Dirichlet's Theorem and Algebraic Number Fields

Pedro Sousa Vieira

February 16, 2012

Abstract

In this paper we look at two different fields of Modern Number Theory: *Analytic Number Theory* and *Algebraic Number Theory*. Making use of analytic methods we demonstrate a classic problem relating prime numbers with arithmetic progressions: *Dirichlet's Theorem*. Using algebraic methods we investigate the structure and properties of algebraic number fields, the basis of Algebraic Number Theory.

Contents

Chapter 1

Introduction

1.1 Context and motivation

The aim of this paper is to introduce two important branches of Modern Number Theory: **Analytic Number Theory** and **Algebraic Number Theory**. As the names suggest, the first one deals with number theoretic problems from an analytic perspective (making use of integrals, series, etc) while the second one studies algebraic structures intimately related with Number Theory such as *rings of algebraic integers*.

This report is a summary of the work I developed for the course *Projecto em Matemática* at Instituto Superior Técnico as a 3rd year undergraduate student of Licenciatura em Matemática Aplicada e Computação under the supervision of Professor Gustavo Granja, to whom I am very grateful for all the collaboration, help and support.

1.2 Contents

The paper is divided into three separate chapters. Chapter 2 is dedicated to proving *Dirichlet's Theorem* involving primes in arithmetic progressions following the classic proof of Dirichlet himself. The proof relies essentially on analytic methods, especially on convergence and divergence of Dirichlet's L-functions. In Chapter 3 we introduce basic concepts of Algebraic Number Theory with special focus on rings of algebraic integers. We'll discuss some properties of these rings and prove that they are *Dedekind rings*. Finally, in Chapter 4 we illustrate two simple but important classes of algebraic number fields: quadratic fields and cyclotomic fields.

Chapter 2

Dirichlet's Theorem

In this chapter we illustrate a proof of *Dirichlet's Theorem*, an outstanding and classic problem in Number Theory relating prime numbers with arithmetic progressions.

Theorem 1 (Dirichlet)**.**
Given a and m relatively prime positive integers there exist infinitely many primes p such that $p \equiv a \pmod{m}$.

As a matter of fact we will prove something a little stronger: prime numbers are "equally" distributed amongst the invertible classes modulo m. Even though this result is somewhat natural, its demonstration is no walk in the park. The method followed will be the one of Dirichlet himself which uses the properties of the Zeta and L-functions as well as modular characters. For a more detailed demonstration the reader should consult [JPS].

2.1 Characters of Finite Abelian Groups

In this section we will talk about characters of finite abelian groups, a simple tool needed for the demonstration of *Dirichlet's Theorem* 1. In what follows, let G be a finite abelian group written multiplicatively with identity e.

Definition 1. *A **character** of G is a homomorphism of G into the multiplicative group $\mathbb{C}^*$. The character χ_1 such that $\chi_1(g) = 1$ for all $g \in G$ is called the **main character**.*

The characters of G form a group $\mathrm{Hom}(G, \mathbb{C}^*)$ known has the *dual* of G which we'll denote by $\hat{G}$.

Notice that if $|G| = n$ then it follows that $(\chi(g))^n = \chi(g^n) = \chi(e) = 1$ for all $g \in G$ and any character χ of G (remember that $g^n = e$ by *Lagrange's Theorem*), i.e., the image of a character of G is a subset of the set of nth roots of unity.

	$1+5\mathbb{Z}$	$2+5\mathbb{Z}$	$3+5\mathbb{Z}$	$4+5\mathbb{Z}$
χ_1	1	1	1	1
χ_2	1	i	$-i$	-1
χ_3	1	-1	-1	1
χ_4	1	$-i$	i	-1

Example 1. *Considering $G = (\mathbb{Z}/5\mathbb{Z})^*$ we have the following 4 characters:*

There are two very important properties of characters which are stated in the following propositions. The second one will be particularly useful in the proof of *Dirichlet's Theorem* 1.

Proposition 1. *The dual group $\hat{G}$ is isomorphic to G.*

This fact can be easily proven by decomposing G into a product of cyclic subgroups (using the classification of finite abelian groups). For a cyclic group with generator g one can easily check that $\phi : \hat{G} \to G$ which assigns χ to $\chi(g)$ is an isomorphism.

Proposition 2 (Ortogonality relations)**.** *Let $|G| = n$ and $\chi \in \hat{G}$. Then:*

$$\sum_{x \in G} \chi(x) = \begin{cases} n & \text{if } \chi = \chi_1 \\ 0 & \text{if } \chi \neq \chi_1 \end{cases}$$

Proof. The result is trivial if $\chi = \chi_1$. If $\chi \neq \chi_1$ let $y \in G$ be such that $\chi(y) \neq 1$. In this case:

$$\sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(xy) = \chi(y) \sum_{x \in G} \chi(x)$$

Since $\chi(y) \neq 1$, it follows that $\sum_{x \in G} \chi(x) = 0$ as intended. □

From Proposition 2 above applied to $\hat{G}$ we get the following corollary.

Corollary 1. *Let $|G| = n$ and $x \in G$. Then:*

$$\sum_{\chi \in \hat{G}} \chi(x) = \begin{cases} n & \text{if } x = e \\ 0 & \text{if } x \neq e \end{cases}$$

Given $m \geq 1$ we denote by $G(m)$ the multiplicative group of invertible elements mod m, that is $(\mathbb{Z}/m\mathbb{Z})^*$. In the proof of *Dirichlet's Theorem* 1 we will consider a particular class of characters known as **Modular Characters**.

Definition 2 (Modular Characters)**.** *A modular character is a character of $G(m)$ for some $m \geq 1$. An element $\chi \in \hat{G}(m)$ is called a character modulo m.*

Notice that we can view a character modulo m, χ, as a totally multiplicative function with values in $\mathbb{C}^*$ defined on the set of integers prime to m. It will be convenient for the proof of *Dirichlet's Theorem* 1 to extend such a function to all of $\mathbb{Z}$ by setting $\chi(a) = 0$ if a is not prime to m. Notice that this function is still totally multiplicative.

Example 2. *$m = 5$. Since $G(5) = \mathbb{Z}/5\mathbb{Z}$ the characters modulo 5 are the ones stated in Example 1. Notice that they extend to functions in $\mathbb{Z}$ in the following way:*

$$\psi_j(x) = \begin{cases} \chi_j(x + 5\mathbb{Z}) & \text{if } 5 \nmid x \\ 0 & \text{if } 5 \mid x \end{cases}$$

for $j = 1, 2, 3, 4$.

2.2 Zeta and L-functions

In this section we will talk about the Zeta and L functions which are very important not only for the proof of the *Dirichlet Theorem* 1 but also in many branches of Mathematics. For example, the famous **Riemann Hypothesis** concerns the locus of zeros of the Zeta function.

In the following we will ignore most questions regarding convergence of series or infinite products as these may be tedious. For more rigorous proofs the reader should consult [JPS] or [MRM].

2.2.1 Zeta function

Definition 3 (Zeta function)**.** *For $s \in \mathbb{C}$ such that $\Re(s) > 1$ we define:*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Absolute convergence of the series for $\Re(s) > 1$ follows from comparison with the integral of $\frac{1}{x^{\Re(s)}}$. An interesting property of the Zeta function is that it factors as an infinite product due to the unique factorization of integers into prime numbers.

Proposition 3. *For $s \in \mathbb{C}$ such that $\Re(s) > 1$:*

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}$$

Proof. Omitting the convergence details we have, due to the unique factorization of integers into prime numbers:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \sum_{k=0}^{\infty} p^{-sk} = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}$$

□

We can still give a better characterization of the Zeta function.

Proposition 4. *The Zeta function is non-zero in the half plane* $\Re(s) > 1$ *and verifies for* $\Re(s) > 0$*:*

$$\zeta(s) = \frac{1}{s-1} + \phi(s)$$

where $\phi(s)$ *is holomorphic for* $\Re(s) > 0$*.*

A proof of the preceding proposition can be found in [JPS]. As a corollary we obtain:

Corollary 2. *As* $s \to 1$*, one has* $\sum_{p\ prime} \frac{1}{p^s} \sim \log\left(\frac{1}{s-1}\right)$.

Proof. From proposition 3 we have:

$$\log \zeta(s) = \log\left(\prod_{p \text{ prime}} (1-p^{-s})^{-1}\right) = -\sum_{p \text{ prime}} \log\left(1-p^{-s}\right) =$$

$$= \sum_{p \text{ prime}} \sum_{k\geq 1} \frac{1}{kp^{ks}} = \sum_{p \text{ prime}} \frac{1}{p^s} + \psi(s)$$

where $\psi(s) = \sum_{p \text{ prime}} \sum_{k\geq 2} \frac{1}{kp^{ks}}$. Notice that $\psi(s)$ is dominated by the series:

$$\sum_{p \text{ prime}} \sum_{k\geq 2} \frac{1}{p^{ks}} = \sum_{p \text{ prime}} \frac{1}{p^s(p^s-1)} \leq \sum_{p \text{ prime}} \frac{1}{p(p-1)} \leq \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1$$

Since $\psi(s)$ is majored as $s \to 1$, by proposition 4, $\log \zeta(s) \sim \log \frac{1}{s-1}$ and the conclusion follows. □

Observe that we can conclude from corollary 2 that the set of prime numbers is infinite. The argument used to prove *Dirichlet's Theorem* 1 is similar. It uses the fact that $\sum_{p\equiv a\ (mod\ m)} \frac{1}{p^s} \sim \frac{1}{\phi(m)} \log\left(\frac{1}{s-1}\right)$ as $s \to 1$ where ϕ is Euler's totient function.

2.2.2 L-functions

In the proof of the *Dirichlet Theorem* 1 we make use of the Dirichlet's L-functions. These functions make use of the modular characters discussed in section 2.1.

Let $m \geq 1$ and let χ be a character modulo m. We define the corresponding L-function by the series:

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

Observe that, in this sum, the only integers n that give a non-zero contribution are the ones which are prime to m. Note also that for $m = 1$ the only character modulo m is the main character χ_1 and for this character $L(s, \chi_1) = \zeta(s)$. For $m > 1$ we can also give a characterization of $L(s, \chi_1)$ in terms of $\zeta(s)$.

Proposition 5. *For $m \geq 1$ one has:*

$$L(s, \chi_1) = F(s)\zeta(s)$$

where $F(s) = \prod_{p|m} \left(1 - \frac{1}{p^s}\right)$. From proposition 4, since $F(s)$ is entire, $L(s, \chi_1)$ is holomorphic in $\Re(s) > 0$ and has a simple pole at $s = 1$.

When we consider characters modulo m other than χ_1, the corresponding L-functions are somewhat better behaved.

Proposition 6. *For $\chi \neq \chi_1$, $L(s, \chi)$ converges in the half plane $\Re(s) > 0$. In the half plane $\Re(s) > 1$, $L(s, \chi)$ converges absolutely and one has:*

$$L(s, \chi) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{\chi(p)}{p^s}}$$

Notice that, in particular, $L(1, \chi)$ is finite if $\chi \neq \chi_1$. In fact, for $\chi \neq \chi_1$, $L(1, \chi)$ in non-zero. This is one of the key points of Dirichlet's proof. A proof of this result can be found in [JPS].

2.3 Dirichlet's Theorem

In this section we prove *Dirichlet's Theorem* 1 using the tools developed in the previous sections. Let P be the set of prime numbers. We know from Corollary 2 that as $s \to 1$

$$\sum_{p \in P} \frac{1}{p^s} \sim \log \frac{1}{s-1}$$

It is then natural that given $A \subseteq P$ we define its density in P as

$$\lim_{s \to 1} \frac{\sum\limits_{p \in A} \frac{1}{p^s}}{\log \frac{1}{s-1}}$$

whenever the limit exists. Notice that P has density 1 and that if A is finite then its density is zero.

The idea of Dirichlet's proof consists in showing that, for $m \geq 1$ and a prime with m, the set of prime numbers such that $p \equiv a \pmod{m}$, herein denoted $P_{a,m}$, has density $\frac{1}{\phi(m)}$ where ϕ is Euler's totient function. Thus, $P_{a,m}$ can't be finite as it would have density zero. To prove this, we will first need three Lemmas.

Let χ be a character modulo m. We set

$$f_\chi(s) = \sum_{p \nmid m} \frac{\chi(p)}{p^s}$$

this expression making sense for $s > 1$.

Lemma 1. *As $s \to 1$ we have $f_{\chi_1} \sim \log \frac{1}{s-1}$.*

This follows from Corollary 2 because f_{χ_1} differs from $\sum\limits_{p \text{ prime}} \frac{1}{p^s}$ by a finite number of terms.

Lemma 2. *If $\chi \neq \chi_1$ then f_χ remains bounded when $s \to 1$.*

This follows from Proposition 6 using a similar argument as the one used in the proof of Corollary 2 and the fact that $L(1, \chi) \neq 0$. A proof can be found in [JPS] and in [MRM].

Now let $g_a(s) = \sum\limits_{p \in P_{a,m}} \frac{1}{p^s}$. We wish to study the behavior of $g_a(s)$ as $s \to 1$.

Lemma 3. *One has:*

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi \in \hat{G}(m)} \chi(a)^{-1} f_\chi(s)$$

Proof. After replacing f_χ by its definition, the right hand side becomes:

$$\frac{1}{\phi(m)} \sum_{p \nmid m} \frac{1}{p^s} \left(\sum_{\chi \in \hat{G}(m)} \chi(a^{-1}) \chi(p) \right)$$

Since $\chi(a^{-1})\chi(p) = \chi(a^{-1}p)$ we have by Corollary 1:

$$\sum_{\chi \in \hat{G}(m)} \chi(a^{-1}p) = \begin{cases} \phi(m) & \text{if } p \equiv a \pmod{m} \\ 0 & \text{if } p \not\equiv a \pmod{m} \end{cases}$$

Since $\gcd(a, m) = 1$ we find that the above expression is equal to $g_a(s)$ as intended. $\square$

We are now ready to show that $P_{a,m}$ has density $\frac{1}{\phi(m)}$. From Lemmas 1 and 2 we know that $f_\chi \sim \log \frac{1}{s-1}$ for $\chi = \chi_1$ and that f_χ remains bounded for $\chi \neq \chi_1$. Hence, by Lemma 3 it is clear that $g_a(s) \sim \frac{1}{\phi(m)} \log \frac{1}{s-1}$, which means that $P_{a,m}$ has density $\frac{1}{\phi(m)}$.

We can interpret this result as meaning that the prime numbers are somewhat equally distributed between the different classes modulo m which are prime to m.

Chapter 3

Algebraic Number Fields

In this chapter we will study algebraic number fields. In the first section we'll introduce some algebra tools needed for the rest of the section, as well as for chapter 4. These include important concepts as the *norm*, the *trace* and the *discriminant*. In the second section we'll be interested in the structure of the ring of algebraic integers of a number field, following more or less what is covered on chapter 12 of [IR].

3.1 Algebra Tools

Let K and L be fields such that L/K is a finite algebraic extension of fields. The dimension of L/K will be denoted by n. To each element $\alpha \in L$ we can assign two elements of K with good properties: the **norm** $N_{L/K}(\alpha)$ and the **trace** $t_{L/K}(\alpha)$.

Definition 4. *Let $\alpha_1, ..., \alpha_n$ be a basis for L/K and let $a_{ij} \in K$ be such that $\alpha\alpha_i = \sum_{j=1}^{n} a_{ij}\alpha_j$. We define the **norm** of α by $N_{L/K}(\alpha) := \det(a_{ij})$ and the **trace** of α by $t_{L/K}(\alpha) := a_{11} + ... + a_{nn}$.*

It is an easy exercise to check that this definition does not depend on the choice of basis $\alpha_1, ..., \alpha_n$. In the following we will use N and t to denote the norm and the trace whenever the extension L/K is clear. The good properties of the norm and the trace we mentioned above are the ones we expect from the usual norm (determinant) and trace of matrices.

Proposition 7. *Let $\alpha, \beta \in L$ and $a \in K$. Then the following holds:*

1. $N(\alpha\beta) = N(\alpha)N(\beta)$;
2. $t(\alpha + \beta) = t(\alpha) + t(\beta)$;
3. $N(a\beta) = a^n N(\beta)$;

4. $t(a\alpha) = at(\alpha)$;

5. *If* $\alpha \neq 0$ *then* $N(\alpha)^{-1} = N(\alpha^{-1})$.

In the case when L is a **separable** extension over K (that is, the minimal polynomial over K of any element in L has distinct roots) we can give an alternative definition of norm and trace. In fact, let $\sigma_1, ..., \sigma_n$ be the distinct isomorphisms of L into a fixed algebraic closure of K which leave K fixed. For $\alpha \in L$ we denote the jth conjugate of α, $\sigma_j(\alpha)$, by $\alpha^{(j)}$ and consider $\alpha^{(1)} = \alpha$.

Proposition 8. *For any* $\alpha \in L$ *one has:*

1. $t(\alpha) = \alpha^{(1)} + ... + \alpha^{(n)}$;

2. $N(\alpha) = \alpha^{(1)}...\alpha^{(n)}$.

Given an n-tuple $\alpha_1, ..., \alpha_n$ of elements of L there is an important element of L to which we can associate.

Definition 5. *Let* $\alpha_1, ..., \alpha_n$ *be elements of* L. *We define the* ***discriminant*** *of* $\alpha_1, ..., \alpha_n$, $\Delta(\alpha_1, ..., \alpha_n)$, *as* $\det(t(\alpha_i\alpha_j))$.

In a separable extension of fields the discriminant of an n-tuple is closely related with it forming a basis of L over K.

Proposition 9. *If* L/K *is separable then* $\alpha_1, ..., \alpha_n$ *is a basis for* L *over* K *if and only if* $\Delta(\alpha_1, ..., \alpha_n) \neq 0$.

As before, when L/K is separable we can give an alternative definition for the discriminant of an n-tuple in terms of its conjugates.

Proposition 10. *For* $\alpha_1, ..., \alpha_n \in L$ *and* L/K *separable one has*

$$\Delta(\alpha_1, ..., \alpha_n) = \det(\alpha_i^{(j)})^2$$

3.2 Algebraic Number Fields and the Ring of Algebraic Integers

In this section we talk about algebraic number fields and their ring of algebraic integers. We'll study the structure of the ring of algebraic integers with the goal of showing that it is a *Dedekind ring* while making use of important concepts in Algebraic Number Theory such as the *class number*. First, we must introduce some definitions.

Definition 6 (Algebraic Number Field)**.** *A subfield* F *of the complex numbers is called an* ***algebraic number field*** *if* F *is a finite dimensional vector space over* $\mathbb{Q}$.

Definition 7 (Ring of Algebraic Integers)**.** *Let F be an algebraic number field. An element $\alpha \in F$ is said to be an* ***algebraic integer*** *if α is the root of some monic polynomial in $\mathbb{Z}[x]$. The subset of F consisting of algebraic integers forms a ring D, called the* ***ring of algebraic integers*** *in F.*

Example 3. *$F = \mathbb{Q}$ is an algebraic number field because $[\mathbb{Q} : \mathbb{Q}] = 1$. In this case we have $D = \mathbb{Z}$.*

In fact, if $\frac{p}{q} \in D$ where p and q are coprime integers ($q \neq 0$) then there is some polynomial $r(x) = x^m + a_{m-1}x^{m-1} + ... + a_1x + a_0 \in \mathbb{Z}[x]$ such that $r(\frac{p}{q}) = 0$. Multiplying both sides of $r(\frac{p}{q}) = 0$ by q^m we get $p^m + a_{m-1}p^{m-1}q + ... + a_1pq^{m-1} + a_0q^m = 0$ implying that $q \mid p^m$. Since p and q where assumed to be coprime we obtain that $\frac{p}{q} \in \mathbb{Z}$ and so $D \subseteq \mathbb{Z}$. On the other hand, it is obvious that $\mathbb{Z} \subseteq D$.

In a ring of algebraic integers D the norm and the trace defined in the previous section are very simple, meaning that if $\alpha \in D$ then $N(\alpha)$ and $t(\alpha)$ are integers. To see this, notice that if α satisfies a monic polynomial in $\mathbb{Z}[x]$ then so do its conjugates, meaning that they are also in D. Using Proposition 8 we see that $N(\alpha)$ and $t(\alpha)$ are in D and using Definition 4 we know that they are also in $\mathbb{Q}$. Hence, from Example 3 we conclude that $N(\alpha)$ and $t(\alpha)$ are integers.

Example 4. *$F = \mathbb{Q}[\sqrt{-5}]$ is an algebraic number field because $[\mathbb{Q}[\sqrt{-5}] : \mathbb{Q}] = 2$. In this case, as we shall see in the next chapter, we have $D = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$. For $a, b \in \mathbb{Z}$, if $\alpha = a + b\sqrt{-5}$ then $N(\alpha) = a^2 + 5b^2$ and $t(\alpha) = 2a$.*

We can see from Example 4 that D is not necessarily a unique factorization domain (UFD) because $D = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ and we have $3 \times 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ and 3, $2 + \sqrt{-5}$ and $2 - \sqrt{-5}$ are irreducible in D. However, D has a property which is almost as good as being a UFD: it is a *Dedekind ring*, i.e., every nonzero ideal of D can be written uniquely as a product of prime ideals.

We will briefly illustrate how to show this using the important notion in Algebraic Number Theory of **class number**.

Definition 8. *Two ideals $A, B \subset D$ are said to be equivalent, $A \sim B$, if there exist nonzero $\alpha, \beta \in D$ such that $(\alpha)A = (\beta)B$. This is an equivalence relation on the set of ideals of D. The equivalence classes are called ideal classes. The number of classes, h_F, is called the class number of F.*

Notice that $h_F = 1$ if and only if D is a principal ideal domain (PID). Thus we can interpret the class number as measuring, in some sense, how far D is from being a PID. We will show that h_F is always finite using two Lemmas, the second of which is due to A. Hurwitz.

Lemma 4. *For any nonzero ideal A, D/A is finite.*

Lemma 5 (A. Hurwitz)**.** *There exists a positive integer M depending only on F with the following property. Given $\alpha, \beta \in D$, $\beta \neq 0$ there is an integer t, $1 \leq t \leq M$, and an element $\omega \in D$ such that $|N(t\alpha - \omega\beta)| < |N(\beta)|$.*

Proofs of these Lemmas can be found in [IR].

Theorem 2. *The class number h_F is finite.*

Proof. Let A be an ideal in D. For $\alpha \in A$, $\alpha \neq 0$, we know that $|N(\alpha)|$ is a positive integer. Choosing $\beta \in A$ nonzero such that $|N(\beta)|$ is minimal, we know from Lemma 5 that there are t, $1 \leq t \leq M$, and $\omega \in D$ such that $|N(t\alpha - \omega\beta)| < |N(\beta)|$. Since $t\alpha - \omega\beta \in A$ we must have $t\alpha - \omega\beta = 0$. It then follows that $M!A \subset (\beta)$ or equivalently $(\beta^{-1})M!A \subset D$. Let $B = (\beta^{-1})M!A$. Then B is an ideal and $M!A = (\beta)B$. Since $\beta \in A$, one must have $M!\beta \in (\beta)B$ and so $M! \in B$. Now, by Lemma 4, we know that $M!$ can be contained in at most finitely many ideals (because $D/(M!)$ is finite). Hence, we have shown that $A \sim B$ where B is one of at most finitely many ideals. Thus h_F is finite, as we wanted to show. □

Using that the class number is finite it is easy to demonstrate the following proposition.

Proposition 11.

1. *For any ideal $A \subset D$ there is an integer k, $1 \leq k \leq h_F$ such that A^k is a principal ideal.*
2. *If A and B are ideals such that $A \subset B$ then there exists and ideal C such that $A = BC$;*
3. *Every ideal can be written as a product of prime ideals.*

Proof. We will only demonstrate *3* using *2*. Let A be a proper ideal. We know from Lemma 4 that D/A is finite and so it is contained in some maximal ideal P_1. By 2) we know that there is some ideal B_1 such that $A = P_1B_1$. If $B_1 \neq D$ we can use similar reasoning to obtain a maximal ideal P_2 and an ideal B_2 such that $A = P_1P_2B_2$. If $B_2, B_3, ... \neq D$ we can continue with this process indefinitely. However, since $A \subset B_1 \subset B_2 \subset ...$ is a proper ascending chain of ideals we get contradiction with Lemma 4 because D/A if finite and so there must be a t such that $B_t = D$. Thus $A = P_1P_2...P_t$. □

It should be stressed that one can show using Proposition 11 *(1)* that the ideal classes can be made into a group. The group structure on the ideal classes is a much studied problem in Modern Algebraic Number Theory.

We are almost done proving that D is a *Dedekind ring*. We've already demonstrated that an ideal of D factors into a product of prime ideals. It just remains to show that this factorization is unique. For that, we need to define the order of a prime ideal in another ideal, an analogous of the order of a prime number in an integer.

Definition 9. *Let P be a prime ideal and A an ideal. Then $ord_P A$ is defined to be the unique nonnegative integer t such that $A \subset P^t$ and $A \not\subset P^{t+1}$.*

It is worthwhile mentioning that this definition makes sense, that is, that such a t always exists and that it is unique. Also, it verifies three rather expected properties.

Proposition 12.

1. *$ord_P P = 1$;*
2. *If $P' \neq P$ is prime then $ord_P P' = 0$;*
3. *$ord_P AB = ord_P A + ord_P B$.*

Making use of Proposition 12 we can now demonstrate that D is a *Dedekind ring.*

Theorem 3. *Let $A \subset D$ be an ideal. Then $A = \prod_P P^{a(P)}$ where the product runs over all prime ideals of D and the $a(P)$ are nonnegative integers all but finitely many of which are zero. The integers $a(P)$ are uniquely determined by $a(P) = ord_P A$.*

Proof. The product representation follows from *3* of Proposition 11. If P_0 is a prime ideal, then to check that $a(P_0) = ord_{P_0} A$ we just need to apply ord_{P_0} to both sides of the product. Using Proposition 12 we obtain:

$$ord_{P_0} A = \sum_P a(P) ord_{P_0} P = a(P_0)$$

□

Chapter 4

Examples of Algebraic Number Fields

In this section we will briefly describe two very simple classes of algebraic number fields: *quadratic number fields* and *cyclotomic fields*. In quadratic number fields the concepts of norm, trace and discriminant are very simple and will be computed in this section. Using them, we will be able to characterize the factorization into prime ideals of the ideals (p) where p is a prime number. For cyclotomic fields, even though the notions of norm, trace and discriminant are not as simple as for quadratic fields, we will still be able to study the structure of the ideals (p). In the end, we will see that these two classes of algebraic number fields are in some sense related: any quadratic number field is contained in some cyclotomic field.

For more information on these algebraic number fields, the interested reader should consult chapter 13 of [IR].

4.1 Quadratic Number Fields

A **quadratic number field** F is a number field such that $[F : \mathbb{Q}] = 2$. Using the results from the previous section we will study the structure of the ring of integers D of a quadratic field F.

Since $[F : \mathbb{Q}] = 2$ we know that $F = \mathbb{Q}[\alpha]$ where α satisfies a quadratic equation in $\mathbb{Q}[x]$. Using the formula for the roots of a quadratic polynomial one can see that in fact $F = \mathbb{Q}[\sqrt{d}]$ where d is a square-free integer. It is now obvious that, given $\alpha = a + b\sqrt{d} \in F$ we have $\alpha^{(1)} = \alpha = a + b\sqrt{d}$ and $\alpha^{(2)} = a - b\sqrt{d}$. Also, the norm and the trace of α are, by Proposition 8 of the previous chapter, $N(\alpha) = a^2 - db^2$ and $t(\alpha) = 2a$.

Example 5. *$F = \mathbb{Q}[\sqrt{-1}] = \mathbb{Q}[i]$ is a quadratic number field. Given $\alpha \in \mathbb{Q}[i]$, the norm of α is the square of the usual norm in the complex numbers. Its trace is $t(\alpha) = 2\Re(\alpha)$.*

In the previous chapter we saw that if $\alpha \in D$ then $t(\alpha)$ and $N(\alpha)$ are integers. For quadratic number field the reciprocal is also true. If $t(\alpha)$ and $N(\alpha)$ are integers then $(x-\alpha^{(1)})(x-\alpha^{(2)}) = x^2 - t(\alpha)x + N(\alpha) \in \mathbb{Z}[x]$ and so $\alpha \in D$. Thus $\alpha \in D$ if and only if $t(\alpha) \in \mathbb{Z}$ and $N(\alpha) \in \mathbb{Z}$. Using this result, it is a simple exercise to describe D explicitly.

Proposition 13.
If $d \equiv 2,\ 3\ (mod\ 4)$ *then* $D = \mathbb{Z} + \mathbb{Z}\sqrt{d}$.
If $d \equiv 1\ (mod\ 4)$ *then* $D = \mathbb{Z} + \mathbb{Z}\left(\frac{-1+\sqrt{d}}{2}\right)$.

With this result we can compute an important value of a quadratic number field known as the **discriminant** of D and denoted by δ_F. Given an **integral basis** $\alpha_1, ..., \alpha_n$ for D, that is, $\alpha_1, ..., \alpha_n$ is a basis for F over $\mathbb{Q}$ and $D = \mathbb{Z}\alpha_1 + ... + \mathbb{Z}\alpha_n$, we define the discriminant of D as $\delta_F = \Delta(\alpha_1, ..., \alpha_n)$. This definition is standard for any number field, not just quadratic number fields. Since for any integral basis $\alpha_1, ..., \alpha_n$ we have $\alpha_i \in D$, we know from Definition 5 that δ_F is an integer. Furthermore, from Proposition 9 it follows that $\delta_F \neq 0$. In particular, for quadratic number fields one has:

Proposition 14.
If $d \equiv 2,\ 3\ (mod\ 4)$ *then* $\delta_F = 4d$.
If $d \equiv 1\ (mod\ 4)$ *then* $\delta_F = d$.

Proof. Using Proposition 13 and Proposition 10 one has:

- If $d \equiv 2,\ 3\ (\text{mod } 4)$ then $\delta_F = \Delta(1, \sqrt{d}) = \det^2 \begin{pmatrix} 1 & \sqrt{d} \\ 1 & -\sqrt{d} \end{pmatrix} = 4d$.
- If $d \equiv 1\ (\text{mod } 4)$ then $\delta_F = \Delta(1, \frac{-1+\sqrt{d}}{2}) = \det^2 \begin{pmatrix} 1 & \frac{-1+\sqrt{d}}{2} \\ 1 & \frac{-1-\sqrt{d}}{2} \end{pmatrix} = d$.

□

We can now describe the factorization into prime ideals of some ideals in D in terms of δ_F. Let p be a prime in $\mathbb{Z}$, P a prime ideal in D containing p and $P^{(2)} = \{\alpha^{(2)} | \alpha \in P\}$ (which is easily seen to be a prime ideal in D containing (p)).

Proposition 15. *Suppose* p *is odd. Then:*

1. *If* $p \nmid \delta_F$ *and* $x^2 \equiv d\ (mod\ p)$ *is solvable in* $\mathbb{Z}$ *then* $(p) = PP^{(2)}$ *and* $P \neq P^{(2)}$.
2. *If* $p \nmid \delta_F$ *and* $x^2 \equiv d\ (mod\ p)$ *is not solvable in* $\mathbb{Z}$ *then* $(p) = P$.
3. *If* $p \mid \delta_F$ *then* $(p) = P^2$.

Proposition 16. *Suppose* $p = 2$. *Then:*

1. *If* $2 \nmid \delta_F$ *and* $d \equiv 1 \pmod 8$ *then* $(2) = PP^{(2)}$ *and* $P \neq P^{(2)}$.

2. *If* $2 \nmid \delta_F$ *and* $d \equiv 5 \pmod 8$ *then* $(2) = P$.

3. *If* $2 \mid \delta_F$ *then* $(2) = P^2$.

The proofs of these propositions can be found in [IR].

4.2 Cyclotomic Fields

Let m be a positive integer and let $\zeta_m = e^{\frac{2\pi i}{m}}$. Note that ζ_m satisfies the polynomial equation $x^m - 1 = 0$, as do all of its powers. Thus, one has $x^m - 1 = (x-1)(x-\zeta_m)...(x-\zeta_m^{m-1})$. The field $F = \mathbb{Q}(\zeta_m)$ is called the **cyclotomic field of mth roots of unity** and it is an algebraic number field.

Example 6. *$F = \mathbb{Q}[v]$ where $v = e^{\frac{2\pi i}{5}}$. Notice that $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$ where the last factor is an irreducible polynomial over $\mathbb{Z}$. Thus, $[F : \mathbb{Q}] = 4$.*

Example 7. *$F = \mathbb{Q}[w]$ where $w = e^{\frac{2\pi i}{6}}$. Notice that $x^6 - 1 = (x-1)(x+1)(x^2-x+1)(x^2+x+1)$ where $x^2 - x + 1 = (x-w)(x-w^5)$. Since $w \notin \mathbb{Q}$, we have $[F : \mathbb{Q}] = 2$. In fact $F = \mathbb{Q}[\sqrt{-3}]$.*

Examples 6 and 7 show that the degree of a cyclotomic extension does not necessarily increase with m. However, this degree is closely related with m and with the **mth cyclotomic polynomial**.

Definition 10. *Let* $\Phi_m(x) = \prod_{\gcd(a,m)=1} (x - \zeta_m^a)$ *where* $1 \leq a \leq m$. *This polynomial is called the* ***mth cyclotomic polynomial***.

Notice that $\Phi_m(x)$ has as roots precisely the roots of unity with order m and that its degree is $\phi(m)$. In fact $\phi(m)$ is also the degree of $\mathbb{Q}[\zeta_m]$ over $\mathbb{Q}$, as a result of the following Theorem.

Theorem 4. *The mth cyclotomic polynomial $\Phi_m(x)$ is in $\mathbb{Z}[x]$ and is irreducible in $\mathbb{Z}[x]$.*

From the above Theorem we can see that $\Phi_m(x)$ is the minimal polynomial of ζ_m in $\mathbb{Z}[x]$ and so $[\mathbb{Q}[\zeta_m] : \mathbb{Q}] = \phi(m)$.

What can be said about the ring of integers D in $\mathbb{Q}[\zeta_m]$? We know that $\mathbb{Z}[\zeta_m] \subseteq D$ because $\mathbb{Z} \subseteq D$ and $\zeta_m \in D$ but is $D = \mathbb{Z}[\zeta_m]$? The answer is yes but the proof is not simple for general m. A proof when m is prime can be found in [IR].

Like we did for quadratic number fields in the previous section, we now wish to study more closely how certain ideals factor in D.

Theorem 5. *Let p be a prime such that $p \nmid m$. Let f be the smallest positive integer such that $p^f \equiv 1 \,(mod\, m)$. Then in $D \subset \mathbb{Q}(\zeta_m)$ we have*

$$(p) = P_1 ... P_g,$$

where each P_i is such that D/P_i has p^f elements and $g = \frac{\phi(m)}{f}$.

Theorem 5 is a very pleasant result on the decomposition of primes which do not divide m. For primes which do divide m we consider only the special case when $m = l$ is prime.

Proposition 17. *Let l be a prime in $\mathbb{Z}$. Then, in $\mathbb{Q}[\zeta_l]$, one has $(l) = L^{l-1}$ where $L = (1 - \zeta_l)$.*

It is interesting to notice that the decomposition of (p) varies drastically from when $p \nmid m$ to when $p \mid m$. In the first case, (p) only decomposes into unramified factors. In the second case, when m is prime, (p) ramifies completely.

To end this chapter we illustrate how quadratic number fields are closely related with cyclotomic fields. First, let's prove that if p is an odd prime then either $\sqrt{p} \subset \mathbb{Q}[\zeta_p]$ or $\sqrt{-p} \subset \mathbb{Q}[\zeta_p]$. From the polynomial identity

$$1 + x + ... + x^{p-1} = \frac{x^p - 1}{x - 1} = \prod_{j=1}^{p-1} (x - \zeta_p^j)$$

substituting $x = 1$ we obtain

$$p = \prod_{j=1}^{p-1} (1 - \zeta_p^j)$$

Grouping together the terms corresponding to j and $p - j$ in the following way

$$(1 - \zeta_p^j)(1 - \zeta_p^{p-j}) = (1 - \zeta_p^j)(1 - \zeta_p^{-j}) = -\zeta_p^{-j}(1 - \zeta_p^j)^2$$

one gets

$$p = (-1)^{\frac{p-1}{2}} \zeta_p^b \prod_{j=1}^{\frac{p-1}{2}} (1 - \zeta_p^j)^2, \text{ where } b = -(1 + 2 + ... + \frac{p-1}{2})$$

Since p is odd, there is $c \in \mathbb{Z}$ such that $2c \equiv 1 \,(\text{mod } p)$. Thus, $\zeta^b = (\zeta^{bc})^2$. It follows that $(-1)^{\frac{p-1}{2}} p$ is a square in $\mathbb{Q}[\zeta_p]$ and hence either $\sqrt{p}$ or $\sqrt{-p}$ are in $\mathbb{Q}[\zeta_p]$. It is now straightforward to prove the next proposition:

Proposition 18. *Let p be a prime number. Then $\mathbb{Q}[\sqrt{p}] \subset \mathbb{Q}[\zeta_{4p}]$.*

Proof. For $p = 2$ the result is trivial. For $p > 2$ we just have to check that $\sqrt{p} \in \mathbb{Q}[\zeta_{4p}]$. From what was said above we know that either $\sqrt{p}$ or $\sqrt{-p}$ are in $\mathbb{Q}[\zeta_p] \subset \mathbb{Q}[\zeta_{4p}]$. Since $i \in \mathbb{Q}[i] \subset \mathbb{Q}[\zeta_{4p}]$ we conclude that $\sqrt{p} \in \mathbb{Q}[\zeta_{4p}]$. □

As a matter of fact, Proposition 18 can be more or less extended to all other quadratic fields.

Proposition 19. *Any quadratic number field is contained in a cyclotomic field.*

Proof. Let's consider the quadratic field $\mathbb{Q}[\sqrt{d}]$ where $d = \pm p_1 p_2 ... p_k$ where the p_j are prime numbers. Using Proposition 18 we get:

$$\mathbb{Q}[\sqrt{d}] \subset \mathbb{Q}[\sqrt{p_1}, ..., \sqrt{p_k}] \subset \mathbb{Q}[\zeta_{4p_1}, ..., \zeta_{4p_k}] \subset \mathbb{Q}[\zeta_{4p_1 p_2 ... p_k}]$$

□

Bibliography

[IR] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, New York, Springer-Verlag, 1990

[JPS] J. P. Serre, *A Course in Arithmetic*, New York, Springer-Verlag, 1973

[MRM] M. Ram Murty, *Problems in Analytic Number Theory*, 2nd Edition, New York, Springer-Verlag, 2008

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