathbb{M}/\mathbb{K}}{\mathfrak{q}}\right] = \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\Big|_{\mathbb{M}}.$$

Remark 2.32. As $\mathfrak{p}$ is unramified in $\mathcal{O}_{\mathbb{L}}$, it is also unramified in $\mathcal{O}_{\mathbb{M}}$ (Proposition 2.5), so if $\mathbb{M}/\mathbb{K}$ is Galois, then the Frobenius element $\left[\frac{\mathbb{M}/\mathbb{K}}{\mathfrak{q}}\right]$ is indeed defined.

Proof. We begin by showing that $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]^{f(\mathfrak{q}|\mathfrak{p})} = \left[\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{P}}\right]$. As this involves two different base fields $\mathbb{M}$ and $\mathbb{K}$, we will use the original notation $\Psi_{\mathfrak{P}|\mathfrak{q}} \colon D(\mathfrak{P}|\mathfrak{q}) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{q}})$ and $\Psi_{\mathfrak{P}|\mathfrak{p}} \colon D(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$, rather than the simpler notation $\Psi_{\mathfrak{P}}$. We have

$$\Psi_{\mathfrak{P}|\mathfrak{p}}\left(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]^{f(\mathfrak{q}|\mathfrak{p})}\right) = \Psi_{\mathfrak{P}|\mathfrak{p}}\left(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\right)^{f(\mathfrak{q}|\mathfrak{p})},$$

[1] This symbol was also introduced by Hasse (see [12, pp. 280, Footnote 12]). Like us, Hasse used it to mean the conjugacy class of G associated to $\mathfrak{p}$, but this meaning is not standard.

because $\Psi_{\mathfrak{P}|\mathfrak{p}}$ is a group homomorphism. Now $\Psi_{\mathfrak{P}|\mathfrak{p}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right])$ is, by definition, the Frobenius automorphism $x \mapsto x^{N(\mathfrak{p})}$ in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. As $N(\mathfrak{q}) = N(\mathfrak{p})^{f(\mathfrak{q}|\mathfrak{p})}$, the Frobenius automorphism $x \mapsto x^{N(\mathfrak{q})}$ in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{q}})$ is related to the Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ by

$$\big(x \mapsto x^{N(\mathfrak{p})}\big)^{f(\mathfrak{q}|\mathfrak{p})} = \big(x \mapsto x^{N(\mathfrak{q})}\big),$$

where the $f(\mathfrak{q}|\mathfrak{p})$-th power on the left means the composition of $x \mapsto x^{N(\mathfrak{p})}$ with itself $f(\mathfrak{q}|\mathfrak{p})$ times. In other words, $\Psi_{\mathfrak{P}|\mathfrak{p}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right])^{f(\mathfrak{q}|\mathfrak{p})}$ is the Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{q}})$. But $\Psi_{\mathfrak{P}|\mathfrak{p}}(\left[\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{P}}\right]) = \Psi_{\mathfrak{P}|\mathfrak{q}}(\left[\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{P}}\right])$ by Remark 2.21, and $\Psi_{\mathfrak{P}|\mathfrak{q}}(\left[\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{P}}\right])$ is, by definition, the Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{q}})$. Hence

$$\Psi_{\mathfrak{P}|\mathfrak{p}}(\left[\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{P}}\right]) = \Psi_{\mathfrak{P}|\mathfrak{p}}\Big(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]^{f(\mathfrak{q}|\mathfrak{p})}\Big).$$

As $\Psi_{\mathfrak{P}|\mathfrak{p}}$ is a bijection, the first part of the proposition follows.

We now prove the second part of the proposition. Suppose that $\mathbb{M}/\mathbb{K}$ is Galois. First, we show that $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}}$ lies in the domain $D(\mathfrak{q}|\mathfrak{p})$ of the function $\Psi_{\mathfrak{q}}$ $(= \Psi_{\mathfrak{q}|\mathfrak{p}})$. As $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}}$ is a $\mathbb{K}$-embedding of $\mathbb{M}$ and the extension $\mathbb{M}/\mathbb{K}$ is Galois, $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}}$ is actually a $\mathbb{K}$-automorphism of $\mathbb{M}$ and thus it is in $\mathrm{Gal}(\mathbb{M}/\mathbb{K})$. But $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$ is in $D(\mathfrak{P}|\mathfrak{p})$, so it fixes $\mathfrak{P}$, and thus also $\mathfrak{q}$ because $\mathfrak{q} \subseteq \mathfrak{P}$. Hence $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}}$ fixes $\mathfrak{q}$, and thus it is in $D(\mathfrak{q}|\mathfrak{p})$.

We wish to show that $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}} = \left[\frac{\mathbb{M}/\mathbb{K}}{\mathfrak{q}}\right]$. To do this, we will show that $\Psi_{\mathfrak{q}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}})$ is the Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$. But the Frobenius automorphism $x \mapsto x^{N(\mathfrak{p})}$ in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_{\mathfrak{p}})$ is the restriction to $\mathbb{F}_{\mathfrak{q}}$ of the Frobenius automorphism $x \mapsto x^{N(\mathfrak{p})}$ in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$, and $\Psi_{\mathfrak{P}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right])$ is by definition the Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$. Hence, it suffices to show that $\Psi_{\mathfrak{q}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}}) = \Psi_{\mathfrak{P}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right])\big|_{\mathbb{F}_{\mathfrak{q}}}$, or equivalently, that

$$\bar{\iota} \circ \Psi_{\mathfrak{q}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}}) = \Psi_{\mathfrak{P}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]) \circ \bar{\iota},$$

where $\bar{\iota}\colon \mathbb{F}_{\mathfrak{q}} \hookrightarrow \mathbb{F}_{\mathfrak{P}}$ is the embedding of $\mathbb{F}_{\mathfrak{q}}$ into $\mathbb{F}_{\mathfrak{P}}$. For all $\alpha \in \mathcal{O}_{\mathbb{M}}$, we have

$$\begin{aligned}\bar{\iota}\big(\Psi_{\mathfrak{q}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}})(\alpha+\mathfrak{q})\big) &= \bar{\iota}\big(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}}(\alpha)+\mathfrak{q}\big) = \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}}(\alpha)+\mathfrak{P} \\ &= \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right](\alpha)+\mathfrak{P} = \Psi_{\mathfrak{P}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right])(\alpha+\mathfrak{P}) = \Psi_{\mathfrak{P}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right])\big(\bar{\iota}(\alpha+\mathfrak{q})\big),\end{aligned}$$

and so $\bar{\iota} \circ \Psi_{\mathfrak{q}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_{\mathbb{M}}) = \Psi_{\mathfrak{P}}(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]) \circ \bar{\iota}$. □

2.3 Dirichlet density

Chebotarev's density theorem is a statement about the frequency of prime ideals with a certain property, amongst all of the prime ideals of the ring of integers of an algebraic number field. The various notions of *density* are mathematical formulations of this idea of frequency, one such notion being that of *natural density*.

Definition 2.33 (Natural density)**.** Let $\mathbb{K}$ be a number field, and let $A \subseteq P(\mathbb{K})$. The *natural density* $d(A)$ of A (in $P(\mathbb{K})$) is defined by the limit

$$d(A) = \lim_{n\to\infty} \frac{|\{\mathfrak{p} \in A : \ N(\mathfrak{p}) \leqslant n\}|}{|\{\mathfrak{p} \in P(\mathbb{K}) : \ N(\mathfrak{p}) \leqslant n\}|},$$

whenever the limit exists.

There is another kind of density called the *Dirichlet density*, which is less obviously related to the notion of frequency. One can show that if the natural density of a set of prime ideals exists, then so does its Dirichlet density, and the two densities have the same value. Chebotarev's density theorem holds if one uses either natural density or Dirichlet density, and, by the remark in the previous sentence, it suffices to prove only the case for natural density. However, in this thesis, we will only consider Dirichlet density because it is easier to work with than natural density.

Definition 2.34 (Dirichlet density)**.** Let $\mathbb{K}$ be a number field, and let $A \subseteq P(\mathbb{K})$. The *Dirichlet density* $\delta(A)$ of A (in $P(\mathbb{K})$) is defined by the limit

$$\delta(A) = \lim_{\sigma\to 1^+} \frac{\sum_{\mathfrak{p}\in A} N(\mathfrak{p})^{-\sigma}}{\sum_{\mathfrak{p}\in P(\mathbb{K})} N(\mathfrak{p})^{-\sigma}},$$

whenever it exists (the sums converge when $\sigma \in (1, \infty)$, see Proposition 2.40).

Remark 2.35. We adopt the convention that σ will always be a real variable, whilst $s = \sigma + it$ will always be a complex variable with real part σ and imaginary part t. In the above definition, by $\sigma \to 1^+$, we mean for the limit to be taken over σ in the subspace $(1, \infty)$ of the metric space $\mathbb{R}$. In Chapter 4, we will consider limits as $s \to 1^+$, by which we mean for such a limit to be taken over s in right half-plane

$$H(1) = \{s \in \mathbb{C} : \ \mathrm{Re}(s) > 1\},$$

which is a subspace of the metric space $\mathbb{C}$. Certainly, if such a certain complex limit exists, then the corresponding real limit must also exist and take the same value.

Remark 2.36. The above definition of Dirichlet density involved sums indexed by sets. Throughout this thesis, we will encounter many such sums and products. Such sums are defined as follows, and the definition for such products is similar.

Definition 2.37. Let $(a_i)_{i\in I}$ be a sequence of complex numbers indexed by a countable set I. If $\sum_{k=1}^{\infty} a_{f(k)}$ is absolutely convergent for some enumeration $f\colon \mathbb{Z}^+ \to I$ of I, then we define

$$\sum_{i\in I} a_i = \sum_{k=1}^{\infty} a_{f(k)}.$$

We require absolute convergence in the above definition so that the value of the sum or product is independent of the particular enumeration order of its terms — we will refer to this property as *generalised commutativity*. To use these definitions for sums and products indexed by sets of ideals, we need the following result.

Proposition 2.38. *Let $\mathbb{K}$ be a number field. Then $\mathcal{I}_{\mathbb{K}}$ is countable.*

Proof. The set $P(\mathbb{K})$ is countable as it is the countable union, over all prime numbers p, of the finitely many prime ideals of $\mathcal{O}_\mathbb{K}$ above $p\mathbb{Z}$. Hence, $\mathcal{I}_\mathbb{K}$ is the countable union, over all natural numbers n, of the countably many non-zero fractional ideals whose unique prime ideal factorisations have n factors (counting multiplicity). □

On occasion, we also use a property of absolutely convergent sums and products that we call *generalised associativity*, formalised for sums in the following theorem.

Theorem 2.39 (Generalised associativity)**.** *Let $(a_i)_{i\in I}$ be a sequence of complex numbers, indexed over a countable index set I. Let $(I_j)_{j\in J}$ be a partition of I into index sets I_j, where J is also a countable index set. For each $j \in J$, let*

$$S_j = \sum_{i\in I_j} a_i$$

Then the series $\sum_{i\in I} a_i$ converges absolutely, if and only if each of the series S_j converges absolutely and the series $\sum_{j\in J} S_j$ converges absolutely. In this case,

$$\sum_{i\in I} a_i = \sum_{j\in J} S_j = \sum_{j\in J} \Big(\sum_{i\in I_j} a_i \Big).$$

Generalised associativity allows us to regroup the terms of an absolutely convergent sum or product however we like, hence the name. For a more through discussion of the rearrangement properties of absolutely convergent series, and proofs of the results that we have just stated, consult Knopp [19, §16].

In light of the above discussion, provided that the series in the numerator and denominator of the limit defining the Dirichlet density actually converge, then they will converge absolutely because $N(\mathfrak{p})^{-\sigma}$ is a positive real number whenever $\sigma \in (1, \infty)$. To make sense of the limit, they must at least converge on some neighbourhood of the limit point 1 inside of the interval $(1, \infty)$ — i.e. on some open interval of the form $(1, 1+\epsilon)$. We will actually show they converge on all of $(1, \infty)$.

Proposition 2.40. *Let $\mathbb{K}$ be a number field, and let $A \subseteq P(\mathbb{K})$. Then the series*

$$\sum_{\mathfrak{p}\in A} N(\mathfrak{p})^{-\sigma}$$

converges for all $\sigma \in (1, \infty)$.

Proof. As $A \subseteq P(\mathbb{K})$, it suffices to show that the sum $\sum_{\mathfrak{p}\in P(\mathbb{K})} N(\mathfrak{p})^{-\sigma}$ converges. By generalised associativity (Theorem 2.39), it suffices in turn to show:

- for each prime number p, the convergence of the series $\sum_{\mathfrak{p}|p\mathcal{O}_\mathbb{K}} N(\mathfrak{p})^{-\sigma}$, taken over all prime ideals $\mathfrak{p}$ of $\mathcal{O}_\mathbb{K}$ lying over $p\mathbb{Z}$; and
- the convergence of the series $\sum_p \sum_{\mathfrak{p}|p\mathcal{O}_\mathbb{K}} N(\mathfrak{p})^{-\sigma}$.

As there are only finitely many prime ideals $\mathfrak{p}$ above each prime ideal $p\mathbb{Z}$, each of the series $\sum_{\mathfrak{p}|p\mathcal{O}_\mathbb{K}} N(\mathfrak{p})^{-\sigma}$ is a finite sum and so converges trivially. Let $n = [\mathbb{K} : \mathbb{Q}]$. As $f(\mathfrak{p}|p\mathbb{Z}) \geqslant 1$, and there are at most n prime ideals $\mathfrak{p}$ above a given prime ideal $p\mathbb{Z}$,

$$\sum_p \sum_{\mathfrak{p}|p\mathcal{O}_\mathbb{K}} \frac{1}{N(\mathfrak{p})^\sigma} = \sum_p \sum_{\mathfrak{p}|p\mathcal{O}_\mathbb{K}} \frac{1}{p^{f(\mathfrak{p}|p\mathbb{Z})\sigma}} \leqslant \sum_p \sum_{\mathfrak{p}|p\mathcal{O}_\mathbb{K}} \frac{1}{p^\sigma} \leqslant n \sum_p \frac{1}{p^\sigma} < n \sum_{j=1}^{\infty} \frac{1}{j^\sigma}.$$

The right-most series is a convergent p-series with $p = \sigma > 1$, and thus the series on the left-hand side converges by comparison. □

At this point, we have all we need to understand the statement of Chebotarev's density theorem (Theorem 2.1). In the rest of this section, we will introduce the related notions of upper and lower Dirichlet densities, which we will use when we prove the abelian case of Chebotarev's density theorem.

2.3.1 Limit superior and inferior of real valued functions at a point

The proof of the abelian case of Chebotarev's density theorem (Chapter 6), relies heavily on the notions of *upper Dirichlet density* and *lower Dirichlet density*. The upper (resp. lower) Dirichlet density is defined similarly to the (ordinary) Dirichlet density, but with the limit at a point replaced with the limit superior (resp. inferior) at the point. The limit superior and inferior of a real valued function at a point are less frequently encountered in introductory analysis courses and textbooks than their cousins, the limit superior and inferior of sequences. To this end, for the reader's convenience, we briefly recall here their definitions and important properties. For proofs, see §5.3 of Beberian [6].

Definition 2.41 (Point limit superior and inferior)**.** Let (X, d) be a metric space. For all $a \in X$ and all $r > 0$, the *punctured ball* in X with center a and radius r is

$$B^\circ(a, r) = \{x \in X : \ 0 < d(x, a) < r\}.$$

If $Y \subseteq X$, $f \colon Y \to \mathbb{R}$, and $a \in X$ is a limit point of Y, then

- the *limit superior* of f as $x \to a$ in X is given by

$$\overline{\lim_{x\to a}} f(x) = \lim_{r\to 0^+} \Big(\sup_{x\in B^\circ(a,r)} f(x) \Big),$$

- the *limit inferior* of f as $x \to a$ in X is given by

$$\underline{\lim_{x\to a}} f(x) = \lim_{r\to 0^+} \Big(\inf_{x\in B^\circ(a,r)} f(x) \Big).$$

The limit superior and inferior enjoy the following properties.

Proposition 2.42. *Let (X, d) be a metric space, let $Y \subseteq X$, let $f, g \colon Y \to \mathbb{R}$, and let $a \in X$ be a limit point of Y. Then the following properties hold:*

(1) $\overline{\lim_{x\to a}} f(x)$ *and* $\underline{\lim_{x\to a}} f(x)$ *always exist (we allow the values* $\pm\infty$*).*

(2) $\underline{\lim_{x\to a}} f(x) \leqslant \overline{\lim_{x\to a}} f(x)$.

(3) $\lim_{x\to a} f(x)$ *exists if and only if* $\underline{\lim_{x\to a}} f(x) = \overline{\lim_{x\to a}} f(x)$*. In this case, all are equal.*

(4) $\overline{\lim\limits_{x\to a}}\big(f(x)+g(x)\big) \leqslant \overline{\lim\limits_{x\to a}} f(x) + \overline{\lim\limits_{x\to a}} g(x)$.
(5) $\underline{\lim\limits_{x\to a}}\big(f(x)+g(x)\big) \geqslant \underline{\lim\limits_{x\to a}} f(x) + \underline{\lim\limits_{x\to a}} g(x)$.
(6) $\overline{\lim\limits_{x\to a}}\big(-g(x)\big) = -\underline{\lim\limits_{x\to a}} g(x)$.

We will also need the following result.

Proposition 2.43. *Let (X,d) be a metric space, let $Y \subseteq X$, let $f,g\colon Y\to\mathbb{R}$, and let $a\in X$ be a limit point of Y. Then*

$$\underline{\lim_{x\to a}}\big(f(x)+g(x)\big) \leqslant \underline{\lim_{x\to a}} f(x) + \overline{\lim_{x\to a}} g(x) \leqslant \overline{\lim_{x\to a}}\big(f(x)+g(x)\big).$$

Proof. By properties (4) and (6) of Proposition 2.42, we have

$$\begin{aligned}\overline{\lim_{x\to a}} g(x) &= \overline{\lim_{x\to a}}\big(f(x)+g(x)-f(x)\big)\\ &\leqslant \overline{\lim_{x\to a}}\big(f(x)+g(x)\big) + \overline{\lim_{x\to a}}\big(-f(x)\big)\\ &= \overline{\lim_{x\to a}}\big(f(x)+g(x)\big) - \underline{\lim_{x\to a}} f(x),\end{aligned}$$

and the right-hand inequality follows. The other inequality is proved similarly. □

2.3.2 Upper and lower Dirichlet densities

We may now define the upper and lower Dirichlet densities.

Definition 2.44. Let $\mathbb{K}$ be a number field, and let $A\subseteq P(\mathbb{K})$.

- The *upper Dirichlet density* of A (in $P(\mathbb{K})$) is defined by the limit superior

$$\delta_{\sup}(A) = \overline{\lim_{\sigma\to 1^+}} \frac{\sum_{\mathfrak{p}\in A} N(\mathfrak{p})^{-\sigma}}{\sum_{\mathfrak{p}\in P(\mathbb{K})} N(\mathfrak{p})^{-\sigma}}.$$

- The *lower Dirichlet density* of A (in $P(\mathbb{K})$) is defined by the limit inferior

$$\delta_{\inf}(A) = \underline{\lim_{\sigma\to 1^+}} \frac{\sum_{\mathfrak{p}\in A} N(\mathfrak{p})^{-\sigma}}{\sum_{\mathfrak{p}\in P(\mathbb{K})} N(\mathfrak{p})^{-\sigma}}.$$

Remark 2.45. By $\overline{\lim}_{\sigma\to1^+}$ and $\underline{\lim}_{\sigma\to1^+}$, we mean $X=\mathbb{R}$, $Y=(1,\infty)$, and $a=1$ with respect to the notation in Definition 2.41.

By Proposition 2.42, the upper and lower Dirichlet densities have the following properties.

Proposition 2.46. *Let $\mathbb{K}$ be a number field. Let $A\subseteq P(\mathbb{K})$. Then*
(1) $0\leqslant\delta_{\inf}(A)\leqslant 1$, $0\leqslant\delta_{\sup}(A)\leqslant 1$, *and if $\delta(A)$ exists then $0\leqslant\delta(A)\leqslant 1$;*
(2) $\delta_{\inf}(A)\leqslant\delta_{\sup}(A)$;
(3) $\delta(A)$ *exists if and only if* $\delta_{\inf}(A)=\delta_{\sup}(A)$, *in which case all three are equal;*
(4) $\delta\big(P(\mathbb{K})\big)=\delta_{\inf}\big(P(\mathbb{K})\big)=\delta_{\sup}\big(P(\mathbb{K})\big)=1$; *and*
(5) $\delta(\emptyset)=\delta_{\inf}(\emptyset)=\delta_{\sup}(\emptyset)=0$.

Proposition 2.47. *Let $\mathbb{K}$ be a number field. Let $A,B\subseteq P(\mathbb{K})$ be disjoint. Then*
(1) $\delta_{\sup}(A\cup B)\leqslant\delta_{\sup}(A)+\delta_{\sup}(B)$;
(2) $\delta_{\inf}(A\cup B)\geqslant\delta_{\inf}(A)+\delta_{\inf}(B)$;

(3) $\delta_{\inf}(A \cup B) \leqslant \delta_{\inf}(A) + \delta_{\sup}(B) \leqslant \delta_{\sup}(A \cup B)$*; and*
(4) if any two of the three Dirichlet densities $\delta(A \cup B)$*,* $\delta(A)$ *and* $\delta(B)$ *exists, then so does the third, in which case* $\delta(A \cup B) = \delta(A) + \delta(B)$*.*

Proof. As A and B are disjoint, we have the equality

$$\frac{\sum_{\mathfrak{p} \in A \cup B} N(\mathfrak{p})^{-\sigma}}{\sum_{\mathfrak{p} \in P(\mathbb{K})} N(\mathfrak{p})^{-\sigma}} = \frac{\sum_{\mathfrak{p} \in A} N(\mathfrak{p})^{-\sigma}}{\sum_{\mathfrak{p} \in P(\mathbb{K})} N(\mathfrak{p})^{-\sigma}} + \frac{\sum_{\mathfrak{p} \in B} N(\mathfrak{p})^{-\sigma}}{\sum_{\mathfrak{p} \in P(\mathbb{K})} N(\mathfrak{p})^{-\sigma}}$$

for all $\sigma \in (1, \infty)$. Properties (1) and (2) follow, respectively, from properties (4) and (5) of Proposition 2.42. Property (3) follows from Proposition 2.43. Property (4) follows by taking the (ordinary) limit as $\sigma \to 1^+$. □

Remark 2.48. If $\delta(A \cup B)$ exists, then property (3) of Proposition 2.46 and property (3) of Proposition 2.47 together imply that

$$\delta(A \cup B) = \delta_{\inf}(A \cup B) \leqslant \delta_{\inf}(A) + \delta_{\sup}(B) \leqslant \delta_{\sup}(A \cup B) = \delta(A \cup B).$$

Hence, in this case, actually $\delta(A \cup B) = \delta_{\inf}(A) + \delta_{\sup}(B)$.

2.4 The Frobenius density theorem

At the start of this chapter, we said that we would return to generalise Example 2.4. Its generalisation is the Frobenius density theorem (mentioned in Chapter 1). In this section, we will state the Frobenius density theorem, explore the relationship between decomposition type and cycle type, and then show that the Frobenius density theorem is implied by Chebotarev's density theorem.

Let $\mathbb{K}$ be a number field. Let $h \in \mathcal{O}_{\mathbb{K}}[X]$ be monic of degree n, with distinct roots $\alpha_1, \ldots, \alpha_n$ in $\mathbb{C}$. Let $\mathbb{L}$ be the splitting field of h over $\mathbb{K}$, that is, $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$. As h is monic and has algebraic integer coefficients, its roots are algebraic integers, so actually $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_{\mathbb{L}}$. Hence, in $\mathcal{O}_{\mathbb{L}}[X]$,

$$h = (X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n).$$

Let $A = \{\alpha_1, \ldots, \alpha_n\}$. As $\mathbb{L}$ is the splitting field of h over $\mathbb{K}$, the restriction of each element of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ to A is a permutation of A. The *cycle type* of an element $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is the unordered list of the lengths of the cycles in a disjoint cycle decomposition of $\sigma|_A$. Given $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ with a disjoint cycle decomposition

$$\big(\alpha_{k(1,1)} \ \cdots \ \alpha_{k(1,f(1))}\big) \cdots \big(\alpha_{k(g,1)} \ \cdots \ \alpha_{k(g,f(g))}\big),$$

and $\tau \in \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, it is well known that $\tau\sigma\tau^{-1}$ has a disjoint cycle decomposition

$$\big(\tau(\alpha_{k(1,1)}) \ \cdots \ \tau(\alpha_{k(1,f(1))})\big) \cdots \big(\tau(\alpha_{k(g,1)}) \ \cdots \ \tau(\alpha_{k(g,f(g))})\big).$$

Hence conjugate elements of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ have the same cycle type.

The *decomposition type* of a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{L}}$ (which we will also refer to as the *decomposition type* of h modulo $\mathfrak{p}$) is the unordered list of the degrees of the irreducible factors of $\overline{h}$ in $\mathbb{F}_{\mathfrak{p}}[X]$, where $\overline{h}$ denotes the polynomial in $\mathbb{F}_{\mathfrak{p}}[X]$ obtained by reducing the coefficients of h modulo $\mathfrak{p}$.

Frobenius proved [14] the following result in the case that $\mathbb{K} = \mathbb{Q}$.

Theorem 2.49 (Frobenius density theorem)**.** *Assume the above notation. Let $f_1, \ldots, f_g$ be positive integers which sum to n. Let*

$$P = \big\{\mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \text{ of decomposition type } f_1, \ldots, f_g\big\},$$
$$C = \big\{\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{K}) : \ \sigma \text{ of cycle type } f_1, \ldots, f_g\big\}.$$

Then

$$\delta(P) = \frac{|C|}{|\mathrm{Gal}(\mathbb{L}/\mathbb{K})|}.$$

Example 2.50. Example 2.4 provides empirical evidence that the Frobenius density theorem holds in the case that $h = X^3 - 2$ and $\mathbb{K} = \mathbb{Q}$.

In order to deduce the Frobenius density theorem from Chebotarev's density theorem, we need the following result.

Proposition 2.51. *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_\mathbb{K}$ that is unramified in $\mathcal{O}_\mathbb{L}$, and which does not divide the ideal $\langle \mathrm{disc}(h) \rangle$ of $\mathcal{O}_\mathbb{K}$. Then the decomposition type of $\mathfrak{p}$ is the same as the cycle type of $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right)$.*

Remark 2.52. Recall, given a field $\mathbb{F}$ (not necessarily a number field), that the *discriminant* of a polynomial $h \in \mathbb{F}[X]$ is defined by

$$\mathrm{disc}(h) = {a_n}^{2n-2} \prod_{1 \leqslant i < j \leqslant n} (\alpha_i - \alpha_j)^2$$

where n is the degree of h, a_n is the leading coefficient of h, and $\alpha_1, \ldots, \alpha_n$ are the roots of h in some algebraic closure of $\mathbb{F}$. Clearly h has distinct roots if and only if $\mathrm{disc}(h) \neq 0$. One can show that $\mathrm{disc}(h) \in \mathbb{F}$.

Proof of Proposition 2.51. It suffices to show that the decomposition type of $\mathfrak{p}$ is the same as the cycle type of $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$, where $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_\mathbb{L}$ above $\mathfrak{p}$. For each $\beta \in \mathcal{O}_\mathbb{L}$, let $\overline{\beta} \in \mathbb{F}_\mathfrak{P}$ denote the reduction of β modulo $\mathfrak{P}$, that is, $\overline{\beta} = \beta + \mathfrak{P}$. Let $\overline{h} \in \mathbb{F}_\mathfrak{P}[X]$ denote the polynomial obtained by reducing the coefficients of h modulo $\mathfrak{P}$. Then, in $\mathbb{F}_\mathfrak{P}[X]$,

$$\overline{h} = (X - \overline{\alpha_1})(X - \overline{\alpha_2}) \ldots (X - \overline{\alpha_n}).$$

Let $\overline{A} = \{\overline{\alpha_1}, \ldots, \overline{\alpha_n}\}$. As $\mathrm{disc}(h) \notin \mathfrak{p}$, we have

$$\mathrm{disc}(\overline{h}) = \overline{\mathrm{disc}(h)} \neq 0,$$

and so the roots $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ of $\overline{h}$ are distinct. In other words, the quotient morphism $\mathcal{O}_\mathbb{L} \to \mathbb{F}_\mathfrak{P}$ restricts to a bijection $\pi \colon A \to \overline{A}$. Let ϕ be the Frobenius automorphism $\overline{\beta} \mapsto \overline{\beta}^{N(\mathfrak{p})}$ of the extension $\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p}$. The diagram of bijections

$$\begin{array}{ccc} A & \xrightarrow{\ \pi\ } & \overline{A} \\ {\scriptstyle \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\big|_A}\downarrow & & \downarrow{\scriptstyle \phi|_{\overline{A}}} \\ A & \xrightarrow[\ \pi\ ]{} & \overline{A} \end{array}$$

commutes by the definition of $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$ (Definition 2.25). So, the action of $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$ on A is the same (up to relabelling) as the action of ϕ on $\overline{A}$, and so the cycle types of $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$ and ϕ are the same.

We will think of $\mathbb{F}_{\mathfrak{p}}[X]$ as a subring of $\mathbb{F}_{\mathfrak{P}}[X]$ via the embedding $\mathbb{F}_{\mathfrak{p}} \hookrightarrow \mathbb{F}_{\mathfrak{P}}$ given by $\beta + \mathfrak{p} \mapsto \beta + \mathfrak{P}$. In this sense, $\overline{h} \in \mathbb{F}_{\mathfrak{p}}[X]$ as the coefficients of h are in $\mathcal{O}_{\mathbb{K}}$. Let

$$\overline{h} = \overline{h_1}\,\overline{h_2}\cdots\overline{h_g}$$

be the irreducible factorisation of $\overline{h}$ in $\mathbb{F}_{\mathfrak{p}}[X]$, and let f_i be the degree of $\overline{h_i}$ for each integer i in the range $1 \leqslant i \leqslant g$. By definition, the decomposition type of $\mathfrak{p}$ is the unordered list $f_1, \ldots, f_g$. As the roots $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ are distinct, so are the polynomials $\overline{h_1}, \ldots, \overline{h_g}$.

To show that the cycle type of the action of ϕ on $\overline{A}$ is $f_1, \ldots, f_g$, it suffices to show, for each integer i in the range $1 \leqslant i \leqslant g$, that ϕ permutes the roots of $\overline{h_i}$ in a cycle (the length of which will be f_i). Let $\overline{\alpha}$ be one of the roots of $\overline{h_i}$. The Galois group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ is generated by the Frobenius automorphism ϕ. As $\overline{h_i}$ is an irreducible polynomial in $\mathbb{F}_{\mathfrak{p}}[X]$ which completely splits in $\mathbb{F}_{\mathfrak{P}}$, the Galois group $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ acts on the roots of $\overline{h_i}$ — so $\phi^k(\overline{\alpha})$ is a root of $\overline{h_i}$ for each integer k, and this action is transitive — so each root of $\overline{h_i}$ is of the form $\phi^k(\overline{\alpha})$. Hence the elements of the cycle of $\overline{\alpha}$ under ϕ are precisely the roots of $\overline{h_i}$. □

Remark 2.53. As above (and still assuming that $\overline{h}$ has distinct roots), let

$$\overline{h} = \overline{h_1}\,\overline{h_2}\cdots\overline{h_g}$$

be the irreducible factorisation of $\overline{h}$ in $\mathbb{F}_{\mathfrak{p}}[X]$, and let f_i be the degree of $\overline{h_i}$. Let α be any root of h. Under some extra assumptions (for example, it suffices that $\mathcal{O}_{\mathbb{K}(\alpha)} = \mathcal{O}_{\mathbb{K}}[\alpha]$), the *Dedekind–Kummer theorem* (Theorem 27 in Marcus [28]) says that the prime ideal factorisation of $\mathfrak{p}\mathcal{O}_{\mathbb{K}(\alpha)}$ in $\mathcal{O}_{\mathbb{K}(\alpha)}$ is given by

$$\mathfrak{p}\mathcal{O}_{\mathbb{K}(\alpha)} = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_g,$$

where, for each integer i satisfying $1 \leqslant i \leqslant g$, the prime ideal $\mathfrak{q}_i$ may be defined by

$$\mathfrak{q}_i = \langle \mathfrak{p}, h_i(\alpha) \rangle$$

for any lift h_i of $\overline{h_i}$ to $\mathcal{O}_{\mathbb{K}}[X]$, and $f(\mathfrak{q}_i|\mathfrak{p}) = f_i$. Given an intermediate field $\mathbb{M}$ of the extension $\mathbb{L}/\mathbb{K}$, define the *splitting type* of $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{M}}$ to be the unordered list of the inertial degrees of the prime ideal factors of $\mathfrak{p}\mathcal{O}_{\mathbb{M}}$. The Dedekind–Kummer theorem says that the decomposition type of h modulo $\mathfrak{p}$ and the splitting type of $\mathfrak{p}$ in $\mathcal{O}_{\mathbb{K}(\alpha)}$ are the same. In other words, we may reinterpret the Frobenius density theorem as a statement about how the non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ split in $\mathcal{O}_{\mathbb{K}(\alpha)}$.

We now have everything that we need to deduce the Frobenius density theorem (Theorem 2.49) from Chebotarev's density theorem (Theorem 2.1).

Proof of Theorem 2.49. We have

$$\begin{aligned}
\delta(P) &= \delta\big(\{\mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \text{ of decomposition type } f_1, \dots, f_g\}\big) \\
&= \delta\left(\left\{\mathfrak{p} \in P(\mathbb{K}) : \begin{array}{l} \mathfrak{p} \text{ unramified in } \mathcal{O}_{\mathbb{L}},\ \mathfrak{p} \nmid \langle \mathrm{disc}(h)\rangle, \\ \mathfrak{p} \text{ of decomposition type } f_1, \dots, f_g \end{array}\right\}\right) \\
&= \delta\left(\left\{\mathfrak{p} \in P(\mathbb{K}) : \begin{array}{l} \mathfrak{p} \text{ unramified in } \mathcal{O}_{\mathbb{L}},\ \mathfrak{p} \nmid \langle \mathrm{disc}(h)\rangle, \\ \left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) \text{ of cycle type } f_1, \dots, f_g \end{array}\right\}\right) \\
&= \delta\big(\{\mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \text{ unramified in } \mathcal{O}_{\mathbb{L}},\ \left(\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) \text{ of cycle type } f_1, \dots, f_g\}\big).
\end{aligned}$$

Indeed, the third equality follows from Proposition 2.51. For the second and fourth equalities, note that there are only finitely many prime ideals which are ramified in $\mathcal{O}_{\mathbb{L}}$ (Corollary 2.8), and there are only finitely many prime ideals which divide the $\mathcal{O}_{\mathbb{K}}$-ideal $\langle \mathrm{disc}(h)\rangle$. These equalities follow because the density of a finite set is zero (we will[1] prove this in Corollary 4.35), and the density of a disjoint union is the sum of the densities of the sets in the union (Proposition 2.47).

Recall that C is the set of elements of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ of cycle type $f_1, \dots, f_g$. From our earlier discussion, C is a disjoint union of conjugacy classes of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$, say $C_1, \dots, C_r$. Hence, by Chebotarev's density theorem,

$$\begin{aligned}
\delta(P) &= \sum_{j=1}^{r} \delta\big(\{\mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \text{ unramified in } \mathcal{O}_{\mathbb{L}},\ \left(\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = C_j\}\big) \\
&= \sum_{j=1}^{r} \frac{|C_j|}{|\mathrm{Gal}(\mathbb{L}/\mathbb{K})|} = \frac{|C|}{|\mathrm{Gal}(\mathbb{L}/\mathbb{K})|}.
\end{aligned}$$

□

Remark 2.54. To prove his density theorem, Frobenius actually proved a stronger result, the statement of which is similar to that of Chebotarev's density theorem, except, rather than considering the prime ideals whose Artin symbol is a given conjugacy class of the Galois group, he considered the prime ideals whose Artin symbol is contained in a given *division* of the Galois group. The *division* of an element ϕ of a group G is the union of the conjugacy classes of the generators of $\langle \phi \rangle$. The partition of a group into its conjugacy classes is a refinement of its partition into its divisions, and this refinement can be strict. For example, $\{\sigma, \sigma^{-1}\}$ and $\{\sigma^2, \sigma^{-2}\}$ are different conjugacy classes of $D_5 = \langle \sigma, \tau \mid \sigma^5 = \tau^2 = 1, \sigma\tau\sigma = \tau \rangle$, but $\{\sigma, \sigma^{-1}, \sigma^2, \sigma^{-2}\}$ is a division of D_5. Also, the partition of a subgroup of S_n into its divisions is a refinement of its partition by cycle types, and, again, this refinement can be strict. For example, $(12)(34)$ and $(13)(24)$ have the same cycle type, but $\langle (12)(34) \rangle$ and $\langle (13)(24) \rangle$ are not conjugate subgroups of $V = \{1, (12)(34), (13)(24), (14)(23)\}$. As there are polynomials in $\mathbb{Q}[X]$ with the Galois groups V (e.g. $X^4 + 36X + 63$), and D_5 (e.g. $X^5 - 5X + 12$), the strong version of the Frobenius density theorem is indeed stronger than the version stated earlier, but weaker than Chebotarev's density theorem.

[1] The argument is not circular as the Frobenius density theorem will not be used in later proofs.

Chapter 3

Cyclotomic extensions, ray class groups and Artin reciprocity

Modern proofs of Chebotarev's density theorem use Artin's law of reciprocity, an important result in class field theory, to deduce the abelian case of Chebotarev's theorem, and follow with an argument like ours in Theorem 5.1 to extend the result to an arbitrary extension of number fields. Our proof of Chebotarev's density theorem is more elementary than this, similar in spirit to Chebotarev's original proof. We will show that Chebotarev's density theorem holds for cyclotomic extensions (along the way proving a part of Artin reciprocity for cyclotomic extensions), and then we will deduce the abelian case using a method similar to Chebotarev's field "crossing" argument.

In Section 3.2, we will see that (a stronger version of) Dirichlet's theorem on prime numbers in arithmetic progressions may be stated as a result about the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ where ζ is a primitive m-th root of unity. Seen in this way, it says, for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, that $1/\varphi(m)$ is the density of the set of prime ideals $p\mathbb{Z}$ unramified in $\mathbb{Q}(\zeta)$ whose Artin symbol satisfies $\left(\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p\mathbb{Z}}\right) = \{\sigma\}$. Recall, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ and $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$ is the Euler totient function. It is traditionally proved by considering the behaviour of the *Dirichlet L-functions*

$$L(s,\chi) = \sum_{\substack{n=1 \\ \gcd(n,m)=1}}^{\infty} \frac{\chi(n+m\mathbb{Z})}{n^s}$$

near $s = 1$, which are defined for each character χ of the group $(\mathbb{Z}/m\mathbb{Z})^\times$. The cyclotomic case of Chebotarev's density theorem is a direct generalisation of Dirichlet's theorem on prime numbers in arithmetic progressions to an arbitrary cyclotomic extension of number fields $\mathbb{L}/\mathbb{K}$, that is, one where $\mathbb{L} \subseteq \mathbb{K}(\zeta)$ for some root of unity ζ. For our purposes, the notion of the *ray class group* from class field theory, which we introduce in Section 3.4, is the "correct" generalisation of the group $(\mathbb{Z}/m\mathbb{Z})^\times$, giving us the *Weber L-functions* which we will use in our proof of the cyclotomic case of Chebotarev's density theorem (in the next chapter) in an analogous way to the use of the *Dirichlet L-functions* in the traditional proof of Dirichlet's theorem on prime numbers in arithmetic progressions.

3.1 Cyclotomic extensions

In this section, we review some basic properties of cyclotomic extensions, following Goldstein [15, p. 96].

Let m be a positive integer. An *m-th root of unity* is a root of the polynomial $X^m - 1$ in $\mathbb{C}$. The m-th roots of unity form a cyclic multiplicative group, whose generators are called *primitive* m-th roots of unity. If ζ is a primitive m-th root of unity, then ζ^k is a primitive m-th root of unity if and only if $\gcd(k, m) = 1$.

Definition 3.1. A *cyclotomic extension* is an extension of number fields $\mathbb{L}/\mathbb{K}$ such that $\mathbb{L} \subseteq \mathbb{K}(\zeta)$ for some root of unity $\zeta \in \mathbb{C}$.

Remark 3.2. The other common definition of a cyclotomic extension requires that $\mathbb{L} = \mathbb{K}(\zeta)$ for some root of unity ζ, and thus is more restrictive than our definition. Lang [21], and Fried and Jarden [13], use the same definition as us.

Proposition 3.3. *Let $\mathbb{K}$ be a number field. Let ζ and ζ' be primitive m-th roots of unity. Then $\mathbb{K}(\zeta) = \mathbb{K}(\zeta')$.*

Proof. As ζ is primitive, ζ' is a power of ζ, and so $\zeta' \in \mathbb{K}(\zeta)$. Also $\mathbb{K} \subseteq \mathbb{K}(\zeta)$, so $\mathbb{K}(\zeta') \subseteq \mathbb{K}(\zeta)$. The other inclusion follows by the symmetry of ζ and ζ'. □

We begin by studying the Galois groups of cyclotomic extensions.

Proposition 3.4. *Let $\mathbb{K}$ be a number field, and let $\zeta \in \mathbb{C}$ be a primitive m-th root of unity. Then each $\sigma \in \mathrm{Gal}(\mathbb{K}(\zeta)/\mathbb{K})$ sends ζ to another primitive m-th root of unity, say $\zeta^{k(\sigma)}$ where $0 \leqslant k(\sigma) < m$ and $\gcd\big(k(\sigma), m\big) = 1$, and the map*

$$\iota\colon \mathrm{Gal}(\mathbb{K}(\zeta)/\mathbb{K}) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times, \qquad \sigma \mapsto k(\sigma) + m\mathbb{Z},$$

is an injective group homomorphism.

Proof. Let $\sigma \in \mathrm{Gal}(\mathbb{K}(\zeta)/\mathbb{K})$. Then $\sigma(\zeta)^m = \sigma(\zeta^m) = \sigma(1) = 1$, so $\sigma(\zeta)$ is an m-th root of unity. As ζ is a primitive m-th root of unity, there is a unique integer $k(\sigma)$ in the range $0 \leqslant k(\sigma) < m$ such that $\sigma(\zeta) = \zeta^{k(\sigma)}$. Assume, for a contradiction, that the order n of $\sigma(\zeta)$ is less than m. As $\sigma(\zeta)^n = 1$, we have $\sigma(\zeta^n) = \sigma(1)$, and so $\zeta^n = 1$ because σ is an isomorphism. As the order of ζ is m, and $m > n$, this is a contradiction. Hence $\sigma(\zeta)$ is a primitive m-th root of unity, and it follows that $k(\sigma)$ and m are coprime. So ι does actually map into $(\mathbb{Z}/m\mathbb{Z})^\times$. As each element of $\mathrm{Gal}(\mathbb{K}(\zeta)/\mathbb{K})$ is uniquely determined by where it sends ζ, the map ι is injective. For each $\sigma, \tau \in \mathrm{Gal}(\mathbb{K}(\zeta)/\mathbb{K})$, we have

$$\zeta^{k(\sigma\tau)} = (\sigma\tau)(\zeta) = \sigma\big(\tau(\zeta)\big) = \sigma\big(\zeta^{k(\tau)}\big) = \sigma(\zeta)^{k(\tau)} = \zeta^{k(\sigma)k(\tau)},$$

and so $\iota(\sigma\tau) = \iota(\sigma)\iota(\tau)$ as ζ has order m. Hence ι is a group homomorphism. □

A field extension is *abelian* if it is Galois and its Galois group is abelian.

Corollary 3.5. *All cyclotomic extensions are abelian.*

Proof. Let $\mathbb{L}/\mathbb{K}$ be a cyclotomic extension of number fields. Then $\mathbb{L} \subseteq \mathbb{K}(\zeta)$, where $\zeta \in \mathbb{C}$ is a primitive m-th root of unity for some positive integer m. As all m-th roots of unity are in $\mathbb{K}(\zeta)$ (they are all powers of ζ), $\mathbb{K}(\zeta)$ is the splitting field of $X^m - 1$ over $\mathbb{K}$, and so $\mathbb{K}(\zeta)/\mathbb{K}$ is Galois. By Proposition 3.4, $\mathrm{Gal}(\mathbb{K}(\zeta)/\mathbb{K})$ is isomorphic to a subgroup of the abelian group $(\mathbb{Z}/m\mathbb{Z})^\times$, and thus is itself an abelian group. As all subgroups of an abelian group are normal, the fundamental theorem of Galois theory says that the intermediate extension $\mathbb{L}/\mathbb{K}$ is Galois, and that it is a quotient group of $\mathrm{Gal}(\mathbb{K}(\zeta)/\mathbb{K})$. The latter statement means that $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is abelian. □

Corollary 3.6. *If $\mathbb{K}$ is a number field, and $\zeta \in \mathbb{C}$ is a primitive m-th root of unity, then $[\mathbb{K}(\zeta) : \mathbb{K}] \leqslant \varphi(m)$, where $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$ is Euler's totient function.*

Proof. This holds because $\mathbb{K}(\zeta)/\mathbb{K}$ is Galois and ι is injective. □

The following result is used multiple times in the rest of this section.

Proposition 3.7. *Let $\zeta \in \mathbb{C}$ be a primitive m-th root of unity. Then*

$$\prod_{\substack{0 \leqslant j,k < m \\ j \neq k}} (\zeta^j - \zeta^k) = (-1)^{m-1} m^m.$$

Proof. We have

$$X^m - 1 = \prod_{k=0}^{m-1} (X - \zeta^k). \tag{3.1.1}$$

Differentiating both sides, we get

$$mX^{m-1} = \sum_{i=0}^{m-1} \prod_{\substack{j=0 \\ j \neq i}}^{m-1} (X - \zeta^j).$$

Setting $X = \zeta^k$, it follows that

$$m(\zeta^k)^{m-1} = \prod_{\substack{j=0 \\ j \neq k}}^{m-1} (\zeta^k - \zeta^j).$$

Taking the product of both sides over all integers k in the range $0 \leqslant k < m$, we get

$$m^m \left(\prod_{k=0}^{m-1} \zeta^k \right)^{m-1} = \prod_{\substack{0 \leqslant j,k < m \\ j \neq k}} (\zeta^k - \zeta^j).$$

But, equating the constant terms of (3.1.1), we see that

$$(-1)^{m-1} = \prod_{k=0}^{m-1} \zeta^k.$$

As $a^2 \equiv a \pmod 2$ for all integers a, it follows that

$$m^m \left(\prod_{k=0}^{m-1} \zeta^k \right)^{m-1} = m^m (-1)^{(m-1)^2} = m^m (-1)^{m-1}.$$ □

Proposition 3.8. *Let $\zeta \in \mathbb{C}$ be a primitive m-th root of unity, and let $f \in \mathbb{Z}[X]$ be its minimal polynomial over $\mathbb{Q}$. Then the roots of f in $\mathbb{C}$ are precisely the $\varphi(m)$ primitive m-th roots of unity, and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(m)$.*

Proof. Let $n = [\mathbb{Q}(\zeta) : \mathbb{Q}]$, which is the degree of f. Then $n = |\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})|$ as $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois, and so $n \leqslant \varphi(m)$ by Corollary 3.6.

As $\mathbb{Q}(\zeta)/\mathbb{Q}$ is Galois, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ acts transitively on the roots of f. Thus each root of f is of the form $\sigma(\zeta)$ for some $\sigma \in G$. That is, by Proposition 3.4, each root of f is of the form ζ^j for some integer $j \in \{1, \ldots, m\}$, and so

$$f(X) = \prod_{j \in J} (X - \zeta^j) \tag{3.1.2}$$

for some $J \subseteq \{1, \ldots, m\}$ (the roots of f are distinct as f is irreducible over $\mathbb{Q}$).

We will show that if $f(\zeta^j) = 0$ and p is a prime number not dividing m, then $f(\zeta^{jp}) = 0$. Suppose that $f(\zeta^j) = 0$ and $f(\zeta^{jp}) \neq 0$. By (3.1.2), $f(\zeta^{jp})$ is a subproduct of the product given in Proposition 3.7. In other words, $f(\zeta^{jp})$ divides m^m in $\mathbb{Z}[\zeta]$. However, p divides the polynomial $f(X^p) - f(X)^p$ in $\mathbb{Z}[X]$ (reduce modulo p the expansion of $f(X)^p$ using $\binom{k}{p} \equiv 0 \,(\mathrm{mod}\, p)$, which holds when $0 < k < p$, and then apply $k^p \equiv k \,(\mathrm{mod}\, p)$), and so p divides $f(\zeta^{jp}) - f(\zeta^j)^p = f(\zeta^{jp})$ in $\mathbb{Z}[\zeta]$. Together, this means that p divides m^m in $\mathbb{Z}$, and thus p divides m in $\mathbb{Z}$.

Let a be a positive integer coprime to m. Let $a = p_1 p_2 \cdots p_k$ be the prime factorisation of a (the p_i may not be distinct). Let $a_0 = 1$ and $a_i = a_{i-1} p_i$ for each integer $i \in \{1, \ldots, k\}$, so that $a = a_k$. Clearly $f(\zeta^{a_0}) = f(\zeta) = 0$. If $f(\zeta^{a_{i-1}}) = 0$, then the previous paragraph implies that $f(\zeta^{a_i}) = f(\zeta^{a_{i-1} p_i}) = 0$. By induction, $f(\zeta^a) = 0$. It follows that all $\varphi(m)$ primitive m-th roots of unity are roots of f, and so $n \geqslant \varphi(m)$. Hence $n = \varphi(m)$, and these are precisely the roots of f. □

Corollary 3.9. *If $\mathbb{K} = \mathbb{Q}$, the map ι from Proposition 3.4 is an isomorphism.*

Proof. As ι is injective and $|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = |(\mathbb{Z}/m\mathbb{Z})^\times|$, ι is surjective. □

Proposition 3.10. *Let m and n be coprime positive integers, and let ζ_m, ζ_n and ζ_{mn} be primitive m-th, n-th, and (mn)-th roots of unity respectively. Then*

$$\mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_{mn}) \qquad \textit{and} \qquad \mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}.$$

Proof. As ζ_m and ζ_n are both mn-th roots of unity, $\mathbb{Q}(\zeta_m, \zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$. We now show the other inclusion. As ζ_{mn}^m is a n-th root of unity, $\zeta_{mn}^m = \zeta_n^k$ for some integer k. Similarly, $\zeta_{mn}^n = \zeta_m^j$ for some integer j. By Bézout's theorem, there are integers u and v such that $um + nv = \gcd(m, n) = 1$. Hence

$$\zeta_{mn} = (\zeta_{mn}^m)^u (\zeta_{mn}^n)^v = (\zeta_n^k)^u (\zeta_m^j)^v \in \mathbb{Q}(\zeta_m, \zeta_n),$$

and so $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_m, \zeta_n)$.

As m and n are coprime, $\varphi(mn) = \varphi(m)\varphi(n)$. We have

$$[\mathbb{Q}(\zeta_m, \zeta_n) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \varphi(mn) = \varphi(m)\varphi(n) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]\,[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$$

by Proposition 3.8, and so $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ by Proposition 2.11. □

We now study the ramification of prime ideals in cyclotomic extensions.

Lemma 3.11. *Let $\zeta \in \mathbb{C}$ be a primitive m-th root of unity. Suppose that p is a prime number such that $p\mathbb{Z}$ ramifies in $\mathcal{O}_{\mathbb{Q}(\zeta)}$. Then p divides m.*

Proof. Let $n = [\mathbb{Q}(\zeta) : \mathbb{Q}]$, and let $\sigma_1, \ldots, \sigma_n$ be the elements of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. From the discussion in Section 2.1.5, we have the following. First, p divides $\mathrm{disc}\big(\mathbb{Q}(\zeta)\big)$. Second, as $1, \zeta, \ldots, \zeta^{n-1}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta)$ consisting of algebraic integers, $\mathrm{disc}\big(\mathbb{Q}(\zeta)\big)$ divides $\mathrm{disc}_{\mathbb{Q}(\zeta)}(1, \zeta, \ldots, \zeta^{n-1})$. Finally,

$$\mathrm{disc}_{\mathbb{Q}(\zeta)}(1, \zeta, \ldots, \zeta^{n-1}) = \prod_{\substack{1 \leqslant j,k \leqslant n \\ j \neq k}} \big(\sigma_j(\zeta) - \sigma_k(\zeta)\big).$$

By Proposition 3.7, this last product divides $(-1)^{m-1}m^m$. Putting this all together, p divides $(-1)^{m-1}m^m$, and thus p divides m as p is prime. □

The next result generalises the above lemma to arbitrary cyclotomic extensions.

Proposition 3.12. *Let $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}(\zeta)$ be a tower of number fields, where $\zeta \in \mathbb{C}$ is a primitive m-th root of unity. Suppose that $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_{\mathbb{K}}$ which is ramified in $\mathcal{O}_{\mathbb{L}}$. Then $\mathfrak{p}$ divides $m\mathcal{O}_{\mathbb{K}}$.*

To prove this proposition, we need the following result, which we will use to relate the inertia groups of $\mathbb{K}(\zeta)/\mathbb{K}$ with those of $\mathbb{Q}(\zeta)/\mathbb{Q}$. Recall Proposition 2.9: if $\mathbb{M}_1$ and $\mathbb{M}_2$ are number fields with a common subfield $\mathbb{F}$, and $\mathbb{M}_1/\mathbb{F}$ is Galois, then $\mathbb{M}_1\mathbb{M}_2/\mathbb{M}_2$ is also Galois and the map $\phi\colon \mathrm{Gal}(\mathbb{M}_1\mathbb{M}_2/\mathbb{M}_2) \to \mathrm{Gal}(\mathbb{M}_1/\mathbb{F})$ given by $\sigma \mapsto \sigma|_{\mathbb{M}_1}$ is injective.

Lemma 3.13. *Assume the notation from the previous paragraph. Let $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}_{\mathbb{M}_1\mathbb{M}_2}$, and let $\mathfrak{p}$, $\mathfrak{Q}$ and $\mathfrak{q}$ be the prime ideals under $\mathfrak{P}$ of $\mathcal{O}_{\mathbb{M}_2}$, $\mathcal{O}_{\mathbb{M}_1}$ and $\mathcal{O}_{\mathbb{F}}$ respectively. Then $\phi\big(I(\mathfrak{P}|\mathfrak{p})\big) \subseteq I(\mathfrak{Q}|\mathfrak{q})$.*

Proof. Let $\sigma \in I(\mathfrak{P}|\mathfrak{p})$, and let $\alpha \in \mathcal{O}_{\mathbb{M}_1}$. By the definition of $I(\mathfrak{P}|\mathfrak{p})$, $\sigma(\alpha) - \alpha \in \mathfrak{P}$. But as $\sigma|_{\mathbb{M}_1} \in \mathrm{Gal}(\mathbb{M}_1/\mathbb{F})$, $\sigma(\alpha)$ is also in $\mathcal{O}_{\mathbb{M}_1}$. Hence $\sigma(\alpha) - \alpha \in \mathfrak{P} \cap \mathcal{O}_{\mathbb{M}_1} = \mathfrak{Q}$. As this holds for all $\alpha \in \mathcal{O}_{\mathbb{M}_1}$, $\sigma|_{\mathbb{M}_1} \in I(\mathfrak{Q}|\mathfrak{q})$ by the definition of $I(\mathfrak{Q}|\mathfrak{q})$. □

Proof of Proposition 3.12. As $\mathfrak{p}$ is ramified in $\mathcal{O}_{\mathbb{L}}$, it is also ramified in $\mathcal{O}_{\mathbb{K}(\zeta)}$ (Proposition 2.5), so there is a prime ideal $\mathfrak{P}$ of $\mathcal{O}_{\mathbb{K}(\zeta)}$ above $\mathfrak{p}$ with $e(\mathfrak{P}|\mathfrak{p}) > 1$. Let $\mathfrak{Q}$ and $q\mathbb{Z}$ be the prime ideals under $\mathfrak{P}$ of $\mathcal{O}_{\mathbb{Q}(\zeta)}$ and $\mathbb{Z}$ respectively. Setting $\mathbb{F} = \mathbb{Q}$, $\mathbb{M}_1 = \mathbb{Q}(\zeta)$ and $\mathbb{M}_2 = \mathbb{K}$ in the lemma, we get $\phi\big(I(\mathfrak{P}|\mathfrak{p})\big) \subseteq I(\mathfrak{Q}|q\mathbb{Z})$, and so

$$e(\mathfrak{Q}|q\mathbb{Z}) = |I(\mathfrak{Q}|q\mathbb{Z})| \geqslant |I(\mathfrak{P}|\mathfrak{p})| = e(\mathfrak{P}|\mathfrak{p}) > 1$$

because ϕ is injective. Hence $q\mathbb{Z}$ is ramified in $\mathcal{O}_{\mathbb{Q}(\zeta)}$. By Lemma 3.11, q divides m. As $\mathfrak{p}$ divides $q\mathcal{O}_{\mathbb{K}}$, it follows that $\mathfrak{p}$ divides $m\mathcal{O}_{\mathbb{K}}$. □

3.2 Dirichlet's theorem on prime numbers in arithmetic progressions

In this section, we will explain how Dirichlet's theorem on prime numbers in arithmetic progressions is a special case of Chebotarev's density theorem. We begin with a statement of Dirichlet's theorem.

Theorem 3.14 (Dirichlet's theorem)**.** *Let a and m be coprime integers, and let*

$$P_a = \{p\mathbb{Z} : \ p \text{ is a prime number}, p \equiv a \,(mod\, m)\}.$$

Then the Dirichlet density of the set P_a exists, and satisfies

$$\delta(P_a) = \frac{1}{\varphi(m)},$$

where $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times|$ is Euler's totient function.

Remark 3.15. Our statement here is stronger than the one that Dirichlet actually proved, stated in Chapter 1, which only claimed that P_a is infinite. Example 2.2 provides empirical evidence for the particular instance of this result where $m = 10$.

The key to relating Dirichlet and Chebotarev's theorems is the following result.

Proposition 3.16. *Let $\mathbb{K}$ be a number field, and let ζ be a primitive m-th root of unity. Let $\iota\colon \mathrm{Gal}(\mathbb{K}(\zeta)/\mathbb{K}) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ be the map from Proposition 3.4. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_\mathbb{K}$ not dividing $m\mathcal{O}_\mathbb{K}$. Then $N(\mathfrak{p})$ is coprime to m and*

$$\iota\left(\left[\tfrac{\mathbb{K}(\zeta)/\mathbb{K}}{\mathfrak{p}}\right]\right) = N(\mathfrak{p}) + m\mathbb{Z}.$$

Remark 3.17. For $\left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\mathfrak{p}}\right]$ to be defined, we need $\mathfrak{p}$ to be unramified in $\mathcal{O}_{\mathbb{K}(\zeta)}$ (Remark 2.30). This is true, by Proposition 3.12, because $\mathfrak{p}$ does not divide $m\mathcal{O}_\mathbb{K}$.

To prove the proposition, we need the following lemma.

Lemma 3.18. *Let $\mathbb{K}$ be a number field, and let $\zeta \in \mathbb{C}$ be a primitive m-th root of unity. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}(\zeta)}$ not dividing $m\mathcal{O}_{\mathbb{K}(\zeta)}$. Then*

$$\zeta^k \equiv \zeta^j \,(mod \mathfrak{P}) \quad \text{if and only if} \quad \zeta^k = \zeta^j.$$

Proof. The "if" direction is clear. Conversely, suppose that $\zeta^k \equiv \zeta^j \,(\mathrm{mod}\,\mathfrak{P})$ and assume, for a contradiction, that $\zeta^k \neq \zeta^j$. From Proposition 3.7, we know that that $\zeta^j - \zeta^k$ divides m^m in $\mathcal{O}_{\mathbb{K}(\zeta)}$, and so $m^m \equiv 0 \,(\mathrm{mod}\,\mathfrak{P})$. This means that $m^m \in \mathfrak{P}$, so $m^m\mathcal{O}_{\mathbb{K}(\zeta)} \subseteq \mathfrak{P}$, and thus $\mathfrak{P}$ divides $m^m\mathcal{O}_{\mathbb{K}(\zeta)}$. But $m^m\mathcal{O}_{\mathbb{K}(\zeta)} = (m\mathcal{O}_{\mathbb{K}(\zeta)})^m$ and $\mathfrak{P}$ is a prime ideal, so $\mathfrak{P}$ actually divides $m\mathcal{O}_{\mathbb{K}(\zeta)}$, contradicting our choice of $\mathfrak{P}$. □

Proof of Proposition 3.16. Let $\mathfrak{P}$ be any prime ideal of $\mathcal{O}_{\mathbb{K}(\zeta)}$ lying above $\mathfrak{p}$. Then $\left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\mathfrak{p}}\right] = \left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\mathfrak{P}}\right]$. From Proposition 2.26, we know that

$$\left[\tfrac{\mathbb{K}(\zeta)/\mathbb{K}}{\mathfrak{P}}\right](\zeta) \equiv \zeta^{N(\mathfrak{p})} \,(\mathrm{mod}\,\mathfrak{P}).$$

But $\left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\mathfrak{P}}\right](\zeta)$ is an m-th root of unity (Proposition 3.4), and $\zeta^{N(\mathfrak{p})}$ is also an m-th root of unity. So long as $\mathfrak{P}$ does not divide $m\mathcal{O}_{\mathbb{K}(\zeta)}$, Lemma 3.18 implies that $\left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\mathfrak{P}}\right](\zeta) = \zeta^{N(\mathfrak{p})}$, and the result follows. Assume that $\mathfrak{P}$ divides $m\mathcal{O}_{\mathbb{K}(\zeta)}$. Then $m\mathcal{O}_{\mathbb{K}(\zeta)} \subseteq \mathfrak{P}$, and so $m\mathcal{O}_\mathbb{K} \subseteq m\mathcal{O}_{\mathbb{K}(\zeta)} \cap \mathcal{O}_\mathbb{K} \subseteq \mathfrak{P} \cap \mathcal{O}_\mathbb{K} = \mathfrak{p}$. This means that $\mathfrak{p}$ divides $m\mathcal{O}_\mathbb{K}$, contradicting our choice of $\mathfrak{p}$. □

The following result is a corollary to Proposition 3.16. Here, P_a is the set defined in Theorem 3.14, and $\iota\colon \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \to (\mathbb{Z}/m\mathbb{Z})^\times$ is the embedding defined in Proposition 3.4. Recall that ι is actually an isomorphism (Corollary 3.9).

Corollary 3.19. *Let ζ be a primitive m-th root of unity. Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, and let a be the integer coprime to m such that $\iota(\sigma) = a + m\mathbb{Z}$. Then the set*

$$P_\sigma = \left\{p\mathbb{Z} :\ p \text{ is a prime number}, p \nmid m, \left[\tfrac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p\mathbb{Z}}\right] = \sigma\right\}$$

and the set P_a are equal.

Proof. If $p \equiv a \pmod m$, then p does not divide m as a and m are coprime. Let p be a prime number not dividing m. As ι is an isomorphism (Corollary 3.9), $\left[\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p\mathbb{Z}}\right] = \sigma$ if and only if $\iota(\left[\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p\mathbb{Z}}\right]) = \iota(\sigma)$. But $\iota(\left[\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p\mathbb{Z}}\right]) = N(p\mathbb{Z}) + m\mathbb{Z} = p + m\mathbb{Z}$, and $\iota(\sigma) = a + m\mathbb{Z}$, so $\iota(\left[\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p\mathbb{Z}}\right]) = \iota(\sigma)$ if and only if $p \equiv a \pmod m$. □

In Chapter 4, we will show that Chebotarev's density theorem holds for cyclotomic extensions (Theorem 4.36), and also that finite sets of primes have Dirichlet density zero (Corollary 4.35). Using these results[1], we may now prove Dirichlet's theorem on prime numbers in arithmetic progressions.

Proof of Theorem 3.14. As $P_a = P_\sigma$ where $\sigma = \iota^{-1}(a + m\mathbb{Z})$ (Corollary 3.19), it suffices to show that $\delta(P_\sigma) = 1/\varphi(m)$. Let

$$P'_\sigma = \left\{p\mathbb{Z} \in P(\mathbb{Q}) :\ p\mathbb{Z} \text{ is unramified in } \mathcal{O}_{\mathbb{Q}(\zeta)}, \left[\tfrac{\mathbb{Q}(\zeta)/\mathbb{Q}}{p\mathbb{Z}}\right] = \sigma\right\}.$$

Chebotarev's density theorem for the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ says that the Dirichlet density $\delta(P'_\sigma)$ exists and equals $1/|\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})| = 1/\varphi(m)$. Now $P_\sigma \subseteq P'_\sigma$ by Proposition 3.12. Also, $P'_\sigma \backslash P_\sigma$ is finite because only finitely many primes divide m, so $\delta(P'_\sigma \backslash P_\sigma) = 0$ by Corollary 4.35. From Proposition 2.47, as $\delta(P'_\sigma)$ and $\delta(P'_\sigma \backslash P_\sigma)$ exist, so does $\delta(P_\sigma)$, and $\delta(P'_\sigma) = \delta(P_\sigma) + \delta(P'_\sigma \backslash P_\sigma)$. Hence $1/\varphi(m) = \delta(P_\sigma)$. □

3.3 The Artin map and cyclotomic extensions

Recall that $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]$ was defined in the case that $\mathbb{L}/\mathbb{K}$ is an abelian extension of number fields and that $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_\mathbb{K}$ that is unramified in $\mathcal{O}_\mathbb{L}$ (Remark 2.30). Also recall that $\mathcal{I}_\mathbb{K}$, the group of non-zero fractional ideals of $\mathcal{O}_\mathbb{K}$, is generated freely by the non-zero prime ideals of $\mathcal{O}_\mathbb{K}$.

Definition 3.20. For each non-zero ideal $\mathfrak{m}$ of $\mathcal{O}_\mathbb{K}$, let $\mathcal{I}_\mathbb{K}^\mathfrak{m}$ denote the subgroup of $\mathcal{I}_\mathbb{K}$ generated by those prime ideals not dividing $\mathfrak{m}$ (i.e. the group of non-zero fractional ideals coprime to $\mathfrak{m}$). Then, provided that all non-zero prime ideals of $\mathcal{O}_\mathbb{K}$ which are ramified in $\mathcal{O}_\mathbb{L}$ divide $\mathfrak{m}$, there is a unique group homomorphism

$$\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_\mathfrak{m} : \mathcal{I}_\mathbb{K}^\mathfrak{m} \to \mathrm{Gal}(\mathbb{L}/\mathbb{K})$$

which agrees with $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]$ on the prime ideals in $\mathcal{I}_\mathbb{K}^\mathfrak{m}$. We call $\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_\mathfrak{m}$ the *Artin map* (or *reciprocity map*) of the extension $\mathbb{L}/\mathbb{K}$ for the modulus $\mathfrak{m}$.

[1] There is no circular argument here as we will not use Dirichlet's theorem on prime numbers in arithmetic progressions until Chapter 6.

Proposition 3.21. *Let $\mathbb{L}/\mathbb{K}$ be an abelian extension of number fields, and let $\mathbb{M}$ be an intermediate field of this extension. Let $r\colon \mathrm{Gal}(\mathbb{L}/\mathbb{K}) \to \mathrm{Gal}(\mathbb{M}/\mathbb{K})$ denote the restriction homomorphism $\sigma \mapsto \sigma|_{\mathbb{M}}$. Let $\mathfrak{m}$ be a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$ divisible by all of the non-zero prime ideals of $\mathcal{O}_{\mathbb{K}}$ which are ramified in $\mathcal{O}_{\mathbb{L}}$. Then*

$$r \circ \left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}} = \left[\frac{\mathbb{M}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}.$$

Remark 3.22. The map r is well defined because the extension $\mathbb{M}/\mathbb{K}$ is Galois. The map $\left[\frac{\mathbb{M}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}$ is defined because the extension $\mathbb{M}/\mathbb{K}$ is abelian (by the fundamental theorem of Galois theory) and $\mathfrak{p}$ is unramified in $\mathcal{O}_{\mathbb{M}}$ (Proposition 2.5).

Proof. In Proposition 2.31, we saw, for all non-zero prime ideals $\mathfrak{p}$ not dividing $\mathfrak{m}$, that $r(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]) = \left[\frac{\mathbb{M}/\mathbb{K}}{\mathfrak{p}}\right]$. These prime ideals generate $\mathcal{I}_{\mathbb{K}}^{\mathfrak{m}}$, and $\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}$, $\left[\frac{\mathbb{M}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}$ and r are group homomorphisms, so the result follows. □

We return now to considering cyclotomic extensions. Let $\mathbb{K}$ be a number field, let ζ be a primitive m-th root of unity, and let $\mathfrak{m}$ be a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$ that is divisible by $m\mathcal{O}_{\mathbb{K}}$. In Proposition 3.16, we showed, for all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ not dividing $\mathfrak{m}$, that $N(\mathfrak{p})$ is coprime to m and

$$\iota(\left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\mathfrak{p}}\right]) = N(\mathfrak{p}) + m\mathbb{Z}. \tag{3.3.1}$$

Let $\pi\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the quotient ring homomorphism. As the ideal norm N is multiplicative on ideals, so is $\pi \circ N$. As $\pi \circ N$ maps the prime ideals in $\mathcal{I}_{\mathbb{K}}^{\mathfrak{m}}$ into the group $(\mathbb{Z}/m\mathbb{Z})^{\times}$ and $\pi \circ N$ is multiplicative, $\pi \circ N$ actually maps all ideals in $\mathcal{I}_{\mathbb{K}}^{\mathfrak{m}}$ into $(\mathbb{Z}/m\mathbb{Z})^{\times}$. Hence, there is a unique group homomorphism

$$\overline{N}\colon \mathcal{I}_{\mathbb{K}}^{\mathfrak{m}} \to (\mathbb{Z}/m\mathbb{Z})^{\times}$$

which agrees with $\pi \circ N$ on all ideals in $\mathcal{I}_{\mathbb{K}}^{\mathfrak{m}}$. We will refer to $\overline{N}$ as the *reduced ideal norm*. Using the uniqueness properties defining $\left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}$ and $\overline{N}$, and the fact that ι is a group homomorphism, (3.3.1) becomes

$$\iota \circ \left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}} = \overline{N}. \tag{3.3.2}$$

This equation will play an important role in Section 3.4 when we prove a part of Artin reciprocity for cyclotomic extensions.

Example 3.23. Let us illustrate the theory above by considering the particular case where $\mathbb{K} = \mathbb{Q}$ and $\mathfrak{m} = m\mathbb{Z}$. The map $\overline{N}$ is surjective. Indeed, given some congruence class $K \in (\mathbb{Z}/m\mathbb{Z})^{\times}$, there is a positive integer a such that $K = a + m\mathbb{Z}$, and $\overline{N}(a\mathbb{Z}) = a + m\mathbb{Z} = K$. Hence, the map $\overline{N}$ descends to an isomorphism

$$\overline{\overline{N}}\colon \mathcal{I}_{\mathbb{Q}}^{m\mathbb{Z}}/\ker(\overline{N}) \to (\mathbb{Z}/m\mathbb{Z})^{\times}$$

by the first isomorphism theorem. We claim that $\ker(\overline{N})$ is equal to the set

$$\mathcal{P}_{\mathbb{K}}^{m\mathbb{Z}} = \left\{\mathfrak{a} \in \mathcal{I}_{\mathbb{Q}} :\ \exists r, s \in \mathbb{Z}^{+}.\, \mathfrak{a} = \tfrac{r}{s}\mathbb{Z},\ r \equiv s \equiv 1 \,(\mathrm{mod}\, m)\right\}.$$

We begin by showing that $\mathcal{P}_{\mathbb{K}}^{m\mathbb{Z}} \subseteq \ker(\overline{N})$. If $\mathfrak{a} \in \mathcal{P}_{\mathbb{K}}^{m\mathbb{Z}}$, then there are $r, s \in \mathbb{Z}^+$ such that $\mathfrak{a} = \frac{r}{s}\mathbb{Z}$ and $r \equiv s \equiv 1 \pmod{m}$. We have that $\mathfrak{a} \in \ker(\overline{N})$ because

$$\overline{N}(\mathfrak{a}) = (r + m\mathbb{Z})(s + m\mathbb{Z})^{-1} = (1 + m\mathbb{Z})(1 + m\mathbb{Z})^{-1} = 1 + m\mathbb{Z}.$$

We now show the other inclusion. Let $\mathfrak{a} \in \ker(\overline{N})$. As $\mathfrak{a} \in \mathcal{I}_{\mathbb{Q}}^{m\mathbb{Z}}$, and $\mathbb{Z}$ is a principal ideal domain, there are $a, b \in \mathbb{Z}^+$, both coprime with m, such that $\mathfrak{a} = \frac{a}{b}\mathbb{Z}$. As $\mathfrak{a} \in \ker(\overline{N})$, we have $1 + m\mathbb{Z} = \overline{N}(\mathfrak{a}) = (a + m\mathbb{Z})(b + m\mathbb{Z})^{-1}$, and so $a \equiv b \pmod{m}$. Let $t \in \mathbb{Z}^+$ be an inverse of b modulo m. Then $at \equiv bt \equiv 1 \pmod{m}$. Set $r = at$ and $s = bt$. As r and s are positive integers, and $\frac{r}{s}\mathbb{Z} = \frac{at}{bt}\mathbb{Z} = \frac{a}{b}\mathbb{Z} = \mathfrak{a}$, and $r \equiv s \equiv 1 \pmod{m}$, we may conclude that $\mathfrak{a} \in \mathcal{P}_{\mathbb{K}}^{m\mathbb{Z}}$.

As $\mathbb{K}$ is now $\mathbb{Q}$, Corollary 3.9 says that ι is an isomorphism. This means that

$$\ker(\left[\tfrac{\mathbb{Q}(\zeta)/\mathbb{Q}}{\cdot}\right]_{m\mathbb{Z}}) = \ker(\overline{N}) = \mathcal{P}_{\mathbb{K}}^{m\mathbb{Z}},$$

and also that $\left[\frac{\mathbb{Q}(\zeta)/\mathbb{Q}}{\cdot}\right]_{m\mathbb{Z}}$ descends to an isomorphism

$$\overline{\left[\tfrac{\mathbb{Q}(\zeta)/\mathbb{Q}}{\cdot}\right]_{m\mathbb{Z}}} : \mathcal{I}_{\mathbb{Q}}^{m\mathbb{Z}}/\mathcal{P}_{\mathbb{K}}^{m\mathbb{Z}} \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$$

which satisfies

$$\iota \circ \overline{\left[\tfrac{\mathbb{Q}(\zeta)/\mathbb{Q}}{\cdot}\right]_{m\mathbb{Z}}} = \overline{\overline{N}}.$$

Remark 3.24. The *ray class groups* arise by trying to generalise the scenario in Example 3.23 to extensions other than $\mathbb{Q}(\zeta)/\mathbb{Q}$. As we will see in the next section, the group $\mathcal{I}_{\mathbb{Q}}^{m\mathbb{Z}}/\mathcal{P}_{\mathbb{K}}^{m\mathbb{Z}}$ is the *narrow ray class group* of $\mathbb{Q}$ for the modulus $\mathfrak{m}$.

3.4 Ray class groups and Artin reciprocity

We begin this section by motivating the study of *ray class groups* (in a similar way to Section 21.2 of Sutherland [30]). There is a special relationship between the group $(\mathbb{Z}/m\mathbb{Z})^\times$ and the field $\mathbb{Q}$. Building on what we saw in the earlier sections of this chapter, we can say the following (where ζ_m is a primitive m-th root of unity):

- **Existence:** For each integer m, the field $\mathbb{Q}(\zeta_m)$ is an abelian extension of $\mathbb{Q}$, whose ramified primes are those which divide m, and for which

$$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times.$$

- **Completeness:** If $\mathbb{K}/\mathbb{Q}$ is an abelian extension, then $\mathbb{K}$ is contained in a field $\mathbb{Q}(\zeta_m)$. This is the well-known Kronecker–Weber theorem. We will not use this result in our proof of Chebotarev's density theorem.
- **Reciprocity:** If $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{Q}(\zeta_m)$, then $\mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ is isomorphic to a quotient of $(\mathbb{Z}/m\mathbb{Z})^\times$. Although this particular case of reciprocity may be deduced from the fundamental theorem of Galois theory ($\mathbb{Q}(\zeta_m)/\mathbb{Q}$ is abelian); in general, reciprocity is actually a statement about the Artin map (see Remark 3.37).

In the language of *class field theory*, we say that $m\mathbb{Z}$ is a *modulus* of $\mathbb{Q}$, the group $(\mathbb{Z}/m\mathbb{Z})^\times$ is the *ray class group* of $\mathbb{Q}$ for the modulus $m\mathbb{Z}$, and $\mathbb{Q}(\zeta_m)$ is the *ray class field* of $\mathbb{Q}$ of modulus $m\mathbb{Z}$. A central focus of *global class field theory* is the generalisation of the statements above to number fields other than $\mathbb{Q}$, and in the

course of our proof of the cyclotomic case of Chebotarev's density theorem we will see part of this generalisation. In this section, we will define the notions of a *modulus* and a *ray class group* for an arbitrary number field, generalising the corresponding formulation for $\mathbb{Q}$ and $m\mathbb{Z}$ that we saw in Example 3.23. Our treatment is inspired by Section 21.3 of Sutherland [30], although our simpler (equivalent) definition of the *ray class group* is closer to the definitions given by Weber, Takagi and Hasse in the terminology of the 1920s [12, p. 38]. We will also explain what Artin reciprocity is, and prove a part of Artin reciprocity for cyclotomic extensions.

The construction of the ray class group is similar to the construction of the well-known *ideal class group* of a number field, the latter first encountered in many undergraduate introductory algebraic number theory courses as a means to measure the degree to which the ring of integers of an algebraic number field fails to be a principal ideal domain.

Definition/Proposition 3.25 ([21, VI, §1])**.** Let $\mathbb{K}$ be a number field. Let $\mathcal{I}_\mathbb{K}$ be the multiplicative group of non-zero fractional ideals of $\mathcal{O}_\mathbb{K}$. Let $\mathcal{P}_\mathbb{K} \subseteq \mathcal{I}_\mathbb{K}$ be the (normal) subgroup of principal fractional ideals. Then the quotient group $\mathrm{Cl}_\mathbb{K} = \mathcal{I}_\mathbb{K}/\mathcal{P}_\mathbb{K}$ is called the *ideal class group of* $\mathbb{K}$. It is a finite group, whose order $h_\mathbb{K}$ is called the *class number* of $\mathbb{K}$.

Remark 3.26. By *embedding*, we mean an injective ring homomorphism. Recall that a number field $\mathbb{K}$ has exactly $n = [\mathbb{K} : \mathbb{Q}]$ embeddings in $\mathbb{C}$. If σ is such an embedding, then so is its complex conjugate $\overline{\sigma}$. Hence $n = r + 2s$ where r is the number of *real embeddings of* $\mathbb{K}$ (i.e. embeddings of $\mathbb{K}$ in $\mathbb{C}$ whose image is contained in $\mathbb{R}$) and $2s$ is the number of *complex embeddings of* $\mathbb{K}$ (i.e. embeddings of $\mathbb{K}$ in $\mathbb{C}$ which are not real embeddings).

Definition 3.27 (Modulus)**.** Let $\mathbb{K}$ be a number field. A *modulus* (or *cycle*) $\mathfrak{m}$ of $\mathbb{K}$ consists of a non-zero ideal $\mathfrak{m}_0$ of $\mathcal{O}_\mathbb{K}$, and a subset $\mathfrak{m}_\infty$ of the real embeddings of $\mathbb{K}$. We write the modulus $\mathfrak{m}$ as a formal product $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$.

Definition/Proposition 3.28 (Ray class group)**.** Let $\mathbb{K}$ be a number field, and let $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ be a modulus of $\mathbb{K}$. Define the following groups:

- $\mathcal{I}_\mathbb{K}^\mathfrak{m}$ is the subgroup of $\mathcal{I}_\mathbb{K}$ generated by the non-zero ideals coprime to $\mathfrak{m}_0$.
- $\mathcal{O}_\mathbb{K}^\mathfrak{m} = \{\alpha \in \mathcal{O}_\mathbb{K} \backslash \{0\} : \ \alpha \equiv 1 \,(\mathrm{mod}\, \mathfrak{m}_0)$, and $\sigma(\alpha) > 0$ for all $\sigma \in \mathfrak{m}_\infty\} \subseteq \mathbb{K}^\times$.
- $\mathbb{K}^\mathfrak{m}$ is the subgroup of $\mathbb{K}^\times$ generated by the set $\mathcal{O}_\mathbb{K}^\mathfrak{m}$.
- $\mathcal{P}_\mathbb{K}^\mathfrak{m} = \{\mathfrak{a} \in \mathcal{I}_\mathbb{K}^\mathfrak{m} : \ \mathfrak{a} = \alpha\mathcal{O}_\mathbb{K}$ for some $\alpha \in \mathbb{K}^\mathfrak{m}\} \trianglelefteq \mathcal{I}_\mathbb{K}^\mathfrak{m}$.

The *ray class group* of $\mathbb{K}$ for the modulus $\mathfrak{m}$ is the quotient group

$$\mathrm{Cl}_\mathbb{K}^\mathfrak{m} = \mathcal{I}_\mathbb{K}^\mathfrak{m}/\mathcal{P}_\mathbb{K}^\mathfrak{m}.$$

Proof. The set $\mathcal{P}_\mathbb{K}^\mathfrak{m}$ is a subgroup of $\mathcal{I}_\mathbb{K}^\mathfrak{m}$ because $\mathbb{K}^\mathfrak{m}$ is a group, and a product of principal fractional ideals is the principal fractional ideal generated by the product of the generators. As $\mathcal{I}_\mathbb{K}^\mathfrak{m}$ is abelian, $\mathcal{P}_\mathbb{K}^\mathfrak{m}$ is trivially a normal subgroup. □

Remark 3.29. In the previous section, the group $\mathcal{I}_\mathbb{K}^\mathfrak{m}$ was defined for non-zero ideals $\mathfrak{m}$ of $\mathcal{O}_\mathbb{K}$. The new definition is only dependent on the ideal part of the modulus, so there should be no ambiguity as to what we mean by $\mathcal{I}_\mathbb{K}^\mathfrak{m}$, regardless of whether $\mathfrak{m}$ is an ideal or a modulus.

Remark 3.30. We say that a subset S of a group G is *multiplicative* if $1_G \in S$ and S is closed under multiplication. It is easy to show that if S is a multiplicative subset of an abelian group G, then the subgroup of G generated by S is given by

$$\langle S \rangle = \{g \in G : \ g = s^{-1}s' \text{ for some } s, s' \in S\}.$$

In the above proposition, the set of non-zero ideals coprime to $\mathfrak{m}_0$ is a multiplicative subset of $\mathcal{I}_{\mathbb{K}}$ (by their prime ideal factorisations), and the set $\mathcal{O}_{\mathbb{K}}^{\mathfrak{m}}$ is also a multiplicative subset of $\mathbb{K}^\times$. As $\mathcal{I}_{\mathbb{K}}$ and $\mathbb{K}^\times$ are abelian groups, it follows that:

$$\mathcal{I}_{\mathbb{K}}^{\mathfrak{m}} = \{\mathfrak{a} \in \mathcal{I}_{\mathbb{K}} : \ \mathfrak{a} = \mathfrak{b}\mathfrak{c}^{-1} \text{ for some } \mathfrak{b}, \mathfrak{c} \trianglelefteq \mathcal{O}_{\mathbb{K}} \text{ coprime to } \mathfrak{m}_0\},$$
$$\mathbb{K}^{\mathfrak{m}} = \{\alpha \in \mathbb{K}^\times : \ \alpha = \beta\gamma^{-1} \text{ for some } \beta, \gamma \in \mathcal{O}_{\mathbb{K}}^{\mathfrak{m}}\}.$$

Remark 3.31. The notation for the various sets and groups introduced in Definition/Proposition 3.28 varies between authors, especially with regards to the subscripts and superscripts. Our notation is inspired by Definition 21.2 of Sutherland [30]. There are two common alternate (equivalent) definitions for the subgroup $\mathbb{K}^{\mathfrak{m}}$ of $\mathbb{K}^\times$ (see §1 of Chapter VI in Lang [21] and Definition 21.2 of Sutherland [30]).

Remark 3.32. The elements of $\mathrm{Cl}_{\mathbb{K}}$ are called *ideal classes*; similarly, we will refer to the elements of $\mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}}$ as *ray classes* modulo $\mathfrak{m}$.

Remark 3.33. We will denote the set of all real embeddings of a number field $\mathbb{K}$ by ∞. If $\mathfrak{m}_0$ is a non-zero ideal of $\mathcal{O}_{\mathbb{K}}$, then $\mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}_0 \cdot \infty}$ is called the *narrow ray class group* of $\mathbb{K}$ for the modulus $\mathfrak{m}_0$ (technically, the modulus is $\mathfrak{m}_0 \cdot \infty$). In the end, our proof of Chebotarev's density theorem will only need narrow ray class groups.

Example 3.34. Let $\mathfrak{m}$ be the modulus $\mathcal{O}_{\mathbb{K}} \cdot \emptyset$ of the number field $\mathbb{K}$ (i.e. $\mathfrak{m}_0 = \mathcal{O}_{\mathbb{K}}$ and $\mathfrak{m}_\infty = \emptyset$). Then $\mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}}$ is just the (ordinary) ideal class group $\mathrm{Cl}_{\mathbb{K}}$. If instead we take $\mathfrak{m} = \mathcal{O}_{\mathbb{K}} \cdot \infty$, we get the *narrow class group* of $\mathbb{K}$.

Example 3.35. Let $\mathfrak{m} = \mathfrak{m}_0 \cdot \infty$ be a modulus of $\mathbb{Q}$, where $\mathfrak{m}_0$ is an ideal of $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Here, the inclusion map $\iota \colon \mathbb{Q} \to \mathbb{R}$ is the *only* real embedding of $\mathbb{Q}$, and so $\infty = \{\iota\}$. As every non-zero ideal of $\mathbb{Z}$ has a unique positive generator, there is a positive integer m such that $\mathfrak{m}_0 = m\mathbb{Z}$, and so

$$\mathcal{I}_{\mathbb{Q}}^{\mathfrak{m}} = \left\{\mathfrak{a} \in \mathcal{I}_{\mathbb{Q}} : \ \exists c, d \in \mathbb{Z}^+. \ \mathfrak{a} = \tfrac{c}{d}\mathbb{Z}, \ \gcd(c, m) = \gcd(d, m) = 1\right\},$$
$$\mathcal{P}_{\mathbb{Q}}^{\mathfrak{m}} = \left\{\mathfrak{a} \in \mathcal{I}_{\mathbb{Q}} : \ \exists r, s \in \mathbb{Z}^+. \ \mathfrak{a} = \tfrac{r}{s}\mathbb{Z}, \ r \equiv s \equiv 1 \pmod{m}\right\}.$$

In Example 3.23, we constructed an isomorphism $\overline{\overline{N}} \colon \mathrm{Cl}_{\mathbb{Q}}^{\mathfrak{m}} \to (\mathbb{Z}/m\mathbb{Z})^\times$.

Suppose now that $\mathfrak{a} \in \mathcal{I}_{\mathbb{Q}}^{\mathfrak{m}}$. We may write $\mathfrak{a} = \frac{c}{d}\mathbb{Z}$ for some $c, d \in \mathbb{Z}^+$ which are both coprime with m. The ray class of $\mathfrak{a}$ modulo $\mathfrak{m}$ is then given by

$$\mathfrak{a}\mathcal{P}_{\mathbb{Q}}^{\mathfrak{m}} = \left\{\mathfrak{b} \in \mathcal{I}_{\mathbb{Q}} : \ \exists u, v \in \mathbb{Z}^+. \ \mathfrak{b} = \tfrac{u}{v}\mathbb{Z}, \ u \equiv c \pmod{m}, \ v \equiv d \pmod{m}\right\}.$$

Indeed, one inclusion follows by setting $u = cr$ and $v = ds$, and the other follows by setting $r = uc'$ and $s = vd'$ where c' and d' are positive integer inverses modulo m of c and d respectively.

Proposition 3.36. *The ray class group $\mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}}$ is finite, and the (ordinary) ideal class group $\mathrm{Cl}_{\mathbb{K}}$ is a quotient group of $\mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}}$. The order of $\mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}}$ is denoted $h_{\mathbb{K}}^{\mathfrak{m}}$.*

Proof. See Theorem 1 of Chapter VI in Lang [21] (or Corollary 21.9 of Sutherland [30], or Exercise 10 of Chapter 6 in Marcus [28]). □

We now have all that we need to state Artin reciprocity. *Artin reciprocity* says, for a suitable choice[1] of the modulus $\mathfrak{m}$ of $\mathbb{K}$, that the Artin map $\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}$ is surjective and that $\mathcal{P}_{\mathbb{K}}^{\mathfrak{m}} \subseteq \ker\left(\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}\right)$. From the first isomorphism theorem, it follows that the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ is isomorphic to a quotient of the ray class group $\mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}}$.

Remark 3.37. For our proof of Chebotarev's density theorem, we only need the special case of Artin reciprocity where $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}(\zeta)$ for a primitive m-th root of unity ζ, and $\mathfrak{m} = \mathfrak{m}_0 \cdot \infty$ where $m\mathcal{O}_{\mathbb{K}}$ divides $\mathfrak{m}_0$. For this special case, we prove in the following theorem that $\mathcal{P}_{\mathbb{K}}^{\mathfrak{m}} \subseteq \ker\left(\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}\right)$, and we will return later to prove that $\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}$ is surjective (Proposition 4.24).

Theorem 3.38. *Let $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}(\zeta)$ be a tower of number fields, where $\zeta \in \mathbb{C}$ is a primitive m-th root of unity. Let $\mathfrak{m} = \mathfrak{m}_0 \cdot \infty$ be a modulus of $\mathbb{K}$, where $m\mathcal{O}_{\mathbb{K}}$ divides $\mathfrak{m}_0$. Then*

$$\mathcal{P}_{\mathbb{K}}^{\mathfrak{m}} \subseteq \ker\left(\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}\right).$$

Proof. Let $r\colon \mathrm{Gal}(\mathbb{K}(\zeta)/\mathbb{K}) \to \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ be the map from Proposition 3.21, and let $\iota\colon \mathrm{Gal}(\mathbb{K}(\zeta)/\mathbb{K}) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times$ be the map from Proposition 3.4. In Proposition 3.21, we showed that that $\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}} = r \circ \left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}$, so

$$\ker\left(\left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}\right) \subseteq \ker\left(\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}\right).$$

As ι is an embedding, we also have

$$\ker\left(\left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}\right) = \ker\left(\iota \circ \left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}\right).$$

Hence, it suffices to show that $\mathcal{P}_{\mathbb{K}}^{\mathfrak{m}} \subseteq \ker\left(\iota \circ \left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}\right)$.

Expanding the definitions of $\mathcal{P}_{\mathbb{K}}^{\mathfrak{m}}$, $\mathbb{K}^{\mathfrak{m}}$ and $\mathcal{O}_{\mathbb{K}}^{\mathfrak{m}}$, we see that $\mathcal{P}_{\mathbb{K}}^{\mathfrak{m}}$ is generated by

$$S = \left\{\mathfrak{a} \in \mathcal{I}_{\mathbb{K}} :\ \exists \alpha \in \mathcal{O}_{\mathbb{K}}.\ \mathfrak{a} = \alpha\mathcal{O}_{\mathbb{K}},\ \alpha \equiv 1 \pmod{\mathfrak{m}_0},\ \sigma(\alpha) > 0 \text{ for all } \sigma \in \infty\right\}.$$

So, it suffices in turn to show that $S \subseteq \ker\left(\iota \circ \left[\frac{\mathbb{K}(\zeta)/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}\right)$. By Equation (3.3.2), this is equivalent to showing that $N(\mathfrak{a}) \equiv 1 \pmod{m}$ for all $\mathfrak{a} \in S$.

Let $\mathfrak{a} \in S$. Then $\mathfrak{a} = \alpha\mathcal{O}_{\mathbb{K}}$ for some $\alpha \in \mathcal{O}_{\mathbb{K}}$ for which $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and $\sigma(\alpha) > 0$ for all $\sigma \in \infty$. As $\alpha\mathcal{O}_{\mathbb{K}}$ is a principal ideal, we have $N(\alpha\mathcal{O}_{\mathbb{K}}) = \left|N_{\mathbb{Q}}^{\mathbb{K}}(\alpha)\right|$. Let $\sigma_1, \ldots, \sigma_r$ be the real embeddings of $\mathbb{K}$, and $\tau_1, \overline{\tau_1}, \ldots, \tau_s, \overline{\tau_s}$ be the complex embeddings of $\mathbb{K}$. Then we have

$$\begin{aligned} N_{\mathbb{Q}}^{\mathbb{K}}(\alpha) &= \sigma_1(\alpha) \cdots \sigma_r(\alpha)\tau_1(\alpha)\overline{\tau_1(\alpha)} \cdots \tau_s(\alpha)\overline{\tau_s(\alpha)} \\ &= \sigma_1(\alpha) \cdots \sigma_r(\alpha)|\tau_1(\alpha)|^2 \cdots |\tau_s(\alpha)|^2. \end{aligned}$$

As $\infty = \left\{\sigma_i\right\}_{i=1}^{r}$, we have $\sigma_k(\alpha) > 0$ for all $k \in \left\{1, \ldots, r\right\}$, and so $N_{\mathbb{Q}}^{\mathbb{K}}(\alpha) > 0$. Hence $N(\alpha\mathcal{O}_{\mathbb{K}}) = N_{\mathbb{Q}}^{\mathbb{K}}(\alpha)$. It remains to show that $N_{\mathbb{Q}}^{\mathbb{K}}(\alpha) \equiv 1 \pmod{m}$.

[1] The minimal such choice is known as the *conductor* of the extension $\mathbb{L}/\mathbb{K}$.

As $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and $m\mathcal{O}_{\mathbb{K}}$ divides $\mathfrak{m}_0$, we have $\alpha - 1 \in \mathfrak{m}_0 \subseteq m\mathcal{O}_{\mathbb{K}}$. Thus there is a $\beta \in \mathcal{O}_{\mathbb{K}}$ such that $\alpha = 1 + m\beta$. It follows that

$$N_{\mathbb{Q}}^{\mathbb{K}}(\alpha) = \prod_{\sigma\colon \mathbb{K}\hookrightarrow\mathbb{C}} \sigma(\alpha) = \prod_{\sigma\colon \mathbb{K}\hookrightarrow\mathbb{C}} \big(1 + m\sigma(\beta)\big) = 1 + m\gamma$$

for some algebraic integer γ. As $\gamma = \big(N_{\mathbb{Q}}^{\mathbb{K}}(\alpha) - 1\big)/m \in \mathbb{Q}$, and the algebraic integers of $\mathbb{Q}$ are just integers, actually $\gamma \in \mathbb{Z}$. Hence $N_{\mathbb{Q}}^{\mathbb{K}}(\alpha) \equiv 1 \pmod{m}$. □

Corollary 3.39. *Assuming the same notation as Theorem 3.38, there is a unique map* $\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}\colon \mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}} = \mathcal{I}_{\mathbb{K}}^{\mathfrak{m}}/\mathcal{P}_{\mathbb{K}}^{\mathfrak{m}} \to \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ *such that*

$$\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{a}\mathcal{P}_{\mathbb{K}}^{\mathfrak{m}}}\right]_{\mathfrak{m}}} = \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{a}}\right]_{\mathfrak{m}} \quad \forall \mathfrak{a} \in \mathcal{I}_{\mathbb{K}}^{\mathfrak{m}};$$

and, additionally, $\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}$ *is a group homomorphism.*

Proof. This follows from the universal property of quotient morphisms. □

Chapter 4

Weber L-functions and the cyclotomic case

Heinrich Martin Weber (1842–1913) was a pioneer of class field theory. In 1886, Weber proved Kronecker's conjecture that every abelian field extension of $\mathbb{Q}$ is a subfield of a cyclotomic field — this result is known today as the Kronecker–Weber theorem. Weber was the first to use the term *class field* (Classenkörper), for the class field of an imaginary quadratic number field, in his book *Elliptic functions and algebraic numbers* [32, p. 439], published in 1891. In 1897 and 1898, Weber published a series of three papers titled *On number groups in algebraic fields* [33–35] in which he established a more general formulation of class field theory, the ideas of which received a thorough treatment in the fourth book, titled *Class fields*, of the third volume of the second edition of his *Textbook of Algebra* [36, pp. 563–622]. See Frei [11] for more on Weber's contributions to class field theory.

In the second of his three papers [35], Weber introduced his *harmonic number groups* [35, p. 90] — groups of ideals of a number field which correspond to our *narrow ray class groups*, and he also defined what we will call the Weber L-functions [35, p. 86] — a generalisation of the Dirichlet L-functions which replaces the group $(\mathbb{Z}/m\mathbb{Z})^\times$ with an ideal group (such as a narrow ray class group) which satisfies certain properties. Just as the Dirichlet L-functions are the key analytic tool that Dirichlet used to prove his theorem on prime numbers in arithmetic progression, the Weber L-functions are the key analytic tool that we will use to prove Chebotarev's density theorem for cyclotomic extensions of number fields.

Although Chebotarev did not use Weber's number groups and class fields in his proof — instead he preferred to work with his own notion of *admissible complexes*, he was aware of Weber's work and its connection to his own. Indeed, in his Russian paper, Chebotarev writes [37, p. 208]:

> *In §III, I generalize Dirichlet's progression theorem. Namely, I prove the existence, in any field, of infinitely many prime ideals whose norms lie in given admissible complexes. Similar generalizations were made by other authors. So, Weber in his article: "Über Zahlgruppen etc.", (Math. Ann., Bd. 49) proves an even more general theorem, but does not express it very clearly (namely, the concept corresponding to my admissible complexes is vague) and, moreover, he assumes the existence of a class field (Klassenkörper), which I avoid by narrowing the scope of the result somewhat and introducing the concept of complexes admissible in a narrow and broad sense.*[1]

[1] Many thanks go to my friend Andrew Kaploun for helping me with this translation.

Interestingly, a large portion of the introduction to Chebotarev's Russian article did not make it into its 1926 German adaptation [31], including this particular paragraph, and another in which Chebotarev mentions B.N. Delaunay's proof of the Kronecker–Weber theorem as his inspiration for a result in §V of his paper (the part of his paper where he presents what we referred to in our introduction as his field "crossing" argument). Stevenhagen and Lenstra, in their 1996 article [29, p. 34], appear to contradict Chebotarev's own personal account when they say:

> *"In fact, Chebotarëv was at the time not yet familiar with class field theory; he proved his theorem essentially with his bare hands."*

It is unclear how Stevenhagen and Lenstra reached this conclusion, although one might guess that they only read the German adaptation of Chebotarev's paper.

Armed with our knowledge about ray class groups and Artin reciprocity for cyclotomic extensions from the previous chapter, in this chapter, we return to prove Chebotarev's density theorem for cyclotomic extensions. Given a tower of number fields $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}(\zeta)$ where ζ is a primitive m-th root of unity, and an element $\tau \in G$ where $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, we would like to show that the Dirichlet density

$$\delta(P_\tau) = \lim_{\sigma \to 1^+} \frac{\sum_{\mathfrak{p} \in P_\tau} N(\mathfrak{p})^{-\sigma}}{\sum_{\mathfrak{p} \in P(\mathbb{K})} N(\mathfrak{p})^{-\sigma}} \tag{4.0.1}$$

exists and equals $1/|G|$, where

$$P_\tau = \left\{ \mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \text{ is unramified in } \mathcal{O}_\mathbb{L}, \ \left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right] = \tau \right\}.$$

The key idea, which, in some form, goes back to Dirichlet's proof of his theorem on prime numbers in arithmetic progressions [25], is to use the second orthogonality relation (Proposition A.11) to rewrite the numerator of the limit in (4.0.1) as

$$\sum_{\mathfrak{p} \in P_\tau} N(\mathfrak{p})^{-\sigma} = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(\tau^{-1}) \sum_{\mathfrak{p}} \frac{\chi(\left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right])}{N(\mathfrak{p})^\sigma} \tag{4.0.2}$$

where the sums on the right-hand side of (4.0.2) are taken over all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_\mathbb{K}$ which are unramified in $\mathcal{O}_\mathbb{L}$. It turns out that a sum of the form

$$\sum_{\mathfrak{p}} \frac{\chi(\left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right])}{N(\mathfrak{p})^s} \tag{4.0.3}$$

differs, by a bounded function of s, from a function of s which, in some sense, may be thought of as the logarithm of a Weber L-function. The Weber L-functions and their logarithms have nice analytic properties — most of this chapter will be spent stating and proving these properties; (4.0.2) will allow us to use these properties to understand the behaviour of the numerator of the limit in (4.0.1) as $\sigma \to 1^+$.

Remark 4.1. Throughout the rest of this chapter, it is assumed that the reader is familiar with the character theory of finite abelian groups, and also with the theory of infinite products. For the reader's convenience, we provide a thorough introduction to these topics, proving all needed results, in Appendix A and Appendix B

respectively. We also remind the reader of the properties of *generalised commutativity* and *generalised associativity* enjoyed by absolutely convergent infinite sums and products, which we discussed in Remark 2.36.

Remark 4.2. Throughout this chapter, we will use the notation

$$H(\sigma) = \{s \in \mathbb{Z} : \ \mathrm{Re}(s) > \sigma\}$$

for the open half-plane in $\mathbb{C}$ to the right of the line $\mathrm{Re}(s) = \sigma$, where $\sigma \in \mathbb{R}$.

4.1 Weber L-functions

The focus of this section is to introduce the Weber L-functions. We begin, however, with a brief overview of the analogous treatment of the simpler Dirichlet L-functions, to provide a point of reference for when we consider the more general case.

The Dirichlet L-function $L(s, \chi)$, where s is a complex variable and χ is a character of the group $(\mathbb{Z}/m\mathbb{Z})^\times$ for some positive integer m, is defined by the series

$$L(s, \chi) = \sum_{\gcd(n,m)=1} \frac{\chi(n + m\mathbb{Z})}{n^s},$$

taken over all positive integers n which are coprime to m. The series converges absolutely for all $s \in H(1)$ by comparison with the p-series $\sum_{n=1}^{\infty} n^{-\sigma}$. One uses the *complete multiplicativity* of the function $n \mapsto \chi(n+m\mathbb{Z})n^{-s}$ to show that $L(s, \chi)$ is also given by the *Euler product*

$$L(s, \chi) = \prod_{p \nmid m} \left(1 - \frac{\chi(p + m\mathbb{Z})}{p^s}\right)^{-1},$$

taken over all prime numbers p not dividing m. As the sum $\sum_{p \nmid m} \chi(p+m\mathbb{Z})p^{-s}$ converges absolutely for all $s \in H(1)$ (also by comparison with the p-series $\sum_{n=1}^{\infty} n^{-\sigma}$), we may use Corollary B.11 to deduce that the Euler product also converges absolutely for all $s \in H(1)$.

For the Dirichlet L-functions, we were able to prove the absolute convergence of the series and Euler product independently. For the Weber L-functions, it is easier to show that their Euler product formula converges absolutely on $H(1)$, because the Euler product is taken over prime ideals rather than arbitrary ideals and so we have the theory of splitting of prime ideals in extensions at our disposal. In our appendix on infinite products (Appendix B), we prove a result about generalised Euler products and their corresponding series (Proposition B.14), which essentially says that if either converges absolutely, then both converge absolutely and to the same value. We will use this result to deduce that the series formula for a Weber L-function is also absolutely convergent on $H(1)$, and that it converges here to the same value as its Euler product.

Remark 4.3. Let $\mathbb{K}$ be a number field, and let $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ be a modulus of $\mathbb{K}$. Recall that $\mathcal{I}_\mathbb{K}^\mathfrak{m}$ denotes the set of non-zero fractional ideals of $\mathcal{O}_\mathbb{K}$ which are coprime to $\mathfrak{m}_0$, and that $\mathrm{Cl}_\mathbb{K}^\mathfrak{m} = \mathcal{I}_\mathbb{K}^\mathfrak{m}/\mathcal{P}_\mathbb{K}^\mathfrak{m}$ denotes the *ray class group* of $\mathbb{K}$ for the modulus $\mathfrak{m}$ (Definition/Proposition 3.28). When it is clear from context which ray class group

is being discussed, rather than explicitly writing $\mathfrak{a}\mathcal{P}_{\mathbb{K}}^{\mathfrak{m}}$ for the ray class of an element $\mathfrak{a}$ of $\mathcal{I}_{\mathbb{K}}^{\mathfrak{m}}$, we will instead write $\tilde{\mathfrak{a}}$.

Definition/Proposition 4.4 (Weber L-function)**.** Let $\mathbb{K}$ be a number field, let $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ be a modulus of $\mathbb{K}$, and let χ be a character of $\mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}}$. The *Weber L-function* $L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi)$ is defined by

$$L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}_0} \left(1 - \frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{\gcd(\mathfrak{a},\mathfrak{m}_0)=1} \frac{\chi(\tilde{\mathfrak{a}})}{N(\mathfrak{a})^s},$$

where the infinite product is taken over all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ which do not divide $\mathfrak{m}_0$, the series is taken over all non-zero ideals $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{K}}$ which are coprime with $\mathfrak{m}_0$, and the series and infinite product are both absolutely convergent and equal for all $s \in H(1)$.

Proof. Let $s \in H(1)$ and let $\sigma = \mathrm{Re}(s)$. For all non-zero prime ideals $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$,

$$\left|\frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right| = \frac{1}{N(\mathfrak{p})^\sigma} < 1$$

because $N(\mathfrak{p}) = |\mathcal{O}_{\mathbb{K}}/\mathfrak{p}| > 1$. This means that the factors in the infinite product defining $L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi)$ are non-zero, and so this infinite product fits within our restricted definition of infinite products (Definition B.1).

In Proposition 2.40, we showed that the series $\sum_{\mathfrak{p}\nmid\mathfrak{m}_0} N(\mathfrak{p})^{-\sigma}$ converges. Hence, the series $\sum_{\mathfrak{p}\nmid\mathfrak{m}_0} \chi(\tilde{\mathfrak{p}})N(\mathfrak{p})^{-s}$ is absolutely convergent. By Corollary B.11, the infinite product $\prod_{\mathfrak{p}\nmid\mathfrak{m}_0}(1-\chi(\tilde{\mathfrak{p}})N(\mathfrak{p})^{-s})$ is thus also absolutely convergent. Hence, the infinite product defining $L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi)$ is absolutely convergent (Proposition B.13).

It remains to show that the series defining $L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi)$ converges absolutely, and that it equals the infinite product defining $L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi)$. In the paragraph preceding Proposition B.14, we introduced the notation I for the set of non-negative integer sequences $i = (i_k)_{k=1}^{\infty}$ with only finitely many of the i_k non-zero. Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots$ be an enumeration of the countably many non-zero prime ideals of $\mathcal{O}_{\mathbb{K}}$ which do not divide $\mathfrak{m}_0$. Define the function $f\colon \mathcal{I}_{\mathbb{K}}^{\mathfrak{m}} \to \mathbb{C}^\times$ by $f(\mathfrak{a}) = \chi(\tilde{\mathfrak{a}})N(\mathfrak{a})^{-s}$. Applying Proposition B.14 to the sequence of complex numbers $\big(f(\mathfrak{p}_1), f(\mathfrak{p}_2), \ldots\big)$, all of which have moduli less than 1, we find that

$$\prod_{\mathfrak{p}\nmid\mathfrak{m}_0} \left(1 - \frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{i\in I} f(\mathfrak{p}_1)^{i_1} f(\mathfrak{p}_2)^{i_2} \cdots,$$

where the series on the right converges absolutely and equals the product on the left because the product on the left converges absolutely. As $f(\mathfrak{ab}) = f(\mathfrak{a})f(\mathfrak{b})$ for all $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}_{\mathbb{K}}^{\mathfrak{m}}$, that is, f is completely multiplicative, we have

$$\sum_{i\in I} f(\mathfrak{p}_1)^{i_1} f(\mathfrak{p}_2)^{i_2} \cdots = \sum_{i\in I} f\big(\mathfrak{p}_1^{i_1}\mathfrak{p}_2^{i_2}\cdots\big) = \sum_{\gcd(\mathfrak{a},\mathfrak{m}_0)=1} f(\mathfrak{a}) = \sum_{\gcd(\mathfrak{a},\mathfrak{m}_0)=1} \frac{\chi(\tilde{\mathfrak{a}})}{N(\mathfrak{a})^s},$$

where the reindexing in the second equality uses the uniqueness of the prime ideal factorisations of the non-zero ideals of $\mathcal{O}_{\mathbb{K}}$. □

Definition 4.5. Let $\mathbb{K}$ be a number field, and let $\mathfrak{c}$ be a non-zero ideal of $\mathbb{K}$. The *Dedekind zeta function* of $\mathbb{K}$ with respect to $\mathfrak{c}$, denoted $\zeta_{\mathbb{K}}^{\mathfrak{c}}$, is defined by

$$\zeta_{\mathbb{K}}^{\mathfrak{c}}(s) = \sum_{\gcd(\mathfrak{a},\mathfrak{c})=1} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}\nmid\mathfrak{c}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1},$$

where the sum and product both converge absolutely and are equal, for all $s \in H(1)$.

Remark 4.6. Evidently, if $\mathfrak{m}$ is a modulus of $\mathbb{K}$ of the form $\mathfrak{m} = \mathfrak{c} \cdot \mathfrak{m}_\infty$, then $\zeta_{\mathbb{K}}^{\mathfrak{c}}(s) = L_{\mathbb{K}}^{\mathfrak{m}}(s, \chi_1)$. Hence, all properties of the Weber L-function $L_{\mathbb{K}}^{\mathfrak{m}}(s, \chi_1)$ transfer to properties of the Dedekind zeta function $\zeta_{\mathbb{K}}^{\mathfrak{c}}$.

4.2 Complex analysis review

As complex analysis will play an important role throughout the rest of the chapter, it is worth recalling the basic definitions and results that we will use. Our summary is similar to the one provided in Section 16.3.1 of Sutherland [30]. Let f, g and h be complex functions defined on an open subset of $\mathbb{C}$.

- f is *differentiable* at $z_0 \in \mathbb{C}$ if $\lim_{z\to z_0} \frac{f(z)-f(z_0)}{z-z_0}$ exists.
- f is *holomorphic* at $z_0 \in \mathbb{C}$ if it is differentiable on an open ball centred at z_0.
- f is *analytic* at $z_0 \in \mathbb{C}$ if there is an open ball centred at z_0 on which f has a (convergent) power series expansion $f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$.
- **Theorem.** *f is holomorphic at $z_0 \in \mathbb{C}$ if and only if it is analytic at z_0.* See Theorem 5.1 in Chapter II of Lang [22, p. 72] for the "if" direction, and Theorem 7.2 in Chapter III of Lang [22, p. 127] for the "only if" direction.
- **Theorem 4.7.** *If a sequence of complex functions $(f_n)_{n=1}^{\infty}$, which are analytic on an open subset U of $\mathbb{C}$, converges uniformly to f on every compact subset of U, then f is analytic on U and the sequence of derivatives $(f_n')_{n=1}^{\infty}$ converges uniformly to f' on every compact subset of U.* See Theorems 1.1 and 1.2 in Chapter V of Lang [22, pp. 156–157].
- **Theorem 4.8** (Identity theorem)**.** *If f and g are analytic on an connected open set U of $\mathbb{C}$, and they are equal on some subset of U which has a limit point, then f and g are equal on all of U.* See Theorem 1.2 in Chapter III of Lang [22, p. 90].
- **Theorem 4.9.** *Suppose that f is analytic on a non-empty connected open set U. Let $a \in U$, and choose $R > 0$ so that $\overline{B(a,R)} \subseteq U$. Then*

$$\left| f(z) - \sum_{k=0}^{n-1} \frac{f^{(k)}(a)}{k!}(z-a)^k \right| \leqslant \frac{M|z-a|^n}{R^{n-1}(R-|z-a|)}$$

for all $n \geqslant 1$ and all $z \in B(a,R)$, where

$$M = \max_{|z-a|=R} |f(z)|.$$

Combine Theorem 8 (Taylor's theorem) of Chapter 4 in Alfhors [1, p. 125] with the upper bound on the remainder term given on the next page.

- If f is holomorphic on a non-empty open set U of $\mathbb{C}$, and g is holomorphic on a connected open set C of $\mathbb{C}$ containing U, and g is equal to f on U, then g is the (unique) *analytic continuation* of f to C.
- The *principal branch* of the complex logarithm is the function $\mathrm{Log}\colon \mathbb{C}\backslash\{0\} \to \mathbb{C}$ given by
$$\mathrm{Log}(z) = \ln|z| + i\,\mathrm{Arg}(z) \qquad \forall z \in \mathbb{C}\backslash\{0\},$$
where $\ln\colon (0,\infty) \to \mathbb{R}$ is the real logarithm, and $\mathrm{Arg}(z)$ is the principal argument of z, that is, the argument of z in the interval $(-\pi, \pi]$.
- **Theorem 4.10.** *The function* Log *is holomorphic on* $\mathbb{C}\backslash(-\infty, 0]$*, where its derivative given by*
$$\mathrm{Log}'(z) = \frac{1}{z} \qquad \forall z \in \mathbb{C}\backslash(-\infty, 0].$$
Also, Log *is discontinuous on* $(-\infty, 0]$. See Chapter 3, §6 of Lang [22].
- **Theorem 4.11.** *The function* $z \mapsto -\mathrm{Log}(1-z)$ *is given by the convergent power series*
$$-\mathrm{Log}(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n},$$
on the open ball centred at 0 *of radius* 1. Indeed, the left and right-hand sides are both primitives of $1/(1-z) = \sum_{n=0}^{\infty} z^n$ on this ball, and they take the same value 0 at $z = 0$.
- $B^\circ(z_0, r) = \{z \in \mathbb{C} :\ 0 < |z - z_0| < r\}$ is the punctured ball centred at z_0 of radius r.
- If f is holomorphic on a punctured ball centred at $z_0 \in \mathbb{C}$, and $|f(z)| \to \infty$ as $z \to z_0$, then z_0 is a *pole* of f. By definition, the poles of f are isolated.
- f is *meromorphic* at $z_0 \in \mathbb{C}$ if it is holomorphic at z_0 or z_0 is a pole of f.
- **Theorem.** *If* f *is meromorphic at* $z_0 \in \mathbb{C}$*, then there is a punctured ball centred at* z_0 *on which* f *has a (convergent) Laurent series expansion*
$$f(z) = \sum_{n=-n_0}^{\infty} a_n (z - z_0)^n.$$
See Theorem 2.1 in Chapter V of Lang [22, p. 162].
- The *order* $\mathrm{ord}_{z_0}(f)$ of a non-zero function f at a point $z_0 \in \mathbb{C}$ where f is meromorphic, is the least index n of all of the non-zero coefficients a_n in the Laurent series expansion $f(z) = \sum_{n=-n_0}^{\infty} a_n (z - z_0)^n$ of f at z_0. Thus z_0 is a pole of f if and only if $\mathrm{ord}_{z_0}(f) < 0$, and z_0 is a zero of f if and only if $\mathrm{ord}_{z_0}(f) > 0$.
- If $\mathrm{ord}_{z_0}(f) = 1$, then z_0 is a *simple zero* of f. If $\mathrm{ord}_{z_0}(f) = -1$, then z_0 is a *simple pole* of f.
- The *residue* $\mathrm{res}_{z_0}(f)$ of a function f at a point $z_0 \in \mathbb{C}$ where f is meromorphic, is the coefficient a_{-1} in the Laurent series expansion $f(z) = \sum_{n=-n_0}^{\infty} a_n (z - z_0)^n$ of f at z_0.

- **Theorem 4.12.** *If $z_0 \in \mathbb{C}$ is a simple pole of f, then*

$$\operatorname{res}_{z_0}(f) = \lim_{z \to z_0} (z - z_0) f(z).$$

This follows by considering the Laurent series expansion of f at z_0.

4.3 Complex analytic properties of the Weber L-functions

The next step is to deduce the complex analytic properties of the Weber L-functions. In particular, we will show that $L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi)$ has an analytic continuation to the half-plane $H\big(1 - \frac{1}{[\mathbb{K}:\mathbb{Q}]}\big)$ when $\chi \neq \chi_1$, and that $L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi_1)$ (equivalently $\zeta^{\mathfrak{c}}_{\mathbb{K}}(s)$) has a meromorphic continuation to the half-plane $H\big(1 - \frac{1}{[\mathbb{K}:\mathbb{Q}]}\big)$, which is analytic except for a simple pole at $s = 1$.

Remark 4.13. Let $\mathbb{K}$ be a number field, let $\mathfrak{m}$ be a modulus of $\mathbb{K}$, let $\chi \in \widehat{\mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}}$, and let $s \in H(1)$. For each positive integer n and each ray class $\mathcal{K} \in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}$, let

$$j_n(\mathcal{K}) = \big|\big\{\mathfrak{a} \trianglelefteq \mathcal{O}_{\mathbb{K}} : \ \mathfrak{a} \in \mathcal{K},\ N(\mathfrak{a}) = n\big\}\big|.$$

Applying generalised associativity (Theorem 2.39) to the series defining $L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi)$, we find that

$$L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi) = \sum_{n=1}^{\infty} \frac{\sum_{\mathcal{K} \in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}} \chi(\mathcal{K}) j_n(\mathcal{K})}{n^s}, \tag{4.3.1}$$

where the inner series is actually a finite sum (Proposition 3.36) and the outer series converges absolutely.

A *Dirichlet series* is a series of the form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where $(a_n)_{n=1}^{\infty}$ is a sequence of complex numbers. General series of this form were first studied by Dirichlet, who was interested in their application to number theory [16, p. 1]. In §101 of Dedekind's notes [10, pp. 254–258] on Dirichlet's lectures on number theory at Göttingen (1856–1857), we see that Dirichlet had proved that if the partial sums $\sum_{n=1}^{N} a_n$ are bounded, then the series $\sum_{n=1}^{\infty} a_n n^{-s}$ is a convergent continuous function of s on the interval $(0, \infty)$. In supplement IX, written by Dedekind and added to later editions of the lecture notes [10, pp. 376–386], Dedekind proved several more important results about these series, which he referred to as "Dirichlet'schen Reihen" (*Dirichlet's series*), but he still only considered real values of the variable s. The first results about general Dirichlet series with s a complex variable are due to Jensen and Cahen. Jensen [18, p. 70] showed that if such a series converges at $s_0 = \sigma_0 + it_0 \in \mathbb{C}$ then it converges on all of $H(\sigma_0)$. Cahen [8, p. 83] showed that if the partial sums of such a series are bounded at s_0, then the series is uniformly convergent on all compact subsets of $H(\sigma_0)$, and thus it converges to an analytic function on $H(\sigma_0)$. For a thorough introduction to Dirichlet series, consult Chapter 11 of Apostol [2].

We will use the following proposition, a stronger version of Cahen's result, to construct our meromorphic continuations of the Weber L-functions.

Proposition 4.14. *Consider the Dirichlet series $D(s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Suppose that at some point $s_0 = \sigma_0 + it_0 \in \mathbb{C}$, the partial sums of $D(s_0)$ satisfy*

$$\sum_{n=1}^{N} \frac{a_n}{n^{s_0}} = \rho N^r + O(N^u) \qquad \text{as } N \to \infty,$$

for some $\rho \in \mathbb{C}$ and some $u, r \in \mathbb{R}$ with $u \leqslant r$. Then $D(s)$ converges to a holomorphic function of s on the half-plane $H(\sigma_0 + r)$, and it has a meromorphic continuation to the half-plane $H(\sigma_0 + u)$ which is holomorphic everywhere except, if $\rho \neq 0$, for a simple pole of residue ρr at $s = s_0 + r$.

Remark 4.15. Let $(a_n)_{n=1}^{\infty}$ and $(b_n)_{n=1}^{\infty}$ be sequences of complex numbers, and let $(c_n)_{n=1}^{\infty}$ be a sequence of positive real numbers. By

$$a_n = b_n + O(c_n) \qquad \text{as } n \to \infty,$$

we mean that there is an integer $n_0 \geqslant 1$ and a real number $C > 0$ such that

$$|a_n - b_n| \leqslant C \cdot c_n \qquad \forall n \geqslant n_0.$$

We will use the following lemma in our proof of Proposition 4.14.

Lemma 4.16. *Let f be a piecewise-continuous complex-valued function defined on $[N, \infty)$ for some $N \geqslant 1$. Suppose that there is a $u \in \mathbb{R}$ and a $C > 0$ such that $|f(x)| \leqslant Cx^u$ for all $x \geqslant N$. Let*

$$F(s) = \int_N^{\infty} f(x) x^{-s-1} dx.$$

Then

(i) The integral $F(s)$ is absolutely convergent for all $s \in H(u)$.

(ii) The function F is holomorphic on $H(u)$, with derivative given by the absolutely convergent integral

$$G(s) = -\int_N^{\infty} \ln(x) f(x) x^{-s-1} dx.$$

Proof. Let $s = \sigma + it \in H(u)$. For all $x \geqslant \max(e, N)$, we have $\ln(x) \geqslant 1$, and so

$$\left| f(x) x^{-s-1} \right| \leqslant \left| \ln(x) f(x) x^{-s-1} \right| \leqslant C \ln(x) x^{u-\sigma-1}.$$

Integrating by parts, and then noting that $\sigma - u > 0$ and that $\ln(M)$ grows more slowly than any positive power of M, we see that $\int_1^{\infty} \ln(x) x^{u-\sigma-1} dx = (\sigma - u)^{-2}$. Hence the integrals $F(s)$ and $G(s)$ both converge absolutely by comparison.

Let $s_0 = \sigma_0 + it_0 \in H(u)$. We will show that $F'(s_0) = G(s_0)$. Let $R = \frac{1}{2}(\sigma_0 - u)$, so that $0 < R < \sigma_0 - u$, and thus $B(s_0, R) \subseteq H(u)$. Let $s \in B(s_0, R)$. Then

$$\begin{aligned}\left|\frac{F(s) - F(s_0)}{s - s_0} - G(s_0)\right| &= \left|\int_N^\infty f(x)x^{-s_0-1}\left(\frac{x^{s_0-s} - 1}{s - s_0} + \ln(x)\right)dx\right| \\ &\leqslant C\int_N^\infty x^{u-\sigma_0-1}\left|\frac{x^{s_0-s} - 1}{s - s_0} + \ln(x)\right|dx \qquad (4.3.2)\end{aligned}$$

For all $x \geqslant 1$, the function $z \mapsto x^{s_0-z}$ is analytic on $\mathbb{C}$, and $s \in B(s_0, R) \subseteq \mathbb{C}$, so

$$\left|x^{s_0-s} - 1 + \ln(x)(s - s_0)\right| \leqslant \frac{M|s - s_0|^2}{R(R - |s - s_0|)}$$

by Theorem 4.9 (taking $n = 2$), where

$$M = \max_{|z-s_0|=R}|x^{s_0-z}| = \max_{|z-s_0|=R} x^{\sigma_0-\mathrm{Re}(z)} = x^R.$$

Hence, continuing from (4.3.2), we have

$$\begin{aligned}\left|\frac{F(s) - F(s_0)}{s - s_0} - G(s_0)\right| &\leqslant C\int_N^\infty x^{u-\sigma_0-1}\frac{x^R|s - s_0|}{R(R - |s - s_0|)}dx \\ &= \frac{C|s - s_0|N^{R+u-\sigma_0}}{R(R - |s - s_0|)(\sigma_0 - R - u)}, \qquad (4.3.3)\end{aligned}$$

where we used the fact that $R + u - \sigma_0 < 0$ to compute the improper integral. The right-hand side of (4.3.3) goes to zero as $s \to s_0$, and thus, by the pinching theorem, so does the left-hand side. This means that $F'(s_0) = G(s_0)$. □

Proof of Proposition 4.14. It suffices to prove the result only in the case where $s_0 = 0$. Suppose that we have already shown that this special case of the result holds. The partial sums of the Dirichlet series

$$E(s) = \sum_{n=1}^\infty \frac{a_n n^{-s_0}}{n^s}$$

at $s = 0$ are the same as the partial sums of $D(s)$ at $s = s_0$. As $\sum_{n=1}^N a_n n^{-s_0} = \rho N^r + O(N^u)$ as $N \to \infty$, by our assumption, $E(s)$ converges to a holomorphic function of s on the half-plane $H(r)$, and it has a meromorphic extension to the half-plane $H(u)$, which is holomorphic everywhere except, if $\rho \neq 0$, for a simple pole of residue ρ at $s = r$. As the translations of $H(r)$, $H(u)$ and r by s_0 are, respectively, $H(\sigma_0 + r)$, $H(\sigma_0 + u)$ and $s_0 + r$, and as $D(s) = E(s - s_0)$, we may conclude that $D(s)$ has the desired properties. So, without loss of generality, assume that $s_0 = 0$.

Let $D_N(s) = \sum_{n=1}^N a_n n^{-s}$ and let $A_N = D_N(0) = \sum_{n=1}^N a_n$ for all integers $N \geqslant 1$. Also let $A_0 = 0$. Since $A_N = \rho N^r + O(N^u)$ as $N \to \infty$, there is a $C > 0$ and an integer $N_0 \geqslant 1$ such that $|A_N - \rho N^r| < CN^u$ for all integers $N \geqslant N_0$. We also have $A_N = O(N^r)$ as $N \to \infty$ because $r \geqslant u$. Hence, by increasing C and N_0 if necessary, we may also assume that $|A_N| \leqslant CN^r$ for all $N \geqslant N_0$.

We begin by showing that D converges on $H(r)$, that is, for all $s \in H(r)$, that $D_N(s)$ converges as $N \to \infty$. Let $s = \sigma + it \in H(r)$. Notice that $a_n = A_n - A_{n-1}$ for all $n \geqslant 1$. Hence, for all $N \geqslant 1$, we have

$$\begin{aligned} D_N(s) = \sum_{n=1}^{N} \frac{a_n}{n^s} = \sum_{n=1}^{N} \frac{A_n - A_{n-1}}{n^s} &= \sum_{n=1}^{N} \frac{A_n}{n^s} - \sum_{n=1}^{N} \frac{A_{n-1}}{n^s} \\ &= \sum_{n=1}^{N} \frac{A_n}{n^s} - \sum_{n=0}^{N-1} \frac{A_n}{(n+1)^s} = \frac{A_N}{N^s} - \sum_{n=1}^{N-1} A_n \left[\frac{1}{(n+1)^s} - \frac{1}{n^s} \right]. \end{aligned}$$

As $s \neq 0$, for all $n \geqslant 1$ we have

$$\int_n^{n+1} \frac{dx}{x^{s+1}} = -\frac{1}{s} \left[\frac{1}{(n+1)^s} - \frac{1}{n^s} \right].$$

It follows, for all $N \geqslant 1$, that

$$D_N(s) = \frac{A_N}{N^s} + s \sum_{n=1}^{N-1} A_n \int_n^{n+1} \frac{dx}{x^{s+1}}.$$

Let $A\colon [1, \infty) \to \mathbb{C}$ be the step function defined by $A(x) = A_{\lfloor x \rfloor}$. For example $A(2.8) = A_2$. Then A is piecewise continuous, and so for all $N \geqslant 1$, we have

$$D_N(s) = \frac{A_N}{N^s} + s \int_1^N \frac{A(x)}{x^{s+1}} dx. \tag{4.3.4}$$

For all $N \geqslant N_0$, we have

$$\left| \frac{A_N}{N^s} \right| \leqslant \frac{CN^r}{N^\sigma} = \frac{C}{N^{\sigma - r}},$$

and the right-hand side tends to zero as $N \to \infty$ because $\sigma - r > 0$. Hence

$$\lim_{N \to \infty} \frac{A_N}{N^s} = 0$$

by the pinching theorem. We also have $|A(x)| < Cx^r$ for all real $x \geqslant N_0$, and so

$$\int_1^\infty \left| \frac{A(x)}{x^{s+1}} \right| dx \leqslant \int_1^{N_0} \left| \frac{A(x)}{x^{s+1}} \right| dx + C \int_{N_0}^\infty \frac{dx}{x^{\sigma - r + 1}},$$

where the right-hand side converges because the improper integral is a p-integral with $p = \sigma - r + 1$ which is greater than 1, and so the left-hand side converges by comparison. Hence, the integral $\int_1^\infty A(x) x^{-(s+1)} dx$ converges absolutely. Combining all of this with (4.3.4), we conclude that $D_N(s)$ converges as $N \to \infty$, and that $D(s)$ is given by the absolutely convergent integral

$$D(s) = \lim_{N \to \infty} D_N(s) = s \int_1^\infty \frac{A(x)}{x^{s+1}} dx. \tag{4.3.5}$$

For all $s \in H(r)$, we have

$$\begin{aligned} D(s) &= \left(D_{N_0}(s) - \frac{A_{N_0}}{N_0^s} \right) + s \int_{N_0}^{\infty} \frac{A(x)}{x^{s+1}} dx \\ &= D_{N_0}(s) - \frac{A_{N_0}}{N_0^s} + s \int_{N_0}^{\infty} \frac{A(x) - \rho x^r}{x^{s+1}} dx + \rho s \int_{N_0}^{\infty} x^{r-s-1} dx \\ &= D_{N_0}(s) - \frac{A_{N_0}}{N_0^s} + s \int_{N_0}^{\infty} \frac{A(x) - \rho x^r}{x^{s+1}} dx + \rho s \frac{N_0^{s-r}}{s-r}. \end{aligned} \tag{4.3.6}$$

Now $D_{N_0}(s)$ and $A_{N_0} {N_0}^{-s}$ are holomorphic functions of s on $\mathbb{C}$. As $A(x) - \rho x^r \leqslant C x^u$ for all $x \geqslant N_0$, Lemma 4.16 implies that $\int_{N_0}^{\infty} (A(x) - \rho x^r) x^{-s-1} dx$ is a holomorphic function of s on $H(u)$. Finally, $\rho s (s-r)^{-1} N_0^{s-r}$ is a meromorphic function of s on $\mathbb{C}$ which is holomorphic everywhere, except, if $\rho \neq 0$, for a simple pole of residue ρr at $s = r$. Overall, the right-hand side of (4.3.6), seen as a function of s, defines a meromorphic continuation of D to $H(u)$ which is analytic everywhere, except, when $\rho \neq 0$, for a simple pole of residue ρr at $s = r$. □

To apply Proposition 4.14 to the series in (4.3.1), we need the following result.

Theorem 4.17. *Assume the same notation as in Remark 4.13. Then there is a real constant $\rho_{\mathbb{K}}^{\mathfrak{m}} > 0$, such that for each class $\mathcal{K} \in \mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}}$,*

$$\sum_{n=1}^{N} j_n(\mathcal{K}) = \rho_{\mathbb{K}}^{\mathfrak{m}} N + O\big(N^{1 - \frac{1}{[\mathbb{K}:\mathbb{Q}]}}\big) \quad \text{as } N \to \infty.$$

Proof. The standard proof of this result is quite technical; and it depends on results about *lattices* in $\mathbb{R}^n$, their *fundamental domains*, and subsets of $\mathbb{R}^n$ which are *k-Lipschitz parameterisable*, as well as the *group of units* of a number field, all of which are orthogonal to the rest of this thesis. Rather than take a large detour to introduce these notions and prove this result, we instead refer the reader to §2 and §3 of Chapter VI in Lang [21, p. 132]. □

Remark 4.18. The specific case of this theorem when $\mathfrak{m} = \mathcal{O}_{\mathbb{K}} \cdot \emptyset$, that is, when the ray classes are just the (ordinary) ideal classes, is a standard step in the proof of the *analytic class number formula*. The usual proof of this special case (Theorem 39 of Marcus [28, pp.111] or Theorem 19.12 of Sutherland [30]) works *mutatis mutandi* for the general case (Exercise 13 in Chapter 6 of Marcus [28, p. 126]).

Remark 4.19. One may wonder whether a large part of the proof of Chebotarev's density theorem is hidden in the proof of this theorem. We claim that this is not the case, at least in the situation where $\mathbb{K} = \mathbb{Q}$ and $\mathfrak{m} = m\mathbb{Z} \cdot \infty$ for some positive integer m. Extending Example 3.23, the ideal norm map restricts to a bijection between the ideals in $\mathcal{I}_{\mathbb{Q}}^{\mathfrak{m}}$ and the positive integers coprime with m, and it induces a bijection between the ray classes of $\mathbb{Q}$ modulo $\mathfrak{m}$ and the congruence classes of $\mathbb{Z}$ modulo m which are coprime to m. In this case, the above theorem says that the number of positive integers less than an upper bound N which fall into a given congruence class modulo m is approximately ρN for some $\rho > 0$, and that the error is asymptotically bounded. But this statement is obviously true, where we may take $\rho = 1/m$, and the error is always at most 1. On the other hand, the corresponding

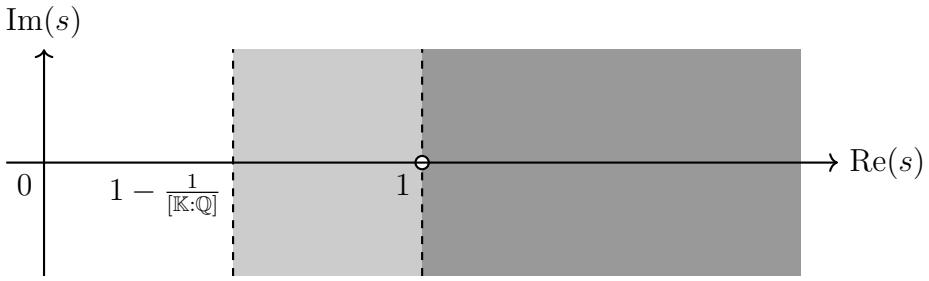


Figure 4.1: The series $L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi)$ is absolutely convergent and an analytic function of s on the dark grey region. This function has a meromorphic continuation to include the light grey region, which is analytic everywhere except, in the case that $\chi=\chi_1$, for a simple pole at $s=1$.

case of Chebotarev's density theorem is Dirichlet's theorem on primes in arithmetic progression, which is a deeper result and is not trivial to prove.

Remark 4.20. The theorem implies that the ideals of $\mathcal{O}_{\mathbb{K}}$ are approximately equidistributed across the ray classes modulo $\mathfrak{m}$. Indeed, for each $N\geqslant 1$, let

$$J_N=\big\{\mathfrak{a}\trianglelefteq\mathcal{O}_{\mathbb{K}}:\ \mathfrak{a}\in\mathcal{I}_{\mathbb{K}}^{\mathfrak{m}},\ N(\mathfrak{a})\leqslant N\big\}.$$

For each ray class $\mathcal{K}$, the theorem says that

$$|J_N\cap\mathcal{K}|=\rho_{\mathbb{K}}^{\mathfrak{m}}N+O\big(N^{1-\frac{1}{[\mathbb{K}:\mathbb{Q}]}}\big)\qquad\text{as } N\to\infty; \tag{4.3.7}$$

and by summing (4.3.7) over all of the ray classes, it also implies that

$$|J_N|=h_{\mathbb{K}}^{\mathfrak{m}}\rho_{\mathbb{K}}^{\mathfrak{m}}N+O\big(N^{1-\frac{1}{[\mathbb{K}:\mathbb{Q}]}}\big)\qquad\text{as } N\to\infty. \tag{4.3.8}$$

The statement $f(N)=\rho N+O(N^{1-\epsilon})$ means that there is a constant $C>0$ such that $|f(N)/N-\rho|\leqslant CN^{-\epsilon}$ for all large enough N. If $\epsilon>0$, then $CN^{-\epsilon}\to 0$ as $N\to\infty$, and thus $f(N)/N\to\rho$ as $N\to\infty$ by the pinching theorem. Applying this to (4.3.7) and (4.3.8), we can deduce that $|J_N\cap\mathcal{K}|/|J_N|\to 1/h_{\mathbb{K}}^{\mathfrak{m}}$ as $N\to\infty$ for each ray class $\mathcal{K}$. In other words, the set of ideals in a given ray class $\mathcal{K}$ has *natural density* $1/h_{\mathbb{K}}^{\mathfrak{m}}$ in the set of all non-zero ideals of $\mathcal{O}_{\mathbb{K}}$.

We now have all we need to prove the main result of this section. Recall that $h_{\mathbb{K}}^{\mathfrak{m}}=|\mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}}|$ is always finite (Proposition 3.36).

Proposition 4.21. *Assume the same notation as in Remark 4.13. Then $L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi)$ is a holomorphic function of s on $H(1)$. Also*

(i) if $\chi=\chi_1$, then this function has a meromorphic continuation to the half-plane $H\big(1-\frac{1}{[\mathbb{K}:\mathbb{Q}]}\big)$ which is holomorphic except for a simple pole at $s=1$ with residue $h_{\mathbb{K}}^{\mathfrak{m}}\rho_{\mathbb{K}}^{\mathfrak{m}}$; and

(ii) if $\chi\neq\chi_1$, then this function has an analytic continuation to the half-plane $H\big(1-\frac{1}{[\mathbb{K}:\mathbb{Q}]}\big)$.

Refer to Figure 4.1.

Proof. The N-th partial sum of $L^{\mathfrak{m}}_{\mathbb{K}}(0,\chi)$ is

$$\sum_{n=1}^{N}\Big(\sum_{\mathcal{K}\in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}} \chi(\mathcal{K}) j_n(\mathcal{K})\Big) n^{-0} = \sum_{\mathcal{K}\in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}} \chi(\mathcal{K})\Big(\sum_{n=1}^{N} j_n(\mathcal{K})\Big).$$

By Theorem 4.17, as $N\to\infty$, we have

$$\begin{aligned}\sum_{\mathcal{K}\in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}} \chi(\mathcal{K})\Big(\sum_{n=1}^{N} j_n(\mathcal{K})\Big) &= \sum_{\mathcal{K}\in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}} \chi(\mathcal{K})\Big(\rho^{\mathfrak{m}}_{\mathbb{K}} N + O\big(N^{1-\frac{1}{[\mathbb{K}:\mathbb{Q}]}}\big)\Big)\\ &= \rho^{\mathfrak{m}}_{\mathbb{K}} N\Big(\sum_{\mathcal{K}\in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}} \chi(\mathcal{K})\Big) + O\big(N^{1-\frac{1}{[\mathbb{K}:\mathbb{Q}]}}\big).\end{aligned}$$

By the first orthogonality relation (Proposition A.11), we know that

$$\sum_{\mathcal{K}\in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}} \chi(\mathcal{K}) = \sum_{\mathcal{K}\in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}} \chi(\mathcal{K})\overline{\chi_1(\mathcal{K})} = \begin{cases} |\mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}| = h^{\mathfrak{m}}_{\mathbb{K}} & \text{if } \chi=\chi_1,\\ 0 & \text{otherwise.}\end{cases}$$

Hence, as $N\to\infty$, we have

$$\sum_{n=1}^{N}\Big(\sum_{\mathcal{K}\in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}} \chi(\mathcal{K}) j_n(\mathcal{K})\Big) = \begin{cases} h^{\mathfrak{m}}_{\mathbb{K}}\rho^{\mathfrak{m}}_{\mathbb{K}} N + O\big(N^{1-\frac{1}{[\mathbb{K}:\mathbb{Q}]}}\big) & \text{if } \chi=\chi_1,\\ O\big(N^{1-\frac{1}{[\mathbb{K}:\mathbb{Q}]}}\big) & \text{otherwise.}\end{cases}$$

The result follows from Proposition 4.14 in the case that $\chi\neq\chi_1$, and from Proposition 4.14 when $\chi=\chi_1$ with $\rho = h^{\mathfrak{m}}_{\mathbb{K}}\rho^{\mathfrak{m}}_{\mathbb{K}} > 0$. □

4.4 Weber L-functions and the Artin map

In Definition 3.20, we defined the Artin map $\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}} : \mathcal{I}^{\mathfrak{m}}_{\mathbb{K}} \to \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. For the special case where $\mathbb{L}/\mathbb{K}$ is cyclotomic and $\mathfrak{m} = \mathfrak{m}_0\cdot\infty$ for some $\mathfrak{m}_0$ divisible by $m\mathcal{O}_{\mathbb{K}}$, we proved, in Corollary 3.39, that the Artin map descends to a group homomorphism

$$\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}} : \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}} \to \mathrm{Gal}(\mathbb{L}/\mathbb{K}).$$

In this section, for the same special case, we will simultaneously show that the Artin map is surjective (this is the other part of Artin reciprocity that we said that we would prove in Remark 3.37), and that the Weber L-functions $L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi\circ\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}})$ are non-zero at $s=1$ if χ is a non-trivial character of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. The argument hinges on the ability to write the Dedekind zeta function of the extension field $\mathbb{L}$ as a product of Weber L-functions of the base field $\mathbb{K}$, so that we may compare the orders of the poles at $s=1$ on both sides of the resulting equality. Deriving this product formula is the focus of the next proposition.

Remark 4.22. Note that $\chi\circ\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}$ is a composition of group homomorphisms, and it maps from $\mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}$ to $\mathbb{C}^\times$, so it is indeed a character of $\mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}$.

Proposition 4.23. *Let $\mathbb{K}\subseteq\mathbb{L}\subseteq\mathbb{K}(\zeta)$ be a tower of number fields, where $\zeta\in\mathbb{C}$ is a primitive m-th root of unity. Let $\mathfrak{m}=\mathfrak{m}_0\cdot\infty$ be a modulus of $\mathbb{K}$ with $\mathfrak{m}_0$ divisible*

by $m\mathcal{O}_{\mathbb{K}}$, and let $\mathfrak{M} = \mathfrak{m}_0\mathcal{O}_{\mathbb{L}}$. Let $G \leqslant \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ be the image of the map $\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}$, and let $n = [\mathrm{Gal}(\mathbb{L}/\mathbb{K}) : G]$. Then for all $s \in H\big(1 - \frac{1}{[\mathbb{L}:\mathbb{Q}]}\big)\backslash\{1\}$, we have

$$\zeta_{\mathbb{L}}^{\mathfrak{M}}(s) = \prod_{\chi \in \widehat{G}} L_{\mathbb{K}}^{\mathfrak{m}}(s, \chi \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}})^n. \tag{4.4.1}$$

Proof. The left and right-hand sides of (4.4.1) are analytic functions of s on the connected open set $H\big(1 - \frac{1}{[\mathbb{L}:\mathbb{Q}]}\big)\backslash\{1\}$ by Proposition 4.21. As $H(1)$ is a subset of $H\big(1 - \frac{1}{[\mathbb{L}:\mathbb{Q}]}\big)\backslash\{1\}$ which contains a limit point, it suffices by the identity theorem (Theorem 4.8) to show that the equality (4.4.1) holds on $H(1)$.

Fix an $s \in H(1)$. If we can show that the factors of the Euler product expansions of the left and right-hand sides of (4.4.1) are the same, then the equality will hold by generalised commutativity and associativity (Remark 2.36). Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$ which does not divide $\mathfrak{m}_0$. By Corollary 2.17, we have

$$\mathfrak{p}\mathcal{O}_{\mathbb{L}} = \prod_{\mathfrak{P} \,|\, \mathfrak{p}\mathcal{O}_{\mathbb{L}}} \mathfrak{P}^e,$$

where the product is taken over the g prime ideals $\mathfrak{P}$ of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{p}$, and these prime ideals have common ramification index $e \geqslant 1$ and common inertial degree $f \geqslant 1$ over $\mathfrak{p}$. Also, $efg = [\mathbb{L} : \mathbb{K}] = |\mathrm{Gal}(\mathbb{L}/\mathbb{K})|$. As $\mathfrak{p}$ does not divide $m\mathcal{O}_{\mathbb{K}}$, it is unramified in $\mathcal{O}_{\mathbb{K}(\zeta)}$ (Proposition 3.12), so it is also unramified in $\mathcal{O}_{\mathbb{L}}$ (Proposition 2.5), and thus $e = 1$. We also know that f is the order of the element $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]$ in $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ (Corollary 2.24), and that $N(\mathfrak{P}) = N(\mathfrak{p})^f$ for all prime ideals $\mathfrak{P}$ of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{p}$. Finally $|\mathrm{Gal}(\mathbb{L}/\mathbb{K})| = [\mathrm{Gal}(\mathbb{L}/\mathbb{K}) : G]\,|G| = n|G|$, and so $g = n|G|/f$. Putting this all together, we find that

$$\prod_{\mathfrak{P} \,|\, \mathfrak{p}\mathcal{O}_{\mathbb{L}}} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right) = \left(1 - \frac{1}{N(\mathfrak{p})^{sf}}\right)^{n|G|/f} = \prod_{\chi \in \widehat{G}} \left(1 - \frac{\chi(\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right])}{N(\mathfrak{p})^s}\right)^n, \tag{4.4.2}$$

where the second equality follows by setting $X = N(\mathfrak{p})^{-s}$ and $\sigma = \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]$ in Proposition A.8. Taking the reciprocal of both sides of (4.4.2), then taking the product of the result over all prime ideals $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ which do not divide $\mathfrak{m}_0$, and finally noting that $\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\tilde{\mathfrak{p}}}\right]_{\mathfrak{m}}} = \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]$, we get

$$\zeta_{\mathbb{L}}^{\mathfrak{M}}(s) = \prod_{\mathfrak{p} \nmid \mathfrak{m}_0} \prod_{\mathfrak{P} \,|\, \mathfrak{p}\mathcal{O}_{\mathbb{L}}} \left(1 - \frac{1}{N(\mathfrak{P})^s}\right)^{-1} = \prod_{\mathfrak{p} \nmid \mathfrak{m}_0} \prod_{\chi \in \widehat{G}} \left(1 - \frac{\chi(\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\tilde{\mathfrak{p}}}\right]_{\mathfrak{m}}})}{N(\mathfrak{p})^s}\right)^{-n},$$

where the first equality holds by generalised associativity because the Euler product defining $\zeta_{\mathbb{L}}^{\mathfrak{M}}(s)$ is absolutely convergent. Applying generalised associativity again to the Euler product on the right-hand side, the result follows. □

Proposition 4.24. *Assume the same notation as Proposition 4.23. Then*

(i) $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$; and

(ii) $L^{\mathfrak{m}}_{\mathbb{K}}(1, \chi \circ \overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}) \neq 0$ *for all non-trivial characters* χ *of* G.

Proof. The left and right-hand sides of (4.4.1) are meromorphic functions of s on $H\big(1 - \frac{1}{[\mathbb{L}:\mathbb{Q}]}\big)$. Equating the orders of these functions at $s = 1$, we get

$$\operatorname{ord}_{s=1}\big(\zeta^{\mathfrak{M}}_{\mathbb{L}}(s)\big) = n \sum_{\chi \in \widehat{G}} \operatorname{ord}_{s=1}\big(L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}})\big). \tag{4.4.3}$$

From Proposition 4.21 and Definition 4.5, we know that $\operatorname{ord}_{s=1}\big(\zeta^{\mathfrak{M}}_{\mathbb{L}}(s)\big) = -1$.

Also from Proposition 4.21, the order of $L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi \circ \overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}})$ at $s = 1$ is -1 if χ is the trivial character of G, and otherwise it is non-negative. Here, we have used the fact that χ is the trivial character of G if and only if $\chi \circ \overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}$ is the trivial character of $\mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}$. The "only if" direction is obvious. Conversely, suppose that χ is not the trivial character of G. Then there is a $\sigma \in G$ such that $\chi(\sigma) \neq 1$. As G is the image of $\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}$, there is a $\mathcal{K} \in \mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}$ such that $\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\mathcal{K}}\right]_{\mathfrak{m}}} = \sigma$, and so $\chi(\overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\mathcal{K}}\right]_{\mathfrak{m}}}) = \chi(\sigma) \neq 1$. Hence $\chi \circ \overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}$ is not the trivial character of $\mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}$.

Putting this all together, (4.4.3) becomes

$$-1 = n\Big(-1 + \sum_{\chi \in \widehat{G}\setminus\{\chi_1\}} \operatorname{ord}_{s=1}\big(L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}})\big)\Big).$$

Hence n divides -1. As $n \geqslant 0$, this means that $n = 1$, and so $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Also,

$$0 = \sum_{\chi \in \widehat{G}\setminus\{\chi_1\}} \operatorname{ord}_{s=1}\big(L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}})\big),$$

and as no term in the sum is negative, they must all be zero. Hence, for all non-trivial characters χ of G, we have $L^{\mathfrak{m}}_{\mathbb{K}}(1, \chi \circ \overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}) \neq 0$. □

4.5 Chebotarev's density theorem for cyclotomic extensions

In this section, we finally prove Chebotarev's density theorem for cyclotomic extensions. Along the way we also prove that the Dirichlet density of a set of prime ideals is given by an alternate formula; the alternate formula is easier to work with and will be used multiple times throughout the rest of this thesis. Both of these results arise from an exploration of the asymptotic properties near $s = 1$ of the function $\ell^{\mathfrak{m}}_{\mathbb{K}}(s, \chi)$, defined momentarily, which we think of as the logarithm of the Weber L-function $L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi)$ (although we do not claim that $\ell^{\mathfrak{m}}_{\mathbb{K}}(s, \chi)$ is the composition of any particular branch of the complex logarithm function with $L^{\mathfrak{m}}_{\mathbb{K}}(s, \chi)$). The function $\ell^{\mathfrak{m}}_{\mathbb{K}}(s, \chi \circ \overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}})$, for a suitable choice of the modulus $\mathfrak{m}$, is the function that, in the introduction to this chapter, we claimed differs from a series of the form (4.0.3) by a bounded function of s — this is what we show in Proposition 4.32. Our final proof of Chebotarev's density theorem (Theorem 4.36) uses the clever application of the second orthogonality relation (Proposition A.11) that we already saw in (4.0.2) to compute the Dirichlet density of interest with the analytic properties of the functions $\ell^{\mathfrak{m}}_{\mathbb{K}}(s, \chi \circ \overline{\left[\frac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}})$.

Definition/Proposition 4.25. Let $\mathbb{K}$ be a number field, let $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ be a modulus of $\mathbb{K}$, let $\chi \in \widehat{\mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}}$, and let $s \in H(1)$. Then the series $\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)$ defined by

$$\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi) = -\sum_{\mathfrak{p}\nmid\mathfrak{m}_0} \mathrm{Log}\left(1 - \frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right)$$

is absolutely convergent, and it satisfies

$$L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi) = e^{\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)}.$$

Proof. Recall that $L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)$ is given by the absolutely convergent product

$$L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi) = \prod_{\mathfrak{p}\nmid\mathfrak{m}_0} \left(1 - \frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right)^{-1}.$$

By Proposition B.13, $L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)^{-1}$ is given by the absolutely convergent product

$$L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)^{-1} = \prod_{\mathfrak{p}\nmid\mathfrak{m}_0} \left(1 - \frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right).$$

As the product for $L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)^{-1}$ converges, by Proposition B.7 the series $-\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)$ also converges and

$$L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)^{-1} = e^{-\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)}.$$

Actually, as the product for $L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)^{-1}$ converges *absolutely*, by the definition of absolute convergence of an infinite product (Definition B.9), we have absolute convergence of the series $-\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)$, and thus also of the series $\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)$. □

Proposition 4.26. *Let $\mathbb{K}$ be a number field, let $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ be a modulus of $\mathbb{K}$, let $\chi \in \widehat{\mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}}$, and let $s \in H(1)$. Then*

$$\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi) = \sum_{\mathfrak{p}\nmid\mathfrak{m}_0} \sum_{k=1}^{\infty} \frac{1}{k} \left(\frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right)^k.$$

Proof. For each prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ not dividing $\mathfrak{m}_0$, the power series expansion

$$\mathrm{Log}\left(1 - \frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right) = -\sum_{k=1}^{\infty} \frac{1}{k} \left(\frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right)^k$$

holds because $|\chi(\tilde{\mathfrak{p}})N(\mathfrak{p})^{-s}| < 1$ (Theorem 4.11). The result follows by applying this expansion to each term in the series defining $\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)$. □

Proposition 4.27. *Let $\mathbb{K}$ be a number field, let $\mathfrak{m}$ be a modulus of $\mathbb{K}$, and let $\chi \in \widehat{\mathrm{Cl}^{\mathfrak{m}}_{\mathbb{K}}}$. Then $\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)$ is a holomorphic function of s on $H(1)$.*

Proof. By Theorem 4.7, it suffices to show that the series defining $\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)$ is uniformly convergent on compact subsets of $H(1)$. As each compact subset of $H(1)$ is contained in a closed halfplane of the form $\overline{H(1+\epsilon)}$ for some $\epsilon > 0$, we only need

to show uniform convergence on sets of this form. Let $\epsilon > 0$, let $s \in \overline{H(1+\epsilon)}$, and let $\sigma = \mathrm{Re}(s)$. As $\sigma \geqslant 1+\epsilon$, and using Proposition 4.26, the modulus of the $\mathfrak{p}$-th term of the series defining $\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)$ satisfies

$$\left|\sum_{k=1}^{\infty} \frac{1}{k}\left(\frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s}\right)^k\right| \leqslant \sum_{k=1}^{\infty} \frac{1}{k}\left(\frac{1}{N(\mathfrak{p})^\sigma}\right)^k \leqslant \sum_{k=1}^{\infty} \frac{1}{k}\left(\frac{1}{N(\mathfrak{p})^{1+\epsilon}}\right)^k.$$

But the right-hand side is the modulus of the $\mathfrak{p}$-th term of the absolutely convergent series defining $\ell^{\mathfrak{m}}_{\mathbb{K}}(1+\epsilon,\chi_1)$. The uniform convergence of $\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi)$ on $\overline{H(1+\epsilon)}$ follows by the Weierstrass M-test. □

The rest of this chapter involves an investigation of the asymptotic behaviour of several complex functions of s near $s = 1$. It will be convenient for us to use big-oh notation, which is defined for complex functions at a point as follows.

Definition 4.28. Let $S \subseteq \mathbb{C}$, and let $s_0 \in \mathbb{C}$ be a limit point of S. Given functions f, g and h defined on S, with f and g complex valued and h positive real valued,

$$f(s) = g(s) + O\big(h(s)\big) \qquad \text{as } s \to s_0 \text{ in } S$$

if there are positive real numbers δ and C such that

$$|f(s) - g(s)| \leqslant Ch(s) \qquad \forall s \in S \cap B^\circ(s_0,\delta).$$

Remark 4.29. Recall that we say that $f(s) \to \ell$ as $s \to s_0$ in S if for all $\epsilon > 0$, there is a $\delta > 0$ such that if $s \in S \cap B^\circ(s_0,\delta)$, then $f(s) \in B(\ell,\epsilon)$. Clearly if $f(s) \to \ell$ as $s \to s_0$ in S, then $f(s) = O(1)$ as $s \to s_0$ in S.

Remark 4.30. In Remark 2.35, we declared that the variable s would always be complex, whilst the variable σ would always be real. By writing "as $s \to 1^+$", we mean "as $s \to 1$ in $H(1)$". By writing "as $\sigma \to 1^+$", we mean "as $\sigma \to 1$ in $(1,\infty)$".

Proposition 4.31. *Let $\mathbb{K}$ be a number field and let $\mathfrak{m}$ be a modulus of $\mathbb{K}$. Then*

$$\ell^{\mathfrak{m}}_{\mathbb{K}}(s,\chi_1) = -\mathrm{Log}(s-1) + O(1) \qquad \textit{as } s \to 1^+.$$

Proof. As $L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi_1)$ has a simple pole at $s = 1$ with residue $\rho = h^{\mathfrak{m}}_{\mathbb{K}}\rho^{\mathfrak{m}}_{\mathbb{K}} > 0$, we have

$$\lim_{s\to 1}\big((s-1)L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi_1)\big) = \rho$$

by Theorem 4.12. In particular, there is a $\delta > 0$ such that $(s-1)L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi_1) \in B(\rho,\frac{1}{2}\rho)$ whenever $s \in B^\circ(1,\delta) \cap H\big(1-\frac{1}{[\mathbb{K}:\mathbb{Q}]}\big)$, and we may assume, without loss of generality, that $\delta < \frac{1}{[\mathbb{K}:\mathbb{Q}]}$. Refer to Figure 4.2. As $\rho > 0$, clearly $B(\rho,\frac{1}{2}\rho) \subseteq \mathbb{C}\backslash(-\infty,0]$, and so Log is continuous on $B(\rho,\frac{1}{2}\rho)$ (Theorem 4.10). Hence the composite function

$$f\colon B^\circ(1,\delta) \to \mathbb{C} \qquad \text{given by} \qquad f(s) = \mathrm{Log}\big((s-1)L^{\mathfrak{m}}_{\mathbb{K}}(s,\chi_1)\big)$$

is continuous, and satisfies

$$\lim_{s\to 1} f(s) = \mathrm{Log}(\rho).$$

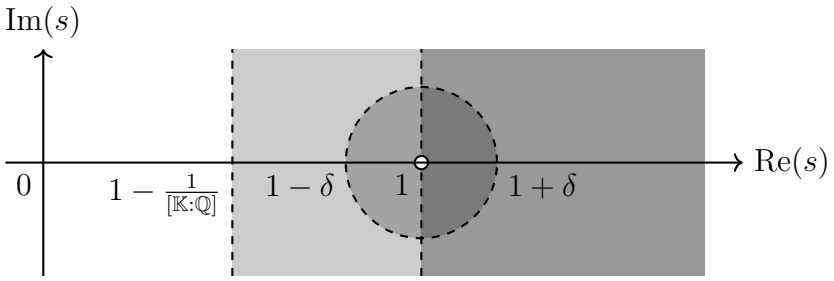


Figure 4.2: Equation (4.5.2) holds on the open halfplane to the right of the line $\mathrm{Re}(s) = 1$ and (4.5.1) holds in the punctured disk centred at 1 of radius δ.

For all $s \in H(1)$, we have

$$e^{\mathrm{Log}(s-1)+\ell_{\mathbb{K}}^{\mathfrak{m}}(s,\chi_1)} = e^{\mathrm{Log}(s-1)}e^{\ell_{\mathbb{K}}^{\mathfrak{m}}(s,\chi_1)} = (s-1)L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi_1). \tag{4.5.1}$$

Also, for all $s \in B^\circ(1,\delta)$, we have

$$e^{f(s)} = e^{\mathrm{Log}[(s-1)L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi_1)]} = (s-1)L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi_1). \tag{4.5.2}$$

Hence, for all $s \in H(1) \cap B^\circ(1,\delta)$, we have

$$e^{\mathrm{Log}(s-1)+\ell_{\mathbb{K}}^{\mathfrak{m}}(s,\chi_1)} = (s-1)L_{\mathbb{K}}^{\mathfrak{m}}(s,\chi_1) = e^{f(s)}.$$

Thus, for all $s \in H(1) \cap B^\circ(1,\delta)$, there is an $n_s \in \mathbb{Z}$ such that

$$\mathrm{Log}(s-1) + \ell_{\mathbb{K}}^{\mathfrak{m}}(s,\chi_1) = f(s) + 2n_s\pi i.$$

As

$$n_s = \frac{1}{2\pi i}\big(\mathrm{Log}(s-1) + \ell_{\mathbb{K}}^{\mathfrak{m}}(s,\chi_1) - f(s)\big)$$

is a continuous function of s on $H(1) \cap B^\circ(1,\delta)$ with a discrete image, it is actually constant, and so we may write $n_s = n$ where n is independent of s. Hence

$$\lim_{s\to 1^+}\big(\mathrm{Log}(s-1) + \ell_{\mathbb{K}}^{\mathfrak{m}}(s,\chi_1)\big) = \lim_{s\to 1^+}\big(2n\pi i + f(s)\big) = 2n\pi i + \mathrm{Log}(\rho). \qquad \square$$

Proposition 4.32. *Let $\mathbb{K}$ be a number field, let $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ be a modulus of $\mathbb{K}$, and let $\chi \in \widehat{\mathrm{Cl}_{\mathbb{K}}^{\mathfrak{m}}}$. Then*

$$\ell_{\mathbb{K}}^{\mathfrak{m}}(s,\chi) = \sum_{\mathfrak{p}\nmid\mathfrak{m}_0} \frac{\chi(\tilde{\mathfrak{p}})}{N(\mathfrak{p})^s} + O(1) \quad \text{as } s \to 1^+.$$

Proof. From Proposition 4.26, we need to show that

$$\sum_{\mathfrak{p}\nmid\mathfrak{m}_0}\sum_{k=2}^{\infty} \frac{\chi(\tilde{\mathfrak{p}})^k}{kN(\mathfrak{p})^{sk}} = O(1) \qquad \text{as } s \to 1^+.$$

Let $s \in H(1)$, and let $\sigma = \mathrm{Re}(s)$. Also let $n = [\mathbb{K} : \mathbb{Q}]$. We have

$$\left|\sum_{\mathfrak{p}\nmid\mathfrak{m}_0}\sum_{k=2}^{\infty}\frac{\chi(\tilde{\mathfrak{p}})^k}{kN(\mathfrak{p})^{sk}}\right| \leqslant \sum_{\mathfrak{p}\nmid\mathfrak{m}_0}\sum_{k=2}^{\infty}\left|\frac{\chi(\tilde{\mathfrak{p}})^k}{kN(\mathfrak{p})^{sk}}\right| = \sum_{\mathfrak{p}\nmid\mathfrak{m}_0}\sum_{k=2}^{\infty}\frac{1}{kN(\mathfrak{p})^{\sigma k}} \leqslant \sum_{\mathfrak{p}}\sum_{k=2}^{\infty}\frac{1}{N(\mathfrak{p})^{\sigma k}}$$
$$= \sum_{p}\sum_{\mathfrak{p}\,|\,p}\sum_{k=2}^{\infty}\frac{1}{N(\mathfrak{p})^{\sigma k}} \leqslant \sum_{p}\sum_{\mathfrak{p}\,|\,p}\sum_{k=2}^{\infty}\frac{1}{p^{\sigma k}} \leqslant n\sum_{p}\sum_{k=2}^{\infty}\frac{1}{p^{\sigma k}},$$

where the reindexing between the first and second line is possible because every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ lies over exactly one prime ideal $p\mathbb{Z}$, the following inequality holds as $N(\mathfrak{p}) = p^{f(\mathfrak{p}|p\mathbb{Z})} \geqslant p$, and the final inequality holds because there are at most $n = [\mathbb{K} : \mathbb{Q}]$ prime ideals $\mathfrak{p}$ above a given prime ideal $p\mathbb{Z}$. For all prime numbers p, we have $p^\sigma \geqslant 2$ because $p \geqslant 2$ and $\sigma \geqslant 1$, and so $0 < \frac{1}{p^\sigma} \leqslant \frac{1}{2}$, which means that $1 > 1 - \frac{1}{p^\sigma} \geqslant \frac{1}{2}$, and thus $1 < (1 - \frac{1}{p^\sigma})^{-1} \leqslant 2$. Hence

$$\sum_{k=2}^{\infty}\frac{1}{p^{\sigma k}} = \frac{1}{p^{2\sigma}}\left(\frac{1}{1-\frac{1}{p^\sigma}}\right) \leqslant 2\frac{1}{p^2},$$

as the left-hand side is a geometric series of ratio $p^{-\sigma} < 1$. It follows that

$$\left|\sum_{\mathfrak{p}\nmid\mathfrak{m}_0}\sum_{k=2}^{\infty}\frac{\chi(\tilde{\mathfrak{p}})^k}{kN(\mathfrak{p})^{sk}}\right| \leqslant n\sum_{p}\sum_{k=2}^{\infty}\frac{1}{p^{\sigma k}} \leqslant 2n\sum_{p}\frac{1}{p^2} \leqslant 2n\sum_{j=1}^{\infty}\frac{1}{j^2},$$

where the right-hand side converges as it is a p-series with $p = 2 > 1$. □

In the next proposition, from what we have already shown, we will derive an alternate formula for the Dirichlet density. As an immediate corollary, the Dirichlet density of a finite set is zero, and we will use both the alternate formula and the corollary in our final proof of the cyclotomic case of Chebotarev's density theorem, as well as in Chapter 5 when we reduce the general case to the cyclic case.

Lemma 4.33. *Let f be a complex function whose domain includes $H(1)$. Suppose that $f(s) = -\mathrm{Log}(s-1) + O(1)$ as $s \to 1^+$. Then*

$$\lim_{s\to 1^+}\frac{f(s)}{-\mathrm{Log}(s-1)} = 1.$$

Proof. There are positive real numbers C and δ such that $|f(s) + \mathrm{Log}(s-1)| \leqslant C$ for all $s \in H(1) \cap B^\circ(1,\delta)$. So, for all $s \in H(1) \cap B^\circ(1,\delta)$, we have

$$\left|\frac{f(s)}{-\mathrm{Log}(s-1)} - 1\right| \leqslant \frac{C}{|-\mathrm{Log}(s-1)|}. \tag{4.5.3}$$

Now $|-\mathrm{Log}(s-1)| \to \infty$ as $s \to 1^+$, and so the right-hand side of (4.5.3) goes to 0 as $s \to 1^+$. By the pinching theorem, the left-hand side of (4.5.3) also goes to 0 as $s \to 1^+$, and the result follows. □

Proposition 4.34. *Let $\mathbb{K}$ be a number field, and let $A \subseteq P(\mathbb{K})$. Then*

$$\delta(A) = \lim_{\sigma \to 1^+} \frac{\sum_{\mathfrak{p} \in A} N(\mathfrak{p})^{-\sigma}}{-\ln(\sigma - 1)}.$$

That is, the Dirichlet density $\delta(A)$ of A exists if and only if the above limit exists, and in this case, their values coincide.

Proof. Recall that $\delta(A)$ is defined by the limit

$$\delta(A) = \lim_{\sigma \to 1^+} \frac{\sum_{\mathfrak{p} \in A} N(\mathfrak{p})^{-\sigma}}{\sum_{\mathfrak{p} \in P(\mathbb{K})} N(\mathfrak{p})^{-\sigma}}.$$

Hence, it suffices to show that

$$\lim_{\sigma \to 1^+} \frac{\sum_{\mathfrak{p} \in P(\mathbb{K})} N(\mathfrak{p})^{-\sigma}}{-\ln(\sigma - 1)} = 1.$$

We will actually show that the corresponding complex limit (i.e. replacing σ with s) holds, from which the real limit follows. By Lemma 4.33, it suffices to show that

$$\sum_{\mathfrak{p} \in P(\mathbb{K})} N(\mathfrak{p})^{-s} = -\mathrm{Log}(s - 1) + O(1) \qquad \text{as } s \to 1^+.$$

Let $\mathfrak{m} = \mathfrak{m}_0 \cdot \mathfrak{m}_\infty$ be any modulus of $\mathbb{K}$. From Proposition 4.32, we have

$$\ell_{\mathbb{K}}^{\mathfrak{m}}(s, \chi_1) = \sum_{\mathfrak{p} \nmid \mathfrak{m}_0} N(\mathfrak{p})^{-s} + O(1) = \sum_{\mathfrak{p} \in P(\mathbb{K})} N(\mathfrak{p})^{-s} + O(1) \qquad \text{as } s \to 1^+,$$

where the series on either side of the second equality differ by a finite sum as only finitely many prime ideals divide $\mathfrak{m}_0$. From Proposition 4.31, we also have

$$\ell_{\mathbb{K}}^{\mathfrak{m}}(s, \chi_1) = -\mathrm{Log}(s - 1) + O(1) \qquad \text{as } s \to 1^+. \qquad \square$$

Corollary 4.35. *Let $\mathbb{K}$ be a number field, and let $A \subseteq P(\mathbb{K})$. If*

$$\sum_{\mathfrak{p} \in A} N(\mathfrak{p})^{-\sigma} = O(1) \qquad \text{as } \sigma \to 1^+,$$

then $\delta(A) = 0$. In particular, if A is finite, then $\delta(A) = 0$.

Proof. Suppose that there is a positive constant C such that $\left|\sum_{\mathfrak{p} \in A} N(\mathfrak{p})^{-\sigma}\right| \leqslant C$ for all $\sigma \in (1, \infty)$ close enough to 1. If $\sigma \in (1, \infty)$ is close enough to 1, then

$$0 \leqslant \left| \frac{\sum_{\mathfrak{p} \in A} N(\mathfrak{p})^{-s}}{-\ln(\sigma - 1)} \right| \leqslant \frac{C}{|\ln(\sigma - 1)|},$$

and the right-hand side tends to 0 as $\sigma \to 1^+$. By the pinching theorem and Proposition 4.34, the result follows. $\square$

Theorem 4.36 (Chebotarev's density theorem for cyclotomic extensions)**.** *Let $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{K}(\zeta)$ be a tower of number fields, where $\zeta \in \mathbb{C}$ is a primitive m-th root of unity. Let $G = \mathrm{Gal}(\mathbb{L}/\mathbb{K})$, let $\tau \in G$, and let*

$$P = \left\{\mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \text{ unramified in } \mathbb{L}, \left(\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = \{\tau\}\right\}.$$

Then

$$\delta(P) = \frac{1}{|G|}.$$

Proof. Let $\mathfrak{m}$ be the modulus $m\mathcal{O}_{\mathbb{K}} \cdot \infty$ of $\mathbb{K}$. Let

$$P' = \left\{\mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \in \mathcal{I}_{\mathbb{K}}^{\mathfrak{m}}, \ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]_{\mathfrak{m}}} = \tau\right\} = \left\{\mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \nmid m\mathcal{O}_{\mathbb{K}}, \ \left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right] = \tau\right\}.$$

By Proposition 3.12, all prime ideals of $\mathcal{O}_{\mathbb{K}}$ which do not divide $m\mathcal{O}_{\mathbb{K}}$ are unramified in $\mathcal{O}_{\mathbb{L}}$, and so $P' \subseteq P$. Also, by Corollary 4.35, $\delta(P \backslash P') = 0$ because the set $P \backslash P'$ is finite. Hence, if $\delta(P')$ exists, then so does $\delta(P)$, and $\delta(P) = \delta(P')$ (Proposition 2.47). If we can show that

$$\lim_{\sigma \to 1^+} \frac{\sum_{\mathfrak{p} \in P'} N(\mathfrak{p})^{-\sigma}}{-\ln(\sigma - 1)} = \frac{1}{|G|},$$

then Proposition 4.34 will imply that $\delta(P') = 1/|G|$. It suffices to show that the corresponding complex limit (i.e. replacing σ with s) holds. By Lemma 4.33, it suffices in turn to show that

(1) $f(s) = |G| \sum_{\mathfrak{p} \in P'} N(\mathfrak{p})^{-s} + O(1)$ as $s \to 1^+$, and

(2) $f(s) = -\mathrm{Log}(s-1) + O(1)$ as $s \to 1^+$,

where

$$f(s) = \sum_{\chi \in \widehat{G}} \chi(\tau^{-1}) \ell_{\mathbb{K}}^{\mathfrak{m}}(s, \chi \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}).$$

For (1), Proposition 4.32 implies that

$$\begin{aligned} f(s) &= \sum_{\chi \in \widehat{G}} \chi(\tau^{-1}) \Big(\sum_{\mathfrak{p} \nmid \mathfrak{m}_0} \chi(\left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]) N(\mathfrak{p})^{-s} + O(1) \Big) \\ &= \sum_{\mathfrak{p} \nmid \mathfrak{m}_0} \Big(\sum_{\chi \in \widehat{G}} \chi(\tau^{-1}) \chi(\left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]) \Big) N(\mathfrak{p})^{-s} + O(1) \\ &= |G| \sum_{\mathfrak{p} \in P'} N(\mathfrak{p})^{-s} + O(1) \end{aligned}$$

as $s \to 1^+$. Here, the last equality is where we used the second orthogonality relation (Proposition A.11), which, in this case, says that

$$\sum_{\chi \in \widehat{G}} \chi(\tau^{-1}) \chi(\left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right]) = \begin{cases} |G| & \text{if } \tau = \left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right], \\ 0 & \text{otherwise.} \end{cases}$$

For (2), by Proposition 4.31, we know that

$$\ell_{\mathbb{K}}^{\mathfrak{m}}(s, \chi_1 \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}) = -\mathrm{Log}(s-1) + O(1) \qquad \text{as } s \to 1^+.$$

Also, Proposition 4.24 implies that

$$\exp\left(\ell_{\mathbb{K}}^{\mathfrak{m}}(1, \chi \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}})\right) = L_{\mathbb{K}}^{\mathfrak{m}}(1, \chi \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}) \in \mathbb{C}\backslash\{0\}$$

whenever χ is a non-trivial character of G. Thus, in this case,

$$\ell_{\mathbb{K}}^{\mathfrak{m}}(s, \chi \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}) = O(1) \qquad \text{as } s \to 1^+.$$

Note also that $\chi_1(\tau^{-1}) = 1$. Hence, as $s \to 1^+$, we have

$$\begin{aligned} f(s) &= \chi_1(\tau^{-1})\ell_{\mathbb{K}}^{\mathfrak{m}}(s, \chi_1 \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}) + \sum_{\chi \in \widehat{G}\backslash\{\chi_1\}} \chi(\tau^{-1})\ell_{\mathbb{K}}^{\mathfrak{m}}(s, \chi \circ \overline{\left[\tfrac{\mathbb{L}/\mathbb{K}}{\cdot}\right]_{\mathfrak{m}}}) \\ &= 1 \cdot \big(-\mathrm{Log}(s-1) + O(1)\big) + \sum_{\chi \in \widehat{G}\backslash\{\chi_1\}} \chi(\tau^{-1}) \cdot O(1) \\ &= -\mathrm{Log}(s-1) + O(1). \end{aligned}$$

□

Chapter 5

Deuring's reduction to the cyclic case

We will use the following notation throughout this section. Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of number fields with Galois group G. Let $\tau \in G$, let $H = \langle \tau \rangle$ and let $\mathbb{M} = \mathbb{L}^H$ so that the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{M})$ is H by the fundamental theorem of Galois theory. Let

$$P = \left\{ \mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \text{ is unramified in } \mathcal{O}_{\mathbb{L}} \text{ and } \left(\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = C \right\},$$

where C is the conjugacy class of τ in G. Similarly, let

$$Q = \left\{ \mathfrak{q} \in P(\mathbb{M}) : \ \mathfrak{q} \text{ is unramified in } \mathcal{O}_{\mathbb{L}} \text{ and } \left(\tfrac{\mathbb{L}/\mathbb{M}}{\mathfrak{q}}\right) = \{\tau\} \right\},$$

where $\{\tau\}$ is the conjugacy class of τ in H because H is abelian. Let

$$n = \frac{|G|}{|C||H|}.$$

In this chapter, we will prove the following theorem, due to Deuring [9], which relates the Dirichlet densities of the sets P and Q. Along the way, we will also show that n is an integer.

Theorem 5.1. *The Dirichlet density of P exists if and only if the Dirichlet density of Q exists, and in this case they satisfy*

$$\delta(Q) = n\,\delta(P).$$

Chebotarev's density theorem implies that the Dirichlet densities of P and Q exist, and that they satisfy

$$\delta(P) = \frac{|C|}{|G|} \qquad \text{and} \qquad \delta(Q) = \frac{1}{|H|}.$$

Hence Theorem 5.1 is consistent with Chebotarev's density theorem.

Throughout this chapter, let

$$Q' = \{ \mathfrak{q} \in Q : \ e(\mathfrak{q}|\mathfrak{q} \cap \mathbb{K}) = f(\mathfrak{q}|\mathfrak{q} \cap \mathbb{K}) = 1 \}.$$

Proposition 5.2. *The Dirichlet density of Q' exists if and only if the Dirichlet density of Q exists, and in this case,*

$$\delta(Q') = \delta(Q).$$

Proof. Let $Q_e = \{\mathfrak{q} \in Q : e(\mathfrak{q}|\mathfrak{q} \cap \mathbb{K}) \geqslant 2\}$ and $Q_f = \{\mathfrak{q} \in Q : f(\mathfrak{q}|\mathfrak{q} \cap \mathbb{K}) \geqslant 2\}$. Notice that Q', Q_f and $Q_e \backslash Q_f$ are pairwise disjoint, and

$$Q = Q' \cup Q_f \cup (Q_e \backslash Q_f).$$

We will show that $\delta(Q_f) = 0$ and that $\delta(Q_e \backslash Q_f) = 0$, from which a double application of Proposition 2.47 gives the desired result.

First, we show that $\delta(Q_f) = 0$. For each prime ideal $p\mathbb{Z}$ of $\mathbb{Z}$, there are at most $[\mathbb{M} : \mathbb{Q}]$ prime ideals $\mathfrak{q}$ of $\mathcal{O}_\mathbb{M}$ above $p\mathbb{Z}$. If $\mathfrak{q} \in Q_f$ is a prime ideal above $p\mathbb{Z}$ then the absolute norm $N(\mathfrak{q}) = p^{f(\mathfrak{q}|p\mathbb{Z})} = p^{f(\mathfrak{q}|\mathfrak{q}\cap\mathbb{K})f(\mathfrak{q}\cap\mathbb{K}|p\mathbb{Z})}$ is at least p^2 because $f(\mathfrak{q}|\mathfrak{q} \cap \mathbb{K}) \geqslant 2$. Hence, for all $\sigma \in (1, \infty)$, we have

$$\sum_{\mathfrak{q} \in Q_f} N(\mathfrak{q})^{-\sigma} \leqslant [\mathbb{M} : \mathbb{Q}] \sum_{p\mathbb{Z} \in P(\mathbb{Q})} p^{-2\sigma} \leqslant [\mathbb{M} : \mathbb{Q}] \sum_{n=1}^{\infty} n^{-2},$$

where the right-hand side is a convergent p-series. By Corollary 4.35, $\delta(Q_f) = 0$.

We now show that $\delta(Q_e \backslash Q_f) = 0$. Notice that the set Q_e is finite because there are only finitely many non-zero prime ideals of $\mathcal{O}_\mathbb{K}$ which are ramified in $\mathcal{O}_\mathbb{M}$ (Corollary 2.8), and only finitely many prime ideals of $\mathcal{O}_\mathbb{M}$ above any given non-zero prime ideal of $\mathcal{O}_\mathbb{K}$. Hence, the subset $Q_e \backslash Q_f$ of Q_e is also finite, and so $\sum_{\mathfrak{q} \in Q_e \backslash Q_f} N(\mathfrak{q})^{-1}$ converges. By Corollary 4.35, $\delta(Q_e \backslash Q_f) = 0$. □

To prove Theorem 5.1, it suffices by Proposition 5.2 to instead prove the following result.

Proposition 5.3. *The Dirichlet density of P exists if and only if the Dirichlet density of Q' exists, and in this case they satisfy*

$$\delta(Q') = n\,\delta(P).$$

To prove Proposition 5.3, we begin by constructing a surjective, n-to-1 function $\upsilon \colon Q' \to P$ which preserves absolute ideal norms. Let

$$R = \left\{\mathfrak{P} \in P(\mathbb{L}) : \left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right] = \tau,\ e(\mathfrak{P}|\mathfrak{P} \cap \mathbb{K}) = 1\right\}.$$

Let $\varphi \colon R \to P$ be defined by $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathbb{K}$ for all $\mathfrak{P} \in R$, and let $\psi \colon R \to Q'$ be defined by $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathbb{M}$ for all $\mathfrak{P} \in R$. In the following lemmas, we show that ψ and φ are well defined, that ψ is bijective, and that $\upsilon = \varphi \circ \psi^{-1}$ satisfies the desired properties.

Lemma 5.4. *The number n is an integer, and φ is a surjective, n-to-1 function.*

To prove this lemma, we will make use of the notion of the centraliser of a group, which we recall here for the reader's convenience.

Definition 5.5. Let G be a group, and let $\sigma \in G$. The *centraliser* $C_G(\sigma)$ of σ in G is the set $\{\rho \in G : \sigma\rho = \rho\sigma\}$.

In particular, we will need to know the relationship between the size of the centraliser of an element and the size of its conjugacy class.

Lemma 5.6. *Let G be a group, let $\sigma \in G$, and let C be the conjugacy class of σ in G. Then $|G| = |C_G(\sigma)||C|$.*

Proof. The group G acts on the set G via conjugation. Under this action, the orbit of σ is C and the stabiliser of σ is $C_G(\sigma)$. By the orbit-stabiliser theorem (Theorem 2.20), $|G| = |C_G(\sigma)||C|$. □

We may now return to prove Lemma 5.4.

Proof of Lemma 5.4. We begin by showing that φ is well defined. Let $\mathfrak{P} \in R$ and $\mathfrak{p} = \mathfrak{P} \cap \mathbb{K}$, so that $\mathfrak{p} = \varphi(\mathfrak{P})$. Then $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_\mathbb{K}$. Also, $\mathbb{L}/\mathbb{K}$ is Galois, so all prime ideals of $\mathcal{O}_\mathbb{L}$ above $\mathfrak{p}$ have the same ramification index over $\mathfrak{p}$ as $\mathfrak{P}$ (Corollary 2.17), that is, they all have ramification index 1, so $\mathfrak{p}$ is unramified in $\mathbb{L}$. Finally, as $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_\mathbb{L}$ above $\mathfrak{p}$, we know that the Artin symbol $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right)$ is the conjugacy class of the Frobenius element $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right] = \tau$ in G (Proposition 2.29), that is, $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = C$. So $\mathfrak{p} \in P$ as required.

It is clear that φ is surjective. Indeed, if $\mathfrak{p} \in P$, then $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = C$. As $\tau \in C$, this means that there is a prime ideal $\mathfrak{P}$ of $\mathcal{O}_\mathbb{L}$ above $\mathfrak{p}$ such that $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right] = \tau$ (Definition 2.28), and $e(\mathfrak{P}|\mathfrak{p}) = 1$ because $\mathfrak{p}$ is unramified in $\mathcal{O}_\mathbb{L}$. Hence $\mathfrak{P} \in R$, and $\varphi(\mathfrak{P}) = \mathfrak{p}$.

Finally, we show that φ is n-to-1. Let $\mathfrak{p} \in \operatorname{im}\varphi$, and let $Y = \varphi^{-1}(\{\mathfrak{p}\})$. As $\mathfrak{p} \in \operatorname{im}\varphi$, Y is non-empty. So let $\mathfrak{P} \in Y$. Let X be the set of prime ideals of $\mathcal{O}_\mathbb{L}$ above $\mathfrak{p}$. Recall that G acts transitively on the set X via $\rho \cdot \mathfrak{P}' = \rho(\mathfrak{P}')$ for all $\rho \in G$ and all $\mathfrak{P}' \in X$ (Proposition 2.16). As the centraliser $C_G(\tau)$ of τ is a subgroup of G, it follows that $C_G(\tau)$ acts on X with the same action as G. Clearly $Y \subseteq X$. We claim that Y is the orbit and H is the stabiliser of $\mathfrak{P}$ under the action of $C_G(\tau)$ on X, and we will apply the orbit-stabiliser theorem to conclude that $|Y| = n$.

The stabiliser of $\mathfrak{P}$ under the action of $C_G(\tau)$ is the set

$$\left\{\rho \in C_G(\tau) : \ \rho(\mathfrak{P}) = \mathfrak{P}\right\} = C_G(\tau) \cap D(\mathfrak{P}|\mathfrak{p}).$$

However, as $\mathfrak{p}$ is unramified in $\mathcal{O}_\mathbb{L}$, we know that the decomposition group $D(\mathfrak{P}|\mathfrak{p})$ is generated by the Frobenius element $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right] = \tau$ (Corollary 2.24). Also, if $\rho \in \langle\tau\rangle$, then ρ is a power of τ and thus commutes with τ, so $\rho \in C_G(\tau)$. Hence $\langle\tau\rangle \subseteq C_G(\tau)$. So the stabiliser of $\mathfrak{P}$ under the action of $C_G(\tau)$ is actually just $H = \langle\tau\rangle$.

We wish to show that Y is the orbit $\mathcal{O}$ of $\mathfrak{P}$ under the action of $C_G(\tau)$ on X. As $Y \subseteq R$, and $\mathfrak{P} \in Y$, we know that the Frobenius element $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]$ is τ. Note that both Y and $\mathcal{O}$ are subsets of X. So let $\mathfrak{P}' \in X$. The desired result follows from the following sequence of equivalent statements:

$$\begin{aligned}
\mathfrak{P}' \in \mathcal{O} &\iff \exists \rho \in C_G(\tau). \quad \mathfrak{P}' = \rho(\mathfrak{P}) && \text{(Definition of orbit)}\\
&\iff \exists \rho \in G. \quad \mathfrak{P}' = \rho(\mathfrak{P}) \text{ and } \rho\tau\rho^{-1} = \tau && \text{(Definition of centraliser)}\\
&\iff \exists \rho \in G. \quad \mathfrak{P}' = \rho(\mathfrak{P}) \text{ and } \rho\left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]\rho^{-1} = \tau && \left(\left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right] = \tau\right)\\
&\iff \exists \rho \in G. \quad \mathfrak{P}' = \rho(\mathfrak{P}) \text{ and } \left[\tfrac{\mathbb{L}/\mathbb{K}}{\rho(\mathfrak{P})}\right] = \tau && \text{(Proposition 2.27)}\\
&\iff \exists \rho \in G. \quad \mathfrak{P}' = \rho(\mathfrak{P}) \text{ and } \left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}'}\right] = \tau\\
&\iff \left[\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}'}\right] = \tau && (G \text{ acts transitively on } X)\\
&\iff \mathfrak{P}' \in Y.
\end{aligned}$$

By the orbit-stabiliser theorem (Theorem 2.20) and Lemma 5.6, it follows that

$$|Y| = \frac{|C_G(\tau)|}{|H|} = \frac{|G|/|C|}{|H|} = n,$$

and this also implies that n is an integer. □

Lemma 5.7. *The function ψ is well defined and bijective.*

Proof. We begin by showing ψ is well defined. Let $\mathfrak{P} \in R$, $\mathfrak{q} = \mathfrak{P} \cap \mathbb{M}$ and $\mathfrak{p} = \mathfrak{P} \cap \mathbb{K}$, so that $\mathfrak{q} = \psi(\mathfrak{P})$, $\mathfrak{p} = \varphi(\mathfrak{P})$, and $\mathfrak{P}$ lies above $\mathfrak{q}$, which lies above $\mathfrak{p}$. Then $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_{\mathbb{M}}$. As $\mathbb{L}/\mathbb{K}$ is Galois, $\mathbb{L}/\mathbb{M}$ is also Galois, so all the prime ideals of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{q}$ have the same ramification index e and inertial degree f over $\mathfrak{q}$ (Corollary 2.17). Now $e(\mathfrak{P}|\mathfrak{q})e(\mathfrak{q}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{p}) = 1$ (Proposition 2.5), so $e(\mathfrak{P}|\mathfrak{q}) = e(\mathfrak{q}|\mathfrak{p}) = 1$. As $\mathfrak{P}$ is one of the prime ideals of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{q}$, we know that $e = e(\mathfrak{P}|\mathfrak{q}) = 1$, and so $\mathfrak{q}$ is unramified in $\mathcal{O}_{\mathbb{L}}$. Let g be the number of prime ideals of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{q}$. As $\mathfrak{p} = \varphi(\mathfrak{P})$, we know that $D(\mathfrak{P}|\mathfrak{p}) = H$ from the proof of Lemma 5.4. If $\mathfrak{P}'$ is a prime ideal of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{q}$, then $\mathfrak{P}' = \rho(\mathfrak{P})$ for some $\rho \in H$ as H acts transitively on the prime ideals of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{q}$ (Proposition 2.16), but $\rho \in D(\mathfrak{P}|\mathfrak{p})$ which fixes $\mathfrak{P}$, so $\mathfrak{P}' = \mathfrak{P}$. Hence $\mathfrak{P}$ is the only prime ideal of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{q}$, and so $g = 1$. Now $\operatorname{ord}\tau = |H| = [\mathbb{L} : \mathbb{M}] = efg = f = f(\mathfrak{P}|\mathfrak{q})$, because $\langle\tau\rangle = H = \operatorname{Gal}(\mathbb{L}/\mathbb{M})$, and $\mathbb{L}/\mathbb{M}$ is Galois, and $e = g = 1$. But $D(\mathfrak{P}|\mathfrak{p}) = \langle\tau\rangle$, so $\operatorname{ord}\tau = f(\mathfrak{P}|\mathfrak{p})$ (Corollary 2.24). As $f(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{q})f(\mathfrak{q}|\mathfrak{p})$ (Proposition 2.5), it follows that $f(\mathfrak{q}|\mathfrak{p}) = 1$. Hence, we also have $\left[\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{P}}\right] = \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]^{f(\mathfrak{q}|\mathfrak{p})} = \tau^1 = \tau$ (Proposition 2.31), and thus $\left(\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{q}}\right)$ is the conjugacy class of τ in H, namely $\{\tau\}$. As $\mathfrak{q}$ is a prime ideal of $\mathcal{O}_{\mathbb{M}}$, $\mathfrak{q}$ is unramified in $\mathcal{O}_{\mathbb{L}}$, and $\left(\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{q}}\right) = \{\tau\}$, we have $\mathfrak{q} \in Q$. Additionally, we have shown that $e(\mathfrak{q}|\mathfrak{p}) = f(\mathfrak{q}|\mathfrak{p}) = 1$, so actually $\mathfrak{q} \in Q'$, and thus ψ is well defined.

In the previous paragraph, we also showed that $g = 1$. This means that for each $\mathfrak{q} \in \operatorname{im}\psi$, there is exactly one prime ideal of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{q}$. As every element of the preimage $\psi^{-1}(\{\mathfrak{q}\})$ is a prime ideal of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{q}$, we must have $|\psi^{-1}(\{\mathfrak{q}\})| \leqslant 1$, and so ψ is injective.

It remains to show ψ is surjective. Let $\mathfrak{q} \in Q'$. As $\mathfrak{q}$ is unramified in $\mathcal{O}_{\mathbb{L}}$ and $\left(\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{q}}\right) = \{\tau\}$, there is a prime ideal $\mathfrak{P}$ of $\mathcal{O}_{\mathbb{L}}$ lying above $\mathfrak{q}$ such that $\left[\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{P}}\right] = \tau$ and $e(\mathfrak{P}|\mathfrak{q}) = 1$. Let $\mathfrak{p} = \mathfrak{q} \cap \mathbb{K}$. As $\mathfrak{q} \in Q'$, we know that $e(\mathfrak{q}|\mathfrak{p}) = f(\mathfrak{q}|\mathfrak{p}) = 1$, so we have $e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\mathfrak{q})e(\mathfrak{q}|\mathfrak{p}) = 1$ (Proposition 2.5), and $\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right] = \left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{P}}\right]^{f(\mathfrak{q}|\mathfrak{p})} = \left[\frac{\mathbb{L}/\mathbb{M}}{\mathfrak{P}}\right] = \tau$ (Proposition 2.31). So $\mathfrak{P} \in R$, and $\psi(\mathfrak{P}) = \mathfrak{q}$. □

Corollary 5.8. *The function υ is surjective and n-to-1.*

Proof. This follows from Lemma 5.7 and Lemma 5.4 as $\upsilon = \varphi \circ \psi^{-1}$. □

Lemma 5.9. *For all $\mathfrak{q} \in Q'$, we have $\upsilon(\mathfrak{q}) = \mathfrak{q} \cap \mathbb{K}$.*

Proof. Let $\mathfrak{q} \in Q'$. Let $\mathfrak{P} = \psi^{-1}(\mathfrak{q})$, which is a prime ideal of $\mathcal{O}_{\mathbb{L}}$ above $\mathfrak{q}$. Then

$$\upsilon(\mathfrak{q}) = \varphi(\mathfrak{P}) = \mathfrak{P} \cap \mathbb{K} = \mathfrak{q} \cap \mathbb{K}.$$ □

Lemma 5.10. *For all $\mathfrak{q} \in Q'$, we have $N(\mathfrak{q}) = N(\upsilon(\mathfrak{q}))$.*

Proof. Let $\mathfrak{q} \in Q'$, and let $\mathfrak{p} = \upsilon(\mathfrak{q})$ so that $\mathfrak{p} = \mathfrak{q} \cap \mathbb{K}$ by Lemma 5.9. Then $f(\mathfrak{q}|\mathfrak{p}) = 1$ because $\mathfrak{q} \in Q'$. Let $\mathbb{F}_\mathfrak{p} = \mathcal{O}_\mathbb{K}/\mathfrak{p}$ and $\mathbb{F}_\mathfrak{q} = \mathcal{O}_\mathbb{M}/\mathfrak{q}$, where $\mathbb{F}_\mathfrak{p}$ may be considered a subfield of $\mathbb{F}_\mathfrak{q}$. Then $[\mathbb{F}_\mathfrak{q} : \mathbb{F}_\mathfrak{p}] = f(\mathfrak{q}|\mathfrak{p}) = 1$, so $\mathbb{F}_\mathfrak{q} = \mathbb{F}_\mathfrak{p}$ and hence $N(\mathfrak{p}) = |\mathbb{F}_\mathfrak{p}| = |\mathbb{F}_\mathfrak{q}| = N(\mathfrak{q})$. □

We now return to prove Proposition 5.3.

Proof of Proposition 5.3. Let $\sigma \in (1, \infty)$. By Corollary 5.8, we know that $Q' = \bigcup_{\mathfrak{p} \in P} \upsilon^{-1}(\{\mathfrak{p}\})$ where the union is disjoint and $|\upsilon^{-1}(\{\mathfrak{p}\})| = n$ for all $\mathfrak{p} \in P$. Also, by Lemma 5.10, for all $\mathfrak{p} \in P$ and all $\mathfrak{q} \in \upsilon^{-1}(\{\mathfrak{p}\})$ we know that $N(\mathfrak{q}) = N(\mathfrak{p})$. So

$$\sum_{\mathfrak{q} \in Q'} N(\mathfrak{q})^{-\sigma} = \sum_{\mathfrak{p} \in P} \sum_{\mathfrak{q} \in \upsilon^{-1}(\{\mathfrak{p}\})} N(\mathfrak{q})^{-\sigma} = \sum_{\mathfrak{p} \in P} \sum_{\mathfrak{q} \in \upsilon^{-1}(\{\mathfrak{p}\})} N(\mathfrak{p})^{-\sigma} = n \sum_{\mathfrak{p} \in P} N(\mathfrak{p})^{-\sigma}.$$

Hence

$$\frac{\sum_{\mathfrak{q} \in Q'} N(\mathfrak{q})^{-\sigma}}{-\ln(\sigma - 1)} = n \, \frac{\sum_{\mathfrak{p} \in P} N(\mathfrak{p})^{-\sigma}}{-\ln(\sigma - 1)}.$$

Taking the limit as $\sigma \to 1^+$, we find that $\delta(P)$ exists if and only if $\delta(Q')$ exists (Proposition 4.34), and in this case, that $\delta(Q') = n\,\delta(P)$. □

This completes the proof of Theorem 5.1. The following is a direct corollary.

Corollary 5.11. *The Dirichlet density of P exists and equals $\frac{|C|}{|G|}$, if and only if the Dirichlet density of Q exists and equals $\frac{1}{|H|}$.*

Hence to prove Chebotarev's density theorem in general, it suffices to prove the special case of the theorem where the field extension under consideration is abelian, which we will do in Chapter 6.

Chapter 6

The abelian case

The main result of this chapter is the abelian case of Chebotarev's density theorem, which is stated in Theorem 6.1. The general case of Chebotarev's theorem follows from Theorem 6.1 by Corollary 5.11.

Theorem 6.1 (Chebotarev's density theorem for abelian extensions)**.** *Let $\mathbb{L}/\mathbb{K}$ be a finite abelian extension of number fields with Galois group G. For each $\tau \in G$, let*

$$P_\tau = \left\{\mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \text{ is unramified in } \mathcal{O}_\mathbb{L},\ \left(\tfrac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = \{\tau\}\right\}.$$

Then for each $\tau \in G$, the Dirichlet density of P_τ exists, and satisfies

$$\delta(P_\tau) = \frac{1}{|G|}.$$

Our proof of Theorem 6.1 elaborates on Part G of Section 6.5 in Fried and Jarden [13]. It has the following structure. In Section 6.1, by summing the Dirichlet densities (which exist by the cyclotomic case of Chebotarev's density theorem) of disjoint subsets $\{P_{\tau,\sigma}\}_{\sigma\in S_\tau}$ of P_τ, where S_τ is a subset of the Galois group H of any auxiliary extension $\mathbb{M}/\mathbb{K}$ which satisfies certain properties, we obtain the lower bound $\frac{|S_\tau|}{|G||H|}$ for $\delta_{\inf}(P_\tau)$ which is dependent on the field $\mathbb{M}$. In Section 6.2, we show that we can actually construct an $\mathbb{M}$ so that $\mathbb{M}/\mathbb{K}$ has these properties, but also so that $\frac{|S_\tau|}{|H|}$ is arbitrarily close to 1, thus strengthening the lower bound for $\delta_{\inf}(P_\tau)$ to $\frac{1}{|G|}$. Finally, in Section 6.3, we use the lower bound on $\delta_{\inf}(P_\tau)$ to show that $\frac{1}{|G|}$ is also an upper bound for $\delta_{\sup}(P_\tau)$, thus proving that $\delta(P_\tau)$ exists and equals $\frac{1}{|G|}$.

6.1 A lower bound on the Dirichlet density

Proposition 6.2. *Assume the same notation as in Theorem 6.1. Suppose $\mathbb{M}/\mathbb{K}$ is a cyclic cyclotomic field extension with Galois group H, such that $\mathbb{M}\cap\mathbb{L} = \mathbb{K}$. Let $\psi\colon \mathrm{Gal}(\mathbb{L}\mathbb{M}/\mathbb{K}) \to G \times H$ be the isomorphism $\rho \mapsto (\rho|_\mathbb{L}, \rho|_\mathbb{M})$. For each $\tau \in G$, let*

$$S_\tau = \left\{\sigma \in H : \ \operatorname{ord}\tau \mid \operatorname{ord}\sigma\right\}.$$

Also, for each $\tau \in G$ and each $\sigma \in H$, let

$$P_{\tau,\sigma} = \left\{\mathfrak{p} \in P(\mathbb{K}) : \ \mathfrak{p} \text{ is unramified in } \mathcal{O}_{\mathbb{L}\mathbb{M}},\ \left(\tfrac{\mathbb{L}\mathbb{M}/\mathbb{K}}{\mathfrak{p}}\right) = \left\{\psi^{-1}(\tau,\sigma)\right\}\right\}.$$

Then for each $\tau \in G$, the lower Dirichlet density of P_τ, which always exists, satisfies

$$\delta_{\inf}(P_\tau) \geqslant \frac{|S_\tau|}{|G||H|}.$$

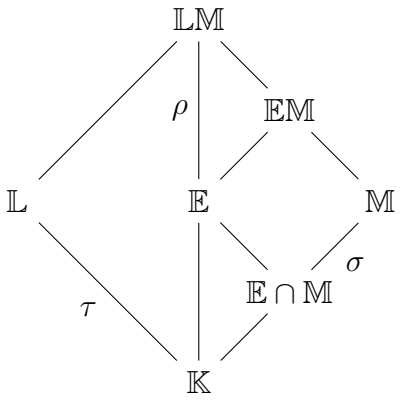
Remark 6.3. The statement of Proposition 6.2 assumes that $\mathbb{LM}/\mathbb{K}$ is abelian (in the definition of $P_{\tau,\sigma}$) and that ψ is a group isomorphism. Both assumptions follow from Proposition 2.11 because $\mathbb{L}/\mathbb{K}$ and $\mathbb{M}/\mathbb{K}$ are abelian and $\mathbb{M} \cap \mathbb{L} = \mathbb{K}$.

To prove Proposition 6.2, we need the following Lemma.

Lemma 6.4. *Assume the same notation as in Proposition 6.2. Then for each $\tau \in G$ and each $\sigma \in S_\tau$, the Dirichlet density of the set $P_{\tau,\sigma}$ exists and satisfies*

$$\delta(P_{\tau,\sigma}) = \frac{1}{|G||H|}.$$

Proof. Let $\tau \in G$ and $\sigma \in S_\tau$. Let $\rho = \psi^{-1}(\tau, \sigma)$, and let $\mathbb{E} = (\mathbb{LM})^{\langle\rho\rangle}$, so that $\mathrm{Gal}(\mathbb{LM}/\mathbb{E}) = \langle\rho\rangle$ by the fundamental theorem of Galois theory. We will show that $\mathbb{LM}/\mathbb{E}$ is a cyclotomic extension.



We claim that $\mathbb{LM} = \mathbb{EM}$. As $\mathbb{M}/\mathbb{K}$ is cyclotomic, it is Galois, and this implies that $\mathbb{EM}/\mathbb{E}$ is also Galois and $\mathrm{Gal}(\mathbb{EM}/\mathbb{E}) \cong \mathrm{Gal}(\mathbb{M}/\mathbb{E}\cap\mathbb{M})$ (Proposition 2.9). Now $\mathbb{E} \cap \mathbb{M} = (\mathbb{LM})^{\langle\rho\rangle} \cap \mathbb{M} = \mathbb{M}^{\langle\rho\rangle} = \mathbb{M}^{\langle\sigma\rangle}$ because $\rho|_{\mathbb{M}} = \sigma$, so $\mathrm{Gal}(\mathbb{M}/\mathbb{E} \cap \mathbb{M}) = \langle\sigma\rangle$. Also, we know that $\mathrm{ord}(\rho) = \mathrm{lcm}(\mathrm{ord}(\tau), \mathrm{ord}(\sigma)) = \mathrm{ord}(\sigma)$ because $\mathrm{ord}(\tau)$ divides $\mathrm{ord}(\sigma)$, so $\mathrm{Gal}(\mathbb{M}/\mathbb{E}\cap\mathbb{M}) = \langle\sigma\rangle \cong \langle\rho\rangle = \mathrm{Gal}(\mathbb{LM}/\mathbb{E})$. From all of this, we find that

$$[\mathbb{EM} : \mathbb{E}] = |\mathrm{Gal}(\mathbb{EM}/\mathbb{E})| = |\mathrm{Gal}(\mathbb{M}/\mathbb{E} \cap \mathbb{M})| = |\mathrm{Gal}(\mathbb{LM}/\mathbb{E})| = [\mathbb{LM} : \mathbb{E}]$$

because $\mathbb{EM}/\mathbb{E}$ and $\mathbb{LM}/\mathbb{E}$ are Galois. Applying the tower law to the tower of extensions $\mathbb{E} \subseteq \mathbb{EM} \subseteq \mathbb{LM}$, we find that $[\mathbb{LM} : \mathbb{EM}] = 1$ and so $\mathbb{LM} = \mathbb{EM}$.

As $\mathbb{M}/\mathbb{K}$ is cyclotomic, there is a root of unity ζ such that $\mathbb{M} \subseteq \mathbb{K}(\zeta)$. Now $\mathbb{LM} = \mathbb{EM} \subseteq \mathbb{EK}(\zeta) = \mathbb{E}(\zeta)$ because $\mathbb{K} \subseteq \mathbb{E}$ and $\mathbb{M} \subseteq \mathbb{K}(\zeta)$, so $\mathbb{LM}/\mathbb{E}$ is cyclotomic.

Let

$$Q = \left\{\mathfrak{q} \in P(\mathbb{E}) : \ \mathfrak{q} \text{ is unramified in } \mathcal{O}_{\mathbb{LM}},\ \left(\tfrac{\mathbb{LM}/\mathbb{E}}{\mathfrak{q}}\right) = \{\rho\}\right\}.$$

Applying the cyclotomic case of Chebotarev's density theorem (Theorem 4.36) to the cyclic cyclotomic extension $\mathbb{LM}/\mathbb{E}$, we find that the Dirichlet density of Q exists

and satisfies $\delta(Q) = 1/|\mathrm{Gal}(\mathbb{LM}/\mathbb{E})|$. As $\mathbb{E} = (\mathbb{LM})^{\langle\rho\rangle}$, we may apply Theorem 5.1 to the tower of extensions $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{LM}$ to conclude that $\delta(P_{\tau,\sigma})$ exists and satisfies

$$\delta(P_{\tau,\sigma}) = \left(\frac{|\mathrm{Gal}(\mathbb{LM}/\mathbb{K})|}{|\{\rho\}||\mathrm{Gal}(\mathbb{LM}/\mathbb{E})|}\right)^{-1}\delta(Q) = \Big(|G||H|\delta(Q)\Big)^{-1}\delta(Q) = \frac{1}{|G||H|}. \qquad \square$$

Proof of Proposition 6.2. Let $\tau \in G$. By Lemma 6.4, we know that $\delta(P_{\tau,\sigma}) = \frac{1}{|G||H|}$ for each $\sigma \in S_\tau$. Also, if σ and σ' are distinct elements of S_τ, then $P_{\tau,\sigma}$ and $P_{\tau,\sigma'}$ are disjoint, because ψ is a bijection. Hence, by Proposition 2.47, we have

$$\delta\Big(\bigcup_{\sigma\in S_\tau} P_{\tau,\sigma}\Big) = \sum_{\sigma\in S_\tau}\delta(P_{\tau,\sigma}) = \frac{|S_\tau|}{|G||H|}.$$

If we can show that $\bigcup_{\sigma\in S_\tau} P_{\tau,\sigma} \subseteq P_\tau$, then it would follow that

$$\delta_{\inf}(P_\tau) \geqslant \delta_{\inf}\Big(\bigcup_{\sigma\in S_\tau} P_{\tau,\sigma}\Big) = \delta\Big(\bigcup_{\sigma\in S_\tau} P_{\tau,\sigma}\Big) = \frac{|S_\tau|}{|G||H|},$$

finishing our proof of the proposition. Indeed, let $\sigma \in S_\tau$ and let $\mathfrak{p} \in P_{\tau,\sigma}$. Then $\mathfrak{p} \in P(\mathbb{K})$ and $\left(\frac{\mathbb{LM}/\mathbb{K}}{\mathfrak{p}}\right) = \{\psi^{-1}(\tau,\sigma)\}$. But $\mathbb{L}$ is an intermediate field of the extension $\mathbb{LM}/\mathbb{K}$, and the extension $\mathbb{L}/\mathbb{K}$ is normal. Hence, by Proposition 2.31, we have

$$\left[\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right] = \left[\frac{\mathbb{LM}/\mathbb{K}}{\mathfrak{p}}\right]\Big|_{\mathbb{L}} = \psi^{-1}(\tau,\sigma)\big|_{\mathbb{L}} = \tau,$$

which means that $\left(\frac{\mathbb{L}/\mathbb{K}}{\mathfrak{p}}\right) = \{\tau\}$, and thus $\mathfrak{p} \in P_\tau$. $\square$

6.2 A stronger lower bound on the Dirichlet density

To strengthen the lower bound on $\delta_{\inf}(P_\tau)$ given in Proposition 6.2, we would like to eliminate the dependence of the result on the field $\mathbb{M}$. First, we will show that we can actually construct, for each m, a cyclic cyclotomic field extension $\mathbb{M}/\mathbb{K}$ of degree m such that $\mathbb{M}\cap\mathbb{L} = \mathbb{K}$; then, we will show that we can make $\frac{|S_\tau|}{|H|}$ arbitrarily close to 1 through our choice of m. From this, we will deduce that $\delta_{\inf}(P_\tau) \geqslant \frac{1}{|G|}$.

6.2.1 Constructing cyclic cyclotomic field extensions

The aim of this subsection is to prove the following proposition.

Proposition 6.5. *Let $\mathbb{L}/\mathbb{K}$ be a finite Galois extension of number fields, and let $m \geqslant 1$. Then there exists a cyclic cyclotomic extension $\mathbb{M}/\mathbb{K}$ of degree m with $\mathbb{M}\cap\mathbb{L} = \mathbb{K}$.*

We begin by proving the following special case of Proposition 6.5, where $\mathbb{K}$ is actually $\mathbb{Q}$, and where $\mathbb{L}/\mathbb{Q}$ is cyclotomic.

Lemma 6.6. *Let $\mathbb{L}/\mathbb{Q}$ be a finite cyclotomic extension, and let $m \geqslant 1$. Then there exists a cyclic cyclotomic extension $\mathbb{M}/\mathbb{Q}$ of degree m such that $\mathbb{M}\cap\mathbb{L} = \mathbb{Q}$.*

Proof. As $\mathbb{L}/\mathbb{Q}$ is cyclotomic, there is a primitive n-th root of unity ζ_n such that $\mathbb{L} \subseteq \mathbb{Q}(\zeta_n)$. By Dirichlet's theorem on prime numbers in arithmetic progressions (Theorem 3.14), there is a prime $p > n$ such that $m \mid p-1$. Now $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a

cyclic extension of degree $p-1$. Let ν be a generator of $J = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, and let $H = \langle \nu^m \rangle$. Note that H is a normal subgroup of J, and

$$\frac{J}{H} \cong \frac{\mathbb{Z}/(p-1)\mathbb{Z}}{m\mathbb{Z}/(p-1)\mathbb{Z}} \cong \frac{\mathbb{Z}}{m\mathbb{Z}}$$

by the second isomorphism theorem as $m \mid p-1$. Hence J/H is cyclic of order m. Let $\mathbb{M} = \mathbb{Q}(\zeta_p)^H$. Then by the fundamental theorem of Galois theory, $\mathbb{M}/\mathbb{Q}$ is Galois and $\mathrm{Gal}(\mathbb{M}/\mathbb{Q}) \cong J/H$ is cyclic of order m. So $\mathbb{M}/\mathbb{Q}$ is a cyclic cyclotomic extension, and $[\mathbb{M} : \mathbb{Q}] = m$. Finally, $\mathbb{M} \cap \mathbb{L} \subseteq \mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ as $\gcd(p, n) = 1$ (Proposition 3.10). □

To generalise Lemma 6.6, we need the following result about the existence of a greatest cyclotomic intermediate field.

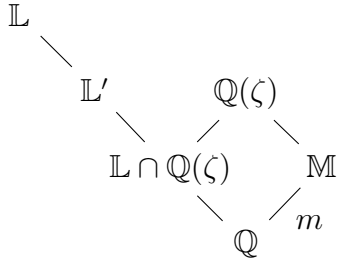
Lemma 6.7. *Let $\mathbb{L}$ be a number field. Let $\mathscr{C}$ be the collection of intermediate fields of the extension $\mathbb{L}/\mathbb{Q}$ which are cyclotomic over $\mathbb{Q}$. Then $\mathscr{C}$ is non-empty, and contains a field $\mathbb{L}'$ which is greatest with respect to inclusion.*

Proof. The extension $\mathbb{Q}/\mathbb{Q}$ is trivially cyclotomic, so $\mathscr{C}$ contains $\mathbb{Q}$, and thus is non-empty. As there is an extension of $\mathbb{L}$ which is Galois over $\mathbb{Q}$, by the fundamental theorem of Galois theory, there are only finitely many elements in $\mathscr{C}$, say $\mathbb{E}_1, \ldots, \mathbb{E}_k$. Let $\mathbb{L}'$ be the compositum $\mathbb{E}_1\mathbb{E}_2 \cdots \mathbb{E}_k$. We claim that $\mathbb{L}'$ is in $\mathscr{C}$. It suffices to show that if $\mathbb{E}$ and $\mathbb{E}'$ are elements of $\mathscr{C}$ then so is the compositum $\mathbb{E}\mathbb{E}'$, and then use induction on k. It is clear that $\mathbb{E}\mathbb{E}'$ is an intermediate field of $\mathbb{L}/\mathbb{Q}$. Let ζ_s and ζ_t be primitive s-th and t-th roots of unity such that $\mathbb{E} \subseteq \mathbb{Q}(\zeta_s)$ and $\mathbb{E}' \subseteq \mathbb{Q}(\zeta_t)$. Let ζ_{st} be a primitive (st)-th root of unity. Then ζ_s and ζ_t are powers of ζ_{st}, and so $\mathbb{E}\mathbb{E}' \subseteq \mathbb{Q}(\zeta_s, \zeta_t) \subseteq \mathbb{Q}(\zeta_{st})$. Hence $\mathbb{E}\mathbb{E}'$ is cyclotomic, and thus is in $\mathscr{C}$. As $\mathbb{L}'$ is the compositum of all fields in $\mathscr{C}$, all fields in $\mathscr{C}$ are subfields of $\mathbb{L}'$, and thus $\mathbb{L}'$ is the greatest element of $\mathscr{C}$ with respect to inclusion. □

Using Lemma 6.6, we now prove the following more general case of Proposition 6.5 which no longer requires $\mathbb{L}/\mathbb{Q}$ to be cyclotomic.

Lemma 6.8. *Let $\mathbb{L}/\mathbb{Q}$ be a finite extension, and let $m \geqslant 1$. Then there exists a cyclic cyclotomic extension $\mathbb{M}/\mathbb{Q}$ of degree m such that $\mathbb{M} \cap \mathbb{L} = \mathbb{Q}$.*

Proof. Let $\mathbb{L}'$ be the greatest intermediate field of $\mathbb{L}/\mathbb{Q}$ which is cyclotomic over $\mathbb{Q}$, which exists by Lemma 6.7. Applying Lemma 6.6 to the extension $\mathbb{L}'/\mathbb{Q}$, there exists a cyclic cyclotomic extension $\mathbb{M}/\mathbb{Q}$ of degree m such that $\mathbb{M} \cap \mathbb{L}' = \mathbb{Q}$. We need to show that $\mathbb{M} \cap \mathbb{L} = \mathbb{Q}$.



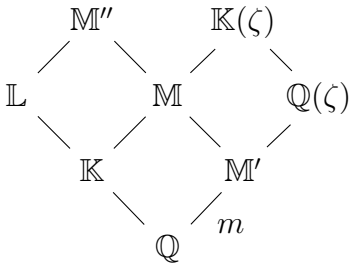
As $\mathbb{M}/\mathbb{Q}$ is cyclotomic, there is a root of unity ζ such that $\mathbb{M} \subseteq \mathbb{Q}(\zeta)$. Notice that $\mathbb{Q} \subseteq \mathbb{Q}(\zeta) \cap \mathbb{L} \subseteq \mathbb{L}$, and $\mathbb{Q}(\zeta) \cap \mathbb{L} \subseteq \mathbb{Q}(\zeta)$, so $\mathbb{Q}(\zeta) \cap \mathbb{L}$ is an intermediate field of $\mathbb{L}/\mathbb{Q}$ which is cyclotomic over $\mathbb{Q}$. As $\mathbb{L}'$ is the greatest intermediate field of $\mathbb{L}/\mathbb{Q}$ which is cyclotomic over $\mathbb{Q}$, we know that $\mathbb{Q}(\zeta) \cap \mathbb{L} \subseteq \mathbb{L}'$. Hence

$$\mathbb{Q} \subseteq \mathbb{M} \cap \mathbb{L} = (\mathbb{M} \cap \mathbb{Q}(\zeta)) \cap \mathbb{L} = \mathbb{M} \cap (\mathbb{Q}(\zeta) \cap \mathbb{L}) \subseteq \mathbb{M} \cap \mathbb{L}' = \mathbb{Q},$$

and thus $\mathbb{M} \cap \mathbb{L} = \mathbb{Q}$ as required. □

Finally, using Lemma 6.8, we return to prove Proposition 6.5.

Proof of Proposition 6.5. Recall that $\mathbb{L}/\mathbb{K}$ is a finite Galois extension of number fields, and m is a positive integer. By Lemma 6.8, there exists a cyclic cyclotomic extension $\mathbb{M}'/\mathbb{Q}$ of degree m such that $\mathbb{M}' \cap \mathbb{L} = \mathbb{Q}$ and $m = [\mathbb{M}' : \mathbb{Q}]$. Let $\mathbb{M} = \mathbb{K}\mathbb{M}'$. We need to show that $\mathbb{M}/\mathbb{K}$ is a cyclic cyclotomic extension of degree m, and that $\mathbb{M} \cap \mathbb{L} = \mathbb{K}$.



Firstly, $\mathbb{Q} \subseteq \mathbb{M}' \cap \mathbb{K} \subseteq \mathbb{M}' \cap \mathbb{L} = \mathbb{Q}$ so $\mathbb{M}' \cap \mathbb{K} = \mathbb{Q}$. Hence $\mathbb{M}/\mathbb{K}$ is Galois and $\mathrm{Gal}(\mathbb{M}/\mathbb{K}) \cong \mathrm{Gal}(\mathbb{M}'/\mathbb{Q})$ (Proposition 2.9). It follows immediately that $\mathbb{M}/\mathbb{K}$ is degree m and cyclic. As $\mathbb{M}'/\mathbb{Q}$ is cyclotomic, there is a root of unity ζ such that $\mathbb{M}' \subseteq \mathbb{Q}(\zeta)$. Notice that $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{K}\mathbb{Q}(\zeta) = \mathbb{K}(\zeta)$, so $\mathbb{M}/\mathbb{K}$ is cyclotomic.

Finally, let $\mathbb{M}'' = \mathbb{L}\mathbb{M}'$ $(= \mathbb{L}\mathbb{M})$. As $\mathbb{M}' \cap \mathbb{L} = \mathbb{Q}$, we know that $\mathrm{Gal}(\mathbb{M}''/\mathbb{L}) \cong \mathrm{Gal}(\mathbb{M}'/\mathbb{Q})$ (Proposition 2.9). Hence the degree of $\mathbb{M}''/\mathbb{L}$ is m. As $\mathbb{L}/\mathbb{K}$ and $\mathbb{M}/\mathbb{K}$ are both Galois, we know that $\mathbb{M} \cap \mathbb{L} = \mathbb{K}$ if and only if $[\mathbb{M}'' : \mathbb{K}] = [\mathbb{M} : \mathbb{K}]\,[\mathbb{L} : \mathbb{K}]$ (Proposition 2.11). But $[\mathbb{M}'' : \mathbb{K}] = [\mathbb{M}'' : \mathbb{L}]\,[\mathbb{L} : \mathbb{K}] = m\,[\mathbb{L} : \mathbb{K}] = [\mathbb{M} : \mathbb{K}]\,[\mathbb{L} : \mathbb{K}]$, so $\mathbb{M} \cap \mathbb{L} = \mathbb{K}$ as required. □

6.2.2 Number of elements in a cyclic group with order divisible by a given integer

Having shown that we can construct a cyclic cyclotomic field extension $\mathbb{M}/\mathbb{K}$ of degree m with $\mathbb{M} \cap \mathbb{L} = \mathbb{K}$, it remains to show how to choose m to make $\frac{|S_\tau|}{|H|}$ "arbitrarily close" to 1. That is the focus of this subsection. We start by showing how to compute the ratio $\frac{|S_\tau|}{|H|}$ explicitly, first in the special case where H is a cyclic group of prime power order, and then more generally. To do so, we need the following well-known result about the order of elements in a cyclic group.

Lemma 6.9. *If $H = \langle \nu \rangle$ is a cyclic group of order m, then for all $k \geqslant 0$, we have*

$$\mathrm{ord}(\nu^k) = \frac{m}{\gcd(m, k)}.$$

Lemma 6.10. *Let a and b be integers such that $1 \leqslant a \leqslant b$. Let H be a cyclic group of order p^b, where p is a prime number. Let $S = \{\sigma \in H : p^a \mid \operatorname{ord}\sigma\}$. Then*

$$|S| = p^b - p^{a-1}.$$

Proof. Using Lemma 6.9, we may express S in terms of a generator ν of H as

$$S = \left\{\nu^k : 0 \leqslant k < p^b,\ p^a \mid \tfrac{p^b}{\gcd(p^b,k)}\right\}.$$

For all integers k, as $\gcd(p^b, k) \mid p^b$ and p is prime, there is an integer c in the range $0 \leqslant c \leqslant b$ such that $\gcd(p^b, k) = p^c$. For all integers c such that $0 \leqslant c \leqslant b$, let

$$S_c = \left\{\nu^k : 0 \leqslant k < p^b,\ \gcd(p^b, k) = p^c\right\}.$$

As $p^a \mid p^{b-c}$ if and only if $b - c \geqslant a$, if and only if $c \leqslant b - a$, it follows that $S = \bigcup_{0\leqslant c\leqslant b-a} S_c$ where the union is disjoint, and so

$$|S| = \sum_{c=0}^{b-a} |S_c|.$$

It is clear that $S_c = \{\nu^{jp^c} : 0 \leqslant j < p^{b-c},\ \gcd(p^{b-c}, j) = 1\}$, and so

$$|S_c| = \varphi(p^{b-c}) = p^{b-c} - p^{b-c-1},$$

where φ is the Euler totient function. Hence

$$|S| = \sum_{c=0}^{b-a} (p^{b-c} - p^{b-c-1}) = p^b - p^{b-(b-a)-1} = p^b - p^{a-1}. \qquad \square$$

We now prove the following generalisation of the previous result.

Proposition 6.11. *Let n be a positive integer, with prime factorisation $p_1^{a_1} \cdots p_r^{a_r}$, where $a_i \geqslant 1$ for all $1 \leqslant i \leqslant r$. Let $m = p_1^{b_1} \cdots p_r^{b_r}$ where $b_i \geqslant a_i$ for all $1 \leqslant i \leqslant r$. Let H be a cyclic group of order m, and $S = \{\sigma \in H : n \mid \operatorname{ord}\sigma\}$. Then*

$$|S| = |H| \prod_{i=1}^{r} (1 - p_i^{a_i - b_i - 1}).$$

Proof. Recall that H is a cyclic group of order $m = p_1^{b_1} \cdots p_r^{b_r}$. By the fundamental theorem of finite abelian groups, we may write H as the internal direct sum $H = H_1 \oplus \cdots \oplus H_r$ where $H_i \leqslant H$ is a cyclic group of order $p_i^{b_i}$ for each integer i in the range $1 \leqslant i \leqslant r$.

Let $\sigma \in H$. Then $\sigma = \sigma_1 \cdots \sigma_r$, for some unique elements $\sigma_1 \in H_1, \ldots, \sigma_r \in H_r$. For each integer i in the range $1 \leqslant i \leqslant r$, we know that the order of σ_i divides $|H_i| = p_i^{b_i}$ by Lagrange's theorem, so the order of σ_i is $p_i^{c_i}$ for some integer c_i in the range $1 \leqslant c_i \leqslant b_i$. Clearly the orders of the σ_i are pairwise coprime, and thus

$$\operatorname{ord}(\sigma) = \operatorname{lcm}(\operatorname{ord}(\sigma_1), \ldots, \operatorname{ord}(\sigma_r)) = \operatorname{ord}(\sigma_1) \cdots \operatorname{ord}(\sigma_r) = p_1^{c_1} \cdots p_r^{c_r}.$$

Now n divides the order of σ if and only if $a_i \leqslant c_i$ for all $1 \leqslant i \leqslant r$, that is, if and only if $p_i^{a_i}$ divides the order of σ_i for all $1 \leqslant i \leqslant r$. By Lemma 6.10, the number of σ_i in H_i such that $p_i^{a_i}$ divides the order of σ_i is $p_i^{b_i} - p_i^{a_i-1}$. It follows that the number of σ in H for which n divides the order of σ is

$$\prod_{i=1}^{r}(p_i^{b_i} - p_i^{a_i-1}) = |H| \prod_{i=1}^{r}(1 - p_i^{a_i-b_i-1}). \qquad \square$$

The following result is a corollary to Proposition 6.11.

Corollary 6.12. *Let $n \in \mathbb{Z}^+$. For all $\epsilon > 0$, there is an $m \in \mathbb{Z}^+$ such that*

$$\frac{|S|}{|H|} > 1 - \epsilon$$

for all cyclic groups H of order m, where $S = \{\sigma \in H : \ n \mid \operatorname{ord}\sigma\}$.

Proof. Let $n = p_1^{a_1} \cdots p_r^{a_r}$ be the prime factorisation of n. Let $\epsilon > 0$. For each integer i in the range $1 \leqslant i \leqslant r$, we know that

$$\lim_{b\to\infty}(1 - p^{a_i-b-1})^r = \left(\lim_{b\to\infty} 1 - p^{a_i-b-1}\right)^r = 1^r = 1,$$

so there is an integer $b_i \geqslant a_i$ such that $(1 - p^{a_i-b_i-1})^r > 1 - \epsilon$, that is, such that $1 - p^{a_i-b_i-1} > \sqrt[r]{1-\epsilon}$. Let $m = p_1^{b_1} \cdots p_r^{b_r}$, and let H be a cyclic group of order m. Let $S = \{\sigma \in H : \ n \mid \operatorname{ord}\sigma\}$. By Proposition 6.11, we know that

$$\frac{|S|}{|H|} = \prod_{i=1}^{r}(1 - p_i^{a_i-b_i-1}) > \prod_{i=1}^{r}\sqrt[r]{1-\epsilon} = 1 - \epsilon. \qquad \square$$

6.2.3 Proof of the stronger lower bound

We may now state and prove the main result of this section.

Proposition 6.13. *Assume the same notation as in Theorem 6.1. Then for each $\tau \in G$, the lower Dirichlet density of P_τ satisfies*

$$\delta_{\inf}(P_\tau) \geqslant \frac{1}{|G|}.$$

Proof. Let $\tau \in G$ and let $\epsilon > 0$. From Corollary 6.12 with $n = \operatorname{ord}(\tau)$, there is a positive integer m such that if $\mathbb{M}/\mathbb{K}$ is a cyclic extension of degree m, then

$$\frac{|S_\tau(\mathbb{M}/\mathbb{K})|}{|\mathrm{Gal}(\mathbb{M}/\mathbb{K})|} > 1 - \epsilon.$$

By Proposition 6.5, we can construct an extension $\mathbb{M}/\mathbb{K}$ which satisfies these properties, but which is also a cyclotomic extension with $\mathbb{M} \cap \mathbb{L} = \mathbb{K}$.

Combining this result with Proposition 6.2, for all $\tau \in G$ and all $\epsilon > 0$, there exists a cyclic cyclotomic field extension $\mathbb{M}/\mathbb{K}$ such that $\mathbb{M} \cap \mathbb{L} = \mathbb{K}$ and

$$\delta_{\inf}(P_\tau) \geqslant \frac{1}{|G|} \frac{|S_\tau(\mathbb{M}/\mathbb{K})|}{|\mathrm{Gal}(\mathbb{M}/\mathbb{K})|} > \frac{1}{|G|}(1-\epsilon).$$

As this inequality is true for all $\epsilon > 0$, we find for all $\tau \in G$ that actually

$$\delta_{\inf}(P_\tau) \geqslant \sup_{\epsilon>0}\left\{\frac{1}{|G|}(1-\epsilon)\right\} = \frac{1}{|G|}. \qquad \square$$

6.3 Proof of the abelian case

We now return to prove the main theorem of this chapter.

Proof of Theorem 6.1. Let $\tau \in G$. Recall that $\delta(P(\mathbb{K})) = 1$ (Proposition 2.46). Hence, by Remark 2.48, we have

$$1 = \delta(P(\mathbb{K})) = \delta_{\sup}(P_\tau) + \delta_{\inf}(P(\mathbb{K})\backslash P_\tau) \tag{6.3.1}$$

Letting P be the set of non-zero prime ideals of $\mathcal{O}_\mathbb{K}$ which are ramified in $\mathcal{O}_\mathbb{L}$, the union

$$P(\mathbb{K})\backslash P_\tau = P \cup \Big(\bigcup_{\sigma \in G\backslash\{\tau\}} P_\sigma \Big)$$

is disjoint. So Proposition 2.47 implies that

$$\delta_{\inf}(P(\mathbb{K})\backslash P_\tau) \geqslant \delta_{\inf}(P) + \sum_{\sigma \in G\backslash\{\tau\}} \delta_{\inf}(P_\sigma). \tag{6.3.2}$$

But P is a finite set (Corollary 2.8), so $\delta(P) = 0$ (Corollary 4.35), so $\delta_{\inf}(P) = 0$. Also $\delta_{\inf}(P_\sigma) \geqslant \frac{1}{|G|}$ for each $\sigma \in G$ (Proposition 6.13). Hence (6.3.2) becomes

$$\delta_{\inf}(P(\mathbb{K})\backslash P_\tau) \geqslant \sum_{\sigma \in G\backslash\{\tau\}} \frac{1}{|G|} = 1 - \frac{1}{|G|},$$

and we may combine this with (6.3.1) to conclude that

$$\delta_{\sup}(P_\tau) \leqslant \frac{1}{|G|}.$$

Hence, by Proposition 6.13 and Proposition 2.46, we have

$$\frac{1}{|G|} \leqslant \delta_{\inf}(P_\tau) \leqslant \delta_{\sup}(P_\tau) \leqslant \frac{1}{|G|},$$

and so all of these inequalities must actually be equalities. By Proposition 2.46, it follows that $\delta(P_\tau)$ exists, and it satisfies

$$\delta(P_\tau) = \delta_{\inf}(P_\tau) = \delta_{\sup}(P_\tau) = \frac{1}{|G|}. \qquad \square$$

Appendix A

Characters of finite abelian groups

In this appendix, we introduce the theory of characters of finite abelian groups. This notion is central to the proof of the cyclotomic case of Chebotarev's density theorem in Chapter 4, starting with our definition of the Weber L-functions in Section 4.1. Our treatment of character theory follows Chapter 6 of Apostol [2].

Definition A.1. A character of a finite abelian group G is a group homomorphism

$$\chi \colon G \to \mathbb{C}^\times.$$

Example A.2. The trivial character of G is the homomorphism χ_1 given by

$$\chi_1(g) = 1 \qquad \forall g \in G.$$

Remark A.3. The *character group* of a finite abelian group G, denoted $\widehat{G}$, is the group whose elements are the characters of G and whose operation is pointwise multiplication of characters — i.e. for all $\chi, \chi' \in \widehat{G}$, the character $\chi\chi'$ is defined by

$$(\chi\chi')(g) = \chi(g)\chi'(g) \qquad \forall g \in G.$$

The identity element of $\widehat{G}$ is χ_1.

We begin by considering the relation between the characters of G and the characters of its subgroups. Clearly if χ is a character of G and $H \leqslant G$, then the restriction of χ to H is a character of H. A natural question to ask is: for each character χ of H, how many of the characters of G have χ as their restriction to H? In other words, how many ways are there to extend a character of H to a character of G? This will be the focus of the next proposition. To extend a character χ of H to a character of G, we will, as an intermediate step, extend χ to a character χ' of the subgroup $\langle H, g\rangle$ of G for some $g \in G \backslash H$. Here, by $\langle H, g\rangle$, we mean the subgroup of G generated by the set $H \cup \{g\}$. The following lemma, which characterises the elements of $\langle H, g\rangle$, will be useful when constructing χ'.

Lemma A.4. *Let G be a finite abelian group, let $H \leqslant G$ and let $g \in G$. Then*

(i) There is a smallest positive integer i such that $g^i \in H$. We call i the indicator of g in H.

(ii) The subgroup $\langle H, g\rangle$ of G may be enumerated explicitly as

$$\langle H, g\rangle = \{hg^k : \ h \in H, 0 \leqslant k < i\},$$

and $|\langle H, g\rangle| = i|H|$.

Remark A.5. The properties $|\langle H, g\rangle| = i|H|$ and $i = [\langle H, g\rangle : H]$ are equivalent.

Proof. For the first property, note that as G is finite, g has a finite order, say n, and we have $g^n = 1 \in H$. By the well-ordering principle, there must be a smallest positive integer i for which $g^i \in H$.

For the equality of sets in the second property, the inclusion of the right-hand side set into the left-hand side set is obvious. For the other inclusion, we proceed as follows. As $\langle H, g\rangle$ is generated by the set $H \cup \{g\}$, each element of $\langle H, g\rangle$ is a word of the form $g_1 g_2 \cdots g_n$ where n is a natural number, and each g_i either satisfies $g_i \in H \cup \{g\}$ or $g_i^{-1} \in H \cup \{g\}$. Here, the zero length word is by convention the identity element of G. As H is a subgroup of G, if $g_i^{-1} \in H$, then also $g_i \in H$. Hence each g_i is an element of the set $H \cup \{g, g^{-1}\}$. As G is abelian, we may rearrange the g_i, collecting together all of the elements of H, which multiply together to give a single element $h' \in H$, and collecting together all of the remaining elements (which are either g or g^{-1}) into a single power g^m of g. By the division algorithm, $m = qi+r$ for some integers q and i with $0 \leqslant i < r$, and so $g^m = (g^i)^q g^r$, where $(g^i)^q \in H$. Hence, letting $h = h'(g^i)^q$, our word is equal to hg^r where $0 \leqslant r < i$ and $h \in H$.

It remains to show that $|\langle H, g\rangle| = i|H|$. Suppose now that $hg^k = h'g^j$ for some $h, h' \in H$ and some integers k and j satisfying $0 \leqslant k, j < i$. Assume without loss of generality that $k \geqslant j$. Then $g^{k-j} = h^{-1}h' \in H$. As i is the smallest positive power of g in H, and $k - j \geqslant 0$, we must have $k - j = 0$, and thus also $h^{-1}h' = g^0 = 1$. So $k = j$ and $h = h'$. It follows that as h ranges over H and k ranges over $0 \leqslant k < i$, we get $i|H|$ distinct elements of the form hg^k. □

Proposition A.6. *Let G be a finite abelian group. Then for each subgroup H of G there are $[G : H]$ ways to extend a character of H to a character of G.*

Proof. We proceed by induction on the index $[G : H]$. For the base case, note that $H = G$ is the only index 1 subgroup of G, and there is exactly one way to extend each character χ of H to a character of G because χ is already a character of G.

Let j be an integer greater than 1, and suppose that the proposition holds for all subgroups of G of index less than j. Suppose that H is a subgroup of G with $[G : H] = j$, and let χ be a character of H. As $H \neq G$, there is a $g \in G \backslash H$, and we have $H < \langle H, g\rangle \leqslant G$ and $[G : \langle H, g\rangle] < [G : H] = j$ because $g \notin H$. We wish to show that there are $[G : H] = [G : \langle H, g\rangle]\,[\langle H, g\rangle : H]$ ways to extend χ to a character of G. It suffices in turn to show that there are $[\langle H, g\rangle : H]$ ways to extend χ to a character of $\langle H, g\rangle$, because each such character of $\langle H, g\rangle$ may be extended to $[G : \langle H, g\rangle] \leqslant j - 1$ characters of G by the induction hypothesis.

Recall Lemma A.4, which says that

$$\langle H, g\rangle = \{hg^k : \ h \in H, k \in \{0, 1, \ldots, i - 1\}\}$$

where $i = [\langle H, g\rangle : H]$ is the indicator of g in H. Suppose first that χ' is an extension of χ to a character of $\langle H, g\rangle$. As χ' is a group homomorphism, we have

$$\chi'(hg^k) = \chi'(h)\chi'(g)^k = \chi(h)\chi'(g)^k$$

for all $h \in H$ and all integers k satisfying $0 \leqslant k < i$. This means that χ' is determined by where it sends g. Recall that $g^i \in H$, so we have

$$\chi(g^i) = \chi'(g^i) = \chi'(g)^i,$$

and thus $\chi'(g)$ must be an i-th root of $\chi(g^i)$. This gives us i distinct candidates for extensions of χ to characters of $\langle H, g\rangle$, namely the maps defined by sending g to each of the i distinct i-th roots of $\chi(g^i)$. We will show that each such candidate is indeed a character of $\langle H, g\rangle$. Indeed, let α be an i-th root of $\chi(g^i)$, and define $\chi' \colon \langle H, g\rangle \to \mathbb{C}^\times$ by

$$\chi'(hg^k) = \chi(h)\alpha^k$$

for all $h \in H$ and all integers k satisfying $0 \leqslant k < i$. We need to check that χ' is a group homomorphism. Let hg^k and $h'g^j$ be arbitrary elements of $\langle H, g\rangle$, where $h, h' \in H$ and k and j are integers satisfying $0 \leqslant k, j < i$. By the division algorithm, we may write $k + j = qi + r$ for some integers q and r such that $0 \leqslant r < i$. It follows that

$$\begin{aligned}\chi'(hg^k \cdot h'g^j) &= \chi'(hh'(g^i)^q \cdot g^r) = \chi(hh'(g^i)^q)\alpha^r = \chi(h)\chi(h')\chi(g^i)^q\alpha^r \\ &= \chi(h)\chi(h')(\alpha^i)^q\alpha^r = \chi(h)\chi(h')\alpha^k\alpha^j = \chi'(hg^k)\chi'(h'g^j). \qquad \square\end{aligned}$$

Corollary A.7. *If G is a finite abelian group of order n, then there are exactly n characters of G. In particular, if G is cyclic and $g \in G$ is a generator of G, then the characters of G are determined by mapping g to each of the n distinct n-th roots of unity in $\mathbb{C}^\times$.*

Proof. If χ is a character of G, then $\chi(1) = 1$, and thus the restriction of χ to the subgroup $\langle 1\rangle$ is the trivial character χ_1 of $\langle 1\rangle$. In other words, every character of G is an extension of the character χ_1 of $\langle 1\rangle$ to a character of G. By Proposition A.6, the character χ_1 of $\langle 1\rangle$ can be extended in $[G : \langle 1\rangle] = |G|$ ways to a character of G. Thus the number of characters of G is $|G|$. In the case that G is cyclic and generated by g, we have $G = \langle\langle 1\rangle, g\rangle$, and thus G is obtained by one step of the inductive procedure outlined in the proof of Proposition A.6. Here, the indicator of g in $\langle 1\rangle$ is the order of g, namely n, and so each extension of the character χ_1 of $\langle 1\rangle$ to a character of G comes from sending g to one of the n distinct n-th roots of $\chi_1(g^n) = 1$. $\square$

The next proposition is just a restatement of the specific case of the previous proposition where $H = \langle g\rangle$ into the language of polynomials.

Proposition A.8. *Let G be a finite abelian group, and let $g \in G$. Then*

$$\prod_{\chi \in \widehat{G}} (1 - \chi(g)X) = (1 - X^f)^{|G|/f}$$

holds in $\mathbb{C}[X]$, where f is the order of g in G.

Proof. Clearly both polynomials in the equality above have constant term 1, so to show that they are equal, it suffices to show that they have the same roots and with the same multiplicities. The roots of the polynomial on the right-hand side of the

equality are all of the f-th roots of unity, each with multiplicity $|G|/f = [G : \langle g \rangle]$. As $\langle g \rangle$ is cyclic, there are exactly f characters of $\langle g \rangle$, each one determined by sending the generator g^{-1} to one of the f distinct f-th roots of unity (Corollary A.7). Hence, the roots of the polynomial on the right-hand side of the equality are the values $\chi'(g^{-1})$ as χ' ranges over $\widehat{\langle g \rangle}$, each with multiplicity $[G : \langle g \rangle]$. Also, the roots of the polynomial on the left-hand side of the equality are the values

$$\chi(g^{-1}) = \chi|_{\langle g \rangle}(g^{-1})$$

as χ ranges over $\widehat{G}$. Hence the result amounts to proving the following two facts:

- the restriction of each character χ of G to $\langle g \rangle$ is a character χ' of $\langle g \rangle$, and
- for each character χ' of $\langle g \rangle$, there are exactly $[G : \langle g \rangle]$ characters χ of G whose restriction to $\langle g \rangle$ is χ',

which we already did in Proposition A.6. □

Our next aim is to prove the well-known first and second orthogonality relations.

Proposition A.9. *Let G be a finite abelian group of order n, let $g \in G$ and let $\chi \in \widehat{G}$. Then $\chi(g)$ is an n-th root of unity.*

Proof. We know that the order of g divides n by Lagrange's theorem, and so

$$\chi(g)^n = \chi(g^n) = \chi(1) = 1.$$ □

Corollary A.10. *Let G be a finite abelian group of order n, let $g \in G$ and let $\chi \in \widehat{G}$. Then*

$$\chi^{-1}(g) = \chi(g^{-1}) = \overline{\chi(g)}.$$

Proof. Indeed, $\chi(g^{-1}) = \chi(g)^{-1}$ as χ is a group homomorphism. As the group operation of $\widehat{G}$ is pointwise multiplication, $\chi^{-1}(g) = \chi(g)^{-1}$. Finally $\chi(g)^{-1} = \overline{\chi(g)}$ because $\chi(g)$ is a complex root of unity. □

We may now prove the well-known first and second orthogonality relations, stated in the following proposition.

Proposition A.11 (Orthogonality relations)**.** *Let $G = \{g_1, \ldots, g_n\}$ be a finite abelian group of order n, with characters $\widehat{G} = \{\chi_1, \ldots, \chi_n\}$. Then*

(i) $\displaystyle\sum_{g \in G} \chi_i(g)\overline{\chi_j(g)} = n\delta_{ij}.$

(ii) $\displaystyle\sum_{\chi \in \widehat{G}} \chi(g_i)\overline{\chi(g_j)} = n\delta_{ij}.$

Remark A.12. Recall that the Kronecker delta symbol δ_{ij} is given by

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We may assume without loss of generality that χ_1 is the trivial character.

We begin by showing that the first orthogonality relation holds in the case that $j = 1$, that is, when χ_j is the trivial character. Indeed, let

$$S = \sum_{g \in G} \chi_i(g)\overline{\chi_1(g)} = \sum_{g \in G} \chi_i(g)$$

denote the sum of interest. If $i = 1$, then $\chi_i(g) = 1$ for all $g \in G$, and so $S = n$. Suppose now that $i \neq 1$. Then as χ_i is not identically 1, there is an element $h \in G$ for which $\chi_i(h) \neq 1$. Recall that the map $g \mapsto hg$ is an permutation of G, so as k ranges between 1 and n, hg_k ranges over all of the elements of G. Hence

$$S = \sum_{k=1}^{n} \chi_i(hg_k) = \chi_i(h) \sum_{k=1}^{n} \chi_i(g_k) = \chi_i(h)S,$$

and so $S\big(1 - \chi_i(h)\big) = 0$. As $\chi_i(h) \neq 1$, we must have $S = 0$. Hence $S = n\delta_{i1}$.

We now show that the first orthogonality relation holds in general. Recall that $\widehat{G}$ is a group under pointwise multiplication, with identity element χ_1 and inverses given by $\chi^{-1}(g) = \overline{\chi(g)}$ for all $\chi \in \widehat{G}$ and all $g \in G$. Hence we have

$$\sum_{k=1}^{n} \chi_i(g_k)\overline{\chi_j(g_k)} = \sum_{k=1}^{n} \chi_i(g_k)\chi_j^{-1}(g_k) = \sum_{k=1}^{n} (\chi_i\chi_j^{-1})(g_k).$$

As inverses in a group are unique, $\chi_i\chi_j^{-1} = \chi_1$ if and only if $i = j$, and so the result now follows from the previous special case of the first orthogonality relation.

We will deduce the second orthogonality relation from the first by using the property that a matrix commutes with its inverse. Let A denote the matrix[1] whose entry in the i-th row and j-th column is given by $[A]_{ij} = \chi_i(g_j)$, and let A^* denote the conjugate transpose of the matrix A. Then the first orthogonality relation amounts to the fact that $AA^* = nI$ where I is the $n \times n$ identity matrix. Indeed, we have

$$[AA^*]_{ij} = \sum_{k=1}^{n} [A]_{ik}[A^*]_{kj} = \sum_{k=1}^{n} [A]_{ik}\overline{[A]_{jk}} = \sum_{k=1}^{n} \chi_i(g_k)\overline{\chi_j(g_k)} = n\delta_{ij}$$

and so $AA^* = nI$. This means that $\frac{1}{n}A^*$ is the inverse of A, and so we also have $A^*A = nI$ because a matrix always commutes with its inverse. Considering the latter equality entrywise, we obtain the second orthogonality relation

$$n\delta_{ij} = [A^*A]_{ij} = \sum_{k=1}^{n} [A^*]_{ik}[A]_{kj} = \sum_{k=1}^{n} \overline{[A]_{ki}}[A]_{kj} = \sum_{k=1}^{n} \overline{\chi_k(g_i)}\chi_k(g_j). \qquad \square$$

[1] The matrix A is known as the *character table* of G.

Appendix B

Infinite products

Infinite products are an important component of the argument for the abelian case of Chebotarev's density theorem. Our treatment here is similar to that in Section 2.2 of Chapter 5 of Ahlfors [1, pp. 191–193].

Definition B.1. Let $(u_k)_{k=1}^{\infty}$ be a sequence of *non-zero* complex numbers. If the limit

$$P = \lim_{n\to\infty} \prod_{k=1}^{n} u_k$$

exists and $P \neq 0$, then we say that the infinite product $\prod_{k=1}^{\infty} u_k$ *converges* to P, and write

$$\prod_{k=1}^{\infty} u_k = P.$$

Otherwise we say that the infinite product *diverges*.

Remark B.2. We have defined convergence of the infinite product $\prod_{k=1}^{\infty} u_k$ with the unusual requirement that $P \neq 0$ so that its convergence is equivalent to the convergence of the series $\sum_{k=1}^{\infty} \operatorname{Log}(u_k)$, as we will prove shortly.

Remark B.3. The definition of convergence of an infinite product can be generalised to handle the possibility that finitely many of the factors are zero, by saying that an infinite product converges to zero if the product of its non-zero factors converges. However, we do not need this level of generality for the purposes of proving Chebotarev's density theorem.

Proposition B.4. *Let $(u_k)_{k=1}^{\infty}$ be a sequence of non-zero complex numbers. If $\prod_{k=1}^{\infty} u_k$ converges, then $\lim_{n\to\infty} u_n = 1$.*

Proof. Let $P = \prod_{k=1}^{\infty} u_k$. Then $P \neq 0$ by the definition of convergence, and so

$$\lim_{n\to\infty} u_n = \frac{\lim_{n\to\infty} \prod_{k=1}^{n} u_k}{\lim_{n\to\infty} \prod_{k=1}^{n-1} u_k} = \frac{P}{P} = 1. \qquad \square$$

Recall the following definition of the principal branch of the complex logarithm.

Definition B.5. The *principal branch* of the complex logarithm is the function $\operatorname{Log}\colon \mathbb{C}\backslash\{0\} \to \mathbb{C}$ given by

$$\operatorname{Log}(z) = \ln|z| + i \operatorname{Arg}(z) \qquad \forall z \in \mathbb{C}\backslash\{0\},$$

where $\operatorname{Arg}(z)$ is the principal argument of z, that is, $\operatorname{Arg}(z)$ is the argument of z in the interval $(-\pi, \pi]$.

In an introductory course on complex analysis, one proves the following result.

Proposition B.6. *The function* Log *is holomorphic on* $\mathbb{C}\backslash(-\infty, 0]$ *with derivative given by*

$$\mathrm{Log}'(z) = \frac{1}{z} \qquad \forall z \in \mathbb{C}\backslash(-\infty, 0],$$

and it is discontinuous on $(-\infty, 0)$.

We only need the fact that Log is continuous on $\mathbb{C}\backslash(-\infty, 0]$, which follows from this result.

Proposition B.7. *Suppose that* $(u_k)_{k=1}^{\infty}$ *is a sequence of non-zero complex numbers. Then the the product* $\prod_{k=1}^{\infty} u_k$ *converges if and only if the sum* $\sum_{k=1}^{\infty} \mathrm{Log}(u_k)$ *converges, and in this case we have*

$$\prod_{k=1}^{\infty} u_k = \exp\Big(\sum_{k=1}^{\infty} \mathrm{Log}(u_k)\Big).$$

Proof. As the u_k are all non-zero, $\mathrm{Log}(u_k)$ is always defined. Also, for each $n \in \mathbb{Z}^+$, there is an $m_n \in \mathbb{Z}$ such that

$$\mathrm{Arg}\Big(\prod_{k=1}^{n} u_k\Big) = \sum_{k=1}^{n} \mathrm{Arg}(u_k) + 2m_n\pi,$$

and thus

$$\mathrm{Log}\Big(\prod_{k=1}^{n} u_k\Big) = \sum_{k=1}^{n} \mathrm{Log}(u_k) + 2m_n\pi i.$$

Suppose that the sum $\sum_{k=1}^{\infty} \mathrm{Log}(u_k)$ converges. Note that exp is continuous on $\mathbb{C}$, and also that

$$\begin{aligned}\prod_{k=1}^{n} u_k &= \exp\bigg(\mathrm{Log}\Big(\prod_{k=1}^{n} u_k\Big)\bigg) \\ &= \exp\Big(\sum_{k=1}^{n} \mathrm{Log}(u_k) + 2m_n\pi i\Big) = \exp\Big(\sum_{k=1}^{n} \mathrm{Log}(u_k)\Big).\end{aligned}$$

Hence, the limit

$$\lim_{n\to\infty} \prod_{k=1}^{n} u_k = \exp\Big(\sum_{k=1}^{\infty} \mathrm{Log}(u_k)\Big)$$

converges, and it is non-zero because it is in the image of exp. It follows that the product $\prod_{k=1}^{\infty} u_k$ converges to $\exp\big(\sum_{k=1}^{\infty} \mathrm{Log}(u_k)\big)$.

Conversely, suppose that $\prod_{k=1}^{\infty} u_k$ converges to P. Then $P \neq 0$ by the definition of convergence. First, we consider the case that $P \notin (-\infty, 0)$. Then Log is continuous at P, and so the limit

$$\lim_{n\to\infty} \mathrm{Log}\Big(\prod_{k=1}^{n} u_k\Big) = \mathrm{Log}\Big(\lim_{n\to\infty} \prod_{k=1}^{n} u_k\Big) = \mathrm{Log}(P)$$

exists. Let

$$c_n = \mathrm{Log}\Big(\prod_{k=1}^{n} u_k\Big) = \sum_{k=1}^{n} \mathrm{Log}(u_k) + 2m_n\pi i,$$

so that $\lim_{n\to\infty} c_n = \mathrm{Log}(P)$. Notice that

$$c_n - c_{n-1} = \mathrm{Log}(u_n) + 2\pi i(m_n - m_{n-1})$$

for all $n \geqslant 2$. As $\lim_{n\to\infty} u_n = 1$ from Proposition B.4, and Log is continuous at 1, it follows that

$$\begin{aligned}\lim_{n\to\infty} &2\pi i(m_n - m_{n-1}) \\ &= \lim_{n\to\infty} c_n - \lim_{n\to\infty} c_{n-1} - \lim_{n\to\infty} \mathrm{Log}(u_n) = -\mathrm{Log}\left(\lim_{n\to\infty} u_n\right) = -\mathrm{Log}(1) = 0.\end{aligned}$$

As the m_n are integers, this limit implies that the sequence $(m_n)_{n=1}^{\infty}$ is eventually constant. That is, there is an $m \in \mathbb{Z}$, such that for all sufficiently large $n \in \mathbb{Z}^+$, we have $m_n = m$ and thus

$$c_n = \sum_{k=1}^{n} \mathrm{Log}(u_k) + 2m\pi i.$$

Hence, the sum

$$\sum_{k=1}^{\infty} \mathrm{Log}(u_k) = \lim_{n\to\infty} \sum_{k=1}^{n} \mathrm{Log}(u_k) = \lim_{n\to\infty} c_n - 2m\pi i = \mathrm{Log}(P) - 2m\pi i$$

converges.

Finally, we handle the case that $P \in (-\infty, 0)$. Now $-P \in (0, \infty)$ is an infinite product with the factors of P and the extra factor -1. By the previous case, we have

$$\mathrm{Log}(-1) + \sum_{k=1}^{\infty} \mathrm{Log}(u_k) = \mathrm{Log}(-P) - 2m\pi i$$

for some integer m. But $\mathrm{Log}(-1) = \ln|-1| + i\,\mathrm{Arg}(-1) = \pi i$, and also

$$\mathrm{Log}(-P) = \ln|-P| + i\,\mathrm{Arg}(-P) = \ln|P| = \ln|P| + i\,\mathrm{Arg}(P) - \pi i = \mathrm{Log}(P) - \pi i$$

as $P \in (-\infty, 0)$. Hence

$$\sum_{k=1}^{\infty} \mathrm{Log}(u_k) = \mathrm{Log}(P) - 2(m+1)\pi i. \qquad \square$$

Remark B.8. It follows that all of the theory of infinite sums that we are familiar with can also be applied to infinite products. For example, if the series $\sum_{k=1}^{\infty} \mathrm{Log}(u_k)$ is absolutely convergent, then it satisfies generalised commutativity and associativity. By the previous proposition, it follows that the infinite product $\prod_{k=1}^{\infty} u_k$ also satisfies generalised commutativity and associativity.

Definition B.9. Let $(u_k)_{k=1}^{\infty}$ be a sequence of non-zero complex numbers. We say that the infinite product $\prod_{k=1}^{\infty} u_k$ is *absolutely convergent* if the corresponding sum $\sum_{k=1}^{\infty} \operatorname{Log}(u_k)$ is absolutely convergent.

Henceforth, it will be convenient to write the factors u_k of our infinite products as $1 + a_k$, where the a_k are complex numbers such that $a_k \neq -1$.

Proposition B.10. *Let $(a_k)_{k=1}^{\infty}$ be a sequence of complex numbers with $a_k \neq -1$ for all $k \in \mathbb{Z}^+$. Then the series $\sum_{k=1}^{\infty} \operatorname{Log}(1 + a_k)$ converges absolutely if and only if the series $\sum_{k=1}^{\infty} a_k$ converges absolutely.*

Proof. If $a \in \mathbb{C}$ and $|a| \leqslant \frac{1}{2}$, then the inequality

$$\frac{1}{2}|a| \leqslant |\operatorname{Log}(1 + a)| \leqslant \frac{3}{2}|a| \tag{B.0.1}$$

holds. Indeed, it follows from the chain of inequalities

$$\begin{aligned} \big||\operatorname{Log}(1 + a)| - |a|\big| \leqslant |\operatorname{Log}(1 + a) - a| &= \left|\sum_{n=2}^{\infty} \frac{(-a)^n}{n}\right| \\ &\leqslant \sum_{n=2}^{\infty} \frac{|a|^n}{n} \leqslant \frac{|a|^2}{2} \sum_{n=2}^{\infty} |a|^{n-2} = \frac{|a|^2}{2} \cdot \frac{1}{1 - |a|} \leqslant \frac{\frac{1}{2}|a|}{2} \cdot 2 = \frac{1}{2}|a| \end{aligned}$$

where we have used the following results in order: the reverse triangle inequality; the Taylor series expansion

$$\operatorname{Log}(1 - z) = -\sum_{n=1}^{\infty} \frac{z^n}{n},$$

which has radius of convergence $1 > \frac{1}{2}$, evaluated at $z = -a$; the triangle inequality; the inequality $\frac{1}{n} \leqslant \frac{1}{2}$ which holds for all $n \geqslant 2$; the formula for a geometric series with ratio $|a|$; and the inequality

$$1 = \frac{1}{1} \leqslant \frac{1}{1 - |a|} \leqslant \frac{1}{1/2} = 2$$

which holds because $1 \geqslant 1 - |a| \geqslant \frac{1}{2}$.

If $\sum_{k=1}^{\infty} \operatorname{Log}(1 + a_k)$ converges absolutely, then so does $\prod_{k=1}^{\infty}(1 + a_k)$ (Proposition B.7), and so $1 + a_k \to 1$ as $k \to \infty$ (Proposition B.4). Hence $a_k \to 0$ as $k \to \infty$, and thus for sufficiently large k we have $|a_k| \leqslant \frac{1}{2}$. The series $\sum_{k=1}^{\infty} a_k$ converges absolutely by comparison with $2\sum_{k=1}^{\infty} |\operatorname{Log}(1 + a_k)|$, using the left-hand inequality of (B.0.1). Conversely, if $\sum_{k=1}^{\infty} a_k$ converges absolutely, then $a_k \to 0$ as $k \to \infty$, hence $|a_k| \leqslant \frac{1}{2}$ for sufficiently large k, and so the series $\sum_{k=1}^{\infty} \operatorname{Log}(u_k)$ converges absolutely by comparison with $\frac{3}{2}\sum_{k=1}^{\infty} |a_k|$, using the right-hand inequality of (B.0.1). □

Corollary B.11. *Assume the same notation as the previous proposition. Then the infinite product $\prod_{k=1}^{\infty}(1 + a_k)$ converges absolutely if and only if the series $\sum_{k=1}^{\infty} a_k$ converges absolutely.*

Proof. This follows directly by combining Proposition B.7 and Proposition B.10. □

Corollary B.12. *Assume the same notation as Corollary B.11. Then the product* $\prod_{k=1}^{\infty}(1+a_k)$ *converges absolutely if and only if the product* $\prod_{k=1}^{\infty}(1+|a_k|)$ *converges.*

Proof. From Corollary B.11, the absolute convergence of the product $\prod_{k=1}^{\infty}(1+a_k)$ is equivalent to the convergence of the series $\sum_{k=1}^{\infty}|a_k| = \sum_{k=1}^{\infty}\big||a_k|\big|$, which in turn is equivalent to the absolute convergence of the product $\prod_{k=1}^{\infty}\big(1+|a_k|\big)$. It remains to show that if the product $\prod_{k=1}^{\infty}\big(1+|a_k|\big)$ converges, then it converges absolutely. By Proposition B.7, it suffices to show that if the series $\sum_{k=1}^{\infty}\operatorname{Log}\big(1+|a_k|\big)$ converges then the series $\sum_{k=1}^{\infty}\big|\operatorname{Log}\big(1+|a_k|\big)\big|$ also converges. As $1+|a_k|$ is real and $1+|a_k| \geqslant 1$, we have $\operatorname{Log}\big(1+|a_k|\big) = \ln\big(1+|a_k|\big) \geqslant 0$, and so $\big|\operatorname{Log}\big(1+|a_k|\big)\big| = \operatorname{Log}\big(1+|a_k|\big)$. Hence the two series of interest are equal. □

Proposition B.13. *Let* $(u_k)_{k=1}^{\infty}$ *be a sequence of non-zero complex numbers. The product* $\prod_{k=1}^{\infty}u_k$ *converges if and only if the product* $\prod_{k=1}^{\infty}u_k^{-1}$ *converges, in which case*

$$\prod_{k=1}^{\infty}u_k^{-1} = \Big(\prod_{k=1}^{\infty}u_k\Big)^{-1}.$$

Additionally, the product $\prod_{k=1}^{\infty}u_k$ *is absolutely convergent if and only if the product* $\prod_{k=1}^{\infty}u_k^{-1}$ *is absolutely convergent.*

Proof. Suppose that the product $\prod_{k=1}^{\infty}u_k$ converges. Then its limit is non-zero (Definition B.1), and so the function $z \mapsto \frac{1}{z}$ is continuous at $z = \prod_{k=1}^{\infty}u_k$. Hence

$$\lim_{n\to\infty}\prod_{k=1}^{n}u_k^{-1} = \lim_{n\to\infty}\Big(\prod_{k=1}^{n}u_k\Big)^{-1} = \Big(\prod_{k=1}^{\infty}u_k\Big)^{-1},$$

and the limiting value is non-zero as it is a reciprocal. Thus the product $\prod_{k=1}^{\infty}u_k^{-1}$ converges to $(\prod_{k=1}^{\infty}u_k)^{-1}$.

Now, let $a_k = u_k - 1$ for each $k \in \mathbb{Z}^+$. Suppose that the product $\prod_{k=1}^{\infty}u_k = \prod_{k=1}^{\infty}(1+a_k)$ converges absolutely. Then the series $\sum_{k=1}^{\infty}a_k$ converges absolutely by Corollary B.11. By Proposition B.4, we know that $|a_k| \leqslant \frac{1}{2}$ for k sufficiently large. If $|a_k| \leqslant \frac{1}{2}$, then $1-|a_k| \geqslant 1-\frac{1}{2} = \frac{1}{2}$, and so by the reverse triangle inequality we have

$$|a_k+1| \geqslant \big||a_k|-1\big| = 1-|a_k| \geqslant \frac{1}{2}.$$

Hence, for k sufficiently large,

$$\left|\frac{1}{a_k+1}-1\right| = \left|\frac{a_k}{a_k+1}\right| \leqslant 2|a_k|.$$

It follows that the series $\sum_{k=1}^{\infty}\left(\frac{1}{a_k+1}-1\right)$ converges absolutely by inequality comparison with $2\sum_{k=1}^{\infty}|a_k|$. Hence $\prod_{k=1}^{\infty}u_k = \prod_{k=1}^{\infty}(1+a_k)^{-1}$ converges absolutely by Corollary B.11.

The converses hold by replacing each u_k with u_k^{-1} in the above arguments. □

The next proposition is about a special kind of infinite product known as a (generalised) *Euler product*. We will need the following notation. Let I denote the set of sequences $i = (i_k)_{k=1}^{\infty}$ of non-negative integers for which only finitely many of the integers i_k are non-zero. For each positive integer m, let

$$I_m = \{i \in I : \ i_m \neq 0 \text{ and } i_k = 0 \text{ for all } k > m\},$$

and set $I_0 = \{(0, 0, \ldots)\}$. Then $(I_m)_{m=0}^{\infty}$ is a partition of I. For each $m \geqslant 0$, the map from I_m to $\mathbb{N}^m$ which projects a sequence onto its first m coordinates is injective, and so I_m is countable because $\mathbb{N}^m$ is countable. Hence I is a countable union of countable sets, and so is itself countable. Hence infinite sums and products indexed over I may be interpreted in the sense described in Remark 2.36, provided that they are absolutely convergent. Note that if $(a_k)_{k=1}^{\infty}$ is a sequence of complex numbers and $i \in I$, then the product $a_1^{i_1} a_2^{i_2} \cdots$ is actually a finite product because only finitely many of the exponents i_k are non-zero. In the case that $i \in I_m$, we actually have $a_1^{i_1} a_2^{i_2} \cdots = a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m}$ because $i_k = 0$ for all $k > m$.

Proposition B.14. *Assume the notation from the preceding paragraph. Let $(a_k)_{k=1}^{\infty}$ be a sequence of complex numbers such that $|a_k| < 1$ for all positive integers k. Let*

$$S = \sum_{i \in I} a_1^{i_1} a_2^{i_2} \cdots \qquad \text{and} \qquad P = \prod_{k=1}^{\infty} (1 - a_k)^{-1}.$$

Then S is absolutely convergent if and only if P is absolutely convergent, in which case $S = P$.

Proof. For each positive integer m, let

$$S_m = \sum_{k=0}^{m} \sum_{i \in I_k} a_1^{i_1} a_2^{i_2} \cdots \qquad \text{and} \qquad P_m = \prod_{k=1}^{m} (1 - a_k)^{-1}.$$

Fix a positive integer m. Then we have the following chain of equalities:

$$\begin{aligned}
P_m &= (1 - a_1)^{-1} (1 - a_2)^{-1} \cdots (1 - a_m)^{-1} \\
&\overset{(1)}{=} \Big(\sum_{i_1 \in \mathbb{N}} a_1^{i_1} \Big) \Big(\sum_{i_2 \in \mathbb{N}} a_2^{i_2} \Big) \cdots \Big(\sum_{i_m \in \mathbb{N}} a_m^{i_m} \Big) \\
&\overset{(2)}{=} \sum_{(i_1, i_2, \ldots, i_m) \in \mathbb{N}^m} a_1^{i_1} a_2^{i_2} \cdots a_m^{i_m} \\
&\overset{(3)}{=} \sum_{i \in \bigcup_{k=0}^{m} I_k} a_1^{i_1} a_2^{i_2} \cdots \\
&\overset{(4)}{=} \sum_{k=0}^{m} \sum_{i \in I_k} a_1^{i_1} a_2^{i_2} \cdots \\
&= S_m,
\end{aligned}$$

and the inner series of S_m are all absolutely convergent. Indeed, we provide justification for each numbered equality below.

(1) For each k, as $|a_k| < 1$, the geometric series on the second line with ratio a_k converges absolutely, and so equals the corresponding factor $(1-a_k)^{-1}$ of P_m on the first line.
(2) We have

$$\Big(\sum_{i_1\in\mathbb{N}} a_1^{i_1}\Big)\Big(\sum_{i_2\in\mathbb{N}} a_2^{i_2}\Big) = \sum_{i_1\in\mathbb{N}}\Big(a_1^{i_1}\sum_{i_2\in\mathbb{N}} a_2^{i_2}\Big) = \sum_{i_1\in\mathbb{N}}\Big(\sum_{i_2\in\mathbb{N}} a_1^{i_1}a_2^{i_2}\Big),$$

where the absolute convergence of all outer and inner sums is a consequence of the fact that a constant multiple of an absolutely convergent series is absolutely convergent. By generalised associativity (Theorem 2.39), we have

$$\sum_{i_1\in\mathbb{N}}\Big(\sum_{i_2\in\mathbb{N}} a_1^{i_1}a_2^{i_2}\Big) = \sum_{(i_1,i_2)\in\mathbb{N}^2} a_1^{i_1}a_2^{i_2},$$

where the sum on the right-hand side is absolutely convergent. Repeating this argument finitely many times, we obtain equality (2) where the series on the third line is absolutely convergent.
(3) As $\bigcup_{k=0}^m I_k$ is the set of all sequences of natural numbers i where $i_j = 0$ for all $j > m$, the map from $\bigcup_{k=0}^m I_k$ to $\mathbb{N}^m$ which projects sequences onto their first m coordinates is a bijection, and so the fourth line is just a reindexing of the third.
(4) By generalised associativity (Theorem 2.39), the inner and outer series on the fifth line are absolutely convergent, and equality (4) holds.

We have just shown, for all positive integers k that $\sum_{i\in I_k} a_1^{i_1}a_2^{i_2}\cdots$ is absolutely convergent, and that $S_m = P_m$ for all positive integers m. If, additionally, one of the limits $\lim_{m\to\infty} S_m$ or $\lim_{m\to\infty} P_m$ exists, then both exist, and

$$\sum_{k=0}^{\infty}\sum_{i\in I_k} a_1^{i_1}a_2^{i_2}\cdots = \lim_{m\to\infty} S_m = \lim_{m\to\infty} P_m = \prod_{k=1}^{\infty}(1-a_k)^{-1}.$$

Now S is absolutely convergent if and only if the sum $\sum_{i\in I}|a_1|^{i_1}|a_2|^{i_2}\cdots$ converges. By generalised associativity (Theorem 2.39), this is equivalent to the convergence of all of the inner sums $\sum_{i\in I_k}|a_1|^{i_1}|a_2|^{i_2}\cdots$, as well as the outer sum $\sum_{k=0}^{\infty}\sum_{i\in I_k}|a_1|^{i_1}|a_2|^{i_2}\cdots$. Applying the result stated in the previous paragraph, but with a_k replaced by $|a_k|$, this is equivalent to the convergence of the product $\prod_{k=1}^{\infty}\Big(1-|a_k|\Big)^{-1}$. Finally, from Corollary B.11 and Proposition B.13, we have the

following equivalences:

$$\begin{aligned}
&\prod_{k=1}^{\infty}(1-a_k)^{-1} \text{ converges absolutely} \\
&\qquad \iff \prod_{k=1}^{\infty}(1-a_k) \text{ converges absolutely} \\
&\qquad \iff \sum_{k=1}^{\infty}|-a_k| = \sum_{k=1}^{\infty}\big|-|a_k|\big| \text{ converges absolutely} \\
&\qquad \iff \prod_{k=1}^{\infty}\big(1-|a_k|\big) \text{ converges absolutely} \\
&\qquad \iff \prod_{k=1}^{\infty}\big(1-|a_k|\big)^{-1} \text{ converges absolutely.}
\end{aligned}$$

□

Remark B.15. The direction "P absolutely convergent implies S absolutely convergent", is exactly Lemma 2 from Chapter 7 in Marcus' "Number theory" [28], and this is the only direction we will need in our proof of Chebotarev's density theorem. On the other hand, most treatments of the Riemann zeta function start with the absolute convergence of the sum

$$\sum_{n=1}^{\infty}\frac{1}{n^s}$$

whenever $s \in \mathbb{C}$ and $\mathrm{Re}(s) > 1$ (observe that this sum is a p-series with $p = \mathrm{Re}(s)$), and use this to deduce the absolute convergence of the corresponding Euler product

$$\prod_{p}\left(1-\frac{1}{p^s}\right)^{-1}$$

for the same s. We chose to write our proof in such a way to reveal the symmetry between the absolute convergence of S and P.

References

All names are written as they were in the cited works.

[1] Lars V. Ahlfors. *Complex Analysis An Introduction to the Theory of Analytic Functions of One Complex Variable*. 3rd ed. McGraw-Hill, Inc., 1979.

[2] Tom M. Apostol. *Introduction to Analytic Number Theory*. 1st ed. Undergraduate Texts in Mathematics. Springer-Verlag New York, 1976. DOI: 10.1007/978-1-4757-5579-4.

[3] E. Artin. 'Beweis des allgemeinen Reziprozitätsgesetzes'. In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 5.1 (Dec. 1927), pp. 353–363. DOI: 10.1007/BF02952531. From July 1927. Reprinted in [5, pp. 131–141].

[4] E. Artin. 'Über eine neue Art von L-Reihen'. In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 3.1 (Dec. 1924), pp. 89–108. DOI: 10.1007/BF02954618. From July 1923. Reprinted in [5, pp. 105–124].

[5] Emil Artin, Serge Lang and John T. Tate. *Collected papers of Emil Artin*. Reading, Massachusetts: Addison-Wesley, 1965.

[6] Sterling K. Berberian. *Fundamentals of Real Analysis*. 1st ed. Universitext. Springer-Verlag New York, 1999. DOI: 10.1007/978-1-4612-0549-4.

[7] *Biodiversity Heritage Library*. URL: https://www.biodiversitylibrary.org (visited on 30/09/2019).

[8] E. Cahen. 'Sur la fonction $\zeta(s)$ de Riemann et sur des fonctions analogues'. In: *Annales scientifiques de l'École Normale Supérieure*. 3rd ser. 11 (1894), pp. 75–164.

[9] Max Deuring. 'Über den Tschebotareffschen Dichtigkeitssatz'. In: *Mathematische Annalen* 110.1 (1935), pp. 414–415. DOI: 10.1007/BF01448036.

[10] P. G. Lejeune Dirichlet and R. Dedekind. *Vorlesungen über Zahlentheorie*. 4th ed. 1894.

[11] Günther Frei. 'Heinrich Weber and the Emergence of Class Field Theory'. In: *The Histroy of Modern Mathematics*. Ed. by David E. Rowe and John McCleary. Vol. Volume I: Ideas and Their Reception. San Diego, California: Academic Press, Inc., 1989, pp. 425–450.

[12] Günther Frei, Franz Lemmemeyer and Peter J. Roquette, eds. *Emil Artin and Helmut Hasse The Correspondence 1923–1958*. Vol. 5. Contributions in Mathematical and Computational Sciences. Springer Basel, 2014. DOI: 10.1007/978-3-0348-0715-9.

[13] Michael D. Fried and Moshe Jarden. *Field Arithmetic*. 3rd ed. Vol. 11. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Springer-Verlag Berlin Heidelberg, 2008. DOI: 10.1007/978-3-540-77270-5.

[14] G. Frobenius. 'Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe'. In: *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* (XXXII June 1896), pp. 689–705.
[15] Larry Joel Goldstein. *Analytic number theory*. Prentice-Hall Englewood Cliffs, NJ, 1971.
[16] G. H. Hardy and Marcel Riesz. *The General Theory of Dirichlet's Series*. 18. London: Cambridge University Press, 1915.
[17] *Internet Archive*. URL: https://archive.org (visited on 30/09/2019).
[18] J. L. W. V. Jensen. 'Om Rækkers Konvergens'. In: *Tidsskrift for Mathematik*. 5th ser. 2 (1884), pp. 63–72.
[19] Konrad Knopp. *Theory and Application of Infinite Series*. London and Glasgow: Blackie & Son Limited, 1954.
[20] Serge Lang. *Algebra*. 3rd ed. Vol. 211. Graduate Texts in Mathematics. Springer Science & Business Media, 2002.
[21] Serge Lang. *Algebraic number theory*. 2nd ed. Vol. 110. Graduate Texts in Mathematics. Springer Science & Business Media, 1994. DOI: 10.1007/978-1-4612-0853-2.
[22] Serge Lang. *Complex Analysis*. 4th ed. Vol. 103. Graduate Texts in Mathematics. Springer Science & Business Media, 1999. DOI: 10.1007/978-1-4757-3083-8.
[23] Serge Lang. *Undergraduate Algebra*. 3rd ed. Springer Science & Business Media, 2005.
[24] G. Lejeune Dirichlet. *G. Lejeune Dirichlet's Werke*. Ed. by Georg Reimer. Vol. 1. Berlin, 1889.
[25] Lejeune-Dirichlet. 'Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält'. In: *Mathematische Abhandlungen der Königlichen Akademie der Wissenschaften zu Berlin* (1839), pp. 45–81. Presented to the Akademie der Wissenschaften on July 27, 1837. French translation [26]. Reprinted in [24, pp. 313–342].
[26] G. Lejeune-Dirichlet. 'Démonstration de cette proposition: Toute progression arithmétique, dont le premier terme et la raison sont des entiers sans diviseur commun, contient une infinité de nombres premiers'. In: *Journal de mathématiques pures et appliquées* 4 (1839), pp. 393–422. Translation of [25] by M. Terquem.
[27] H.W. Lenstra, Jr. and P. Stevenhagen. 'Artin reciprocity and Mersenne primes'. In: *Nieuw Archief voor Wiskunde* 5.1 (Mar. 2000), pp. 44–54.
[28] Daniel A. Marcus. *Number Fields*. 2nd ed. Springer International Publishing AG, 2018. DOI: 10.1007/BF01448036.
[29] P. Stevenhagen and H. W. Lenstra, Jr. 'Chebotarëv and his density theorem'. In: *The Mathematical Intelligencer* 18.2 (1996), pp. 26–37.
[30] Andrew Sutherland. *18.785 - Number theory I*. Fall 2018. URL: http://math.mit.edu/classes/18.785/2018fa/lectures.html (visited on 30/09/2019).
[31] N. Tschebotareff. 'Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören'. In: *Mathematische Annalen* 95.1 (1926), pp. 191–228. DOI: 10.1007/BF01206606.

[32] H. Weber. *Elliptische Functionen und algebraische Zahlen*. Braunschweig: Druck und Verlag von Friedrich Vieweg und Sohn, 1891.

[33] H. Weber. 'Ueber Zahlengruppen in algebraischen Körpern'. In: *Mathematische Annalen* 48.4 (1897), pp. 433–473. DOI: 10.1007/BF01447919.

[34] H. Weber. 'Ueber Zahlengruppen in algebraischen Körpern. Dritte Abhandlung.' In: *Mathematische Annalen* 50.1 (1898), pp. 1–26. DOI: 10.1007/BF01444435.

[35] H. Weber. 'Ueber Zahlengruppen in algebraischen Körpern (Zweite Abhandlung.)' In: *Mathematische Annalen* 49.1 (1897), pp. 83–100. DOI: 10.1007/BF01445362.

[36] Heinrich Weber. *Lehrbuch der Algebra*. 2nd ed. Vol. 3. Braunschweig: Druck und Verlag von Friedrich Vieweg und Sohn, 1908.

[37] Н. Чеботарева. «Определение плотности совокупности простых чисел, принадлежащих к заданному классу подстановок». В: *Известия Российской Академии Наук* 17 (1-18 1923), с. 205—250.