Chapter 5
The Zeta Function of an Algebraic Number Field and Some Applications

At the end of Sect. 4.6 of Chap. 4, we left ourselves with the problem of determining the finite nonempty subsets S of the positive integers such that for infinitely many primes p, S is a set of non-residues of p. We observed there that if S has this property then the product of all the elements in every subset of S of odd cardinality is never a square. The object of this chapter is to prove the converse of this statement, i.e., we wish to prove Theorem 4.12. The proof of Theorem 4.12 that we present uses ideas that are closely related to the ones that Dirichlet used in his proof of Theorem 4.5, together with some technical improvements due to Hilbert. The key tool that we need is an analytic function attached to algebraic number fields, called the *zeta function* of the field. The definition of this function requires a significant amount of mathematical technology from the theory of algebraic numbers, and so in Sect. 5.1 we begin with a discussion of the results from algebraic number theory that will be required, with Dedekind's Ideal Distribution Theorem as the final goal of this section. The zeta function of an algebraic number field is defined and studied in Sect. 5.2; in particular, the Euler-Dedekind product formula for the zeta function is derived here. In Sect. 5.3 a product formula for the zeta function of a quadratic number field that will be required in the proof of Theorem 4.12 is derived from the Euler-Dedekind product formula. The proof of Theorem 4.12, the principal object of this chapter, is carried out in Sect. 5.4 and some results which are closely related to that theorem are also established there. In the interest of completeness, we prove in Sect. 5.5 the Fundamental Theorem of Ideal Theory, Theorem 3.16 of Chap. 3, since it is used in an essential way in the derivation of the Euler-Dedekind product formula.

S. Wright, *Quadratic Residues and Non-Residues*, Lecture Notes in Mathematics 2171, DOI 10.1007/978-3-319-45955-4_5

5.1 Dedekind's Ideal Distribution Theorem

We have already seen in Sects. 3.11 and 3.12 of Chap. 3 how the factorization of ideals in a quadratic number field can be used to prove the Law of Quadratic Reciprocity. The crucial fact on which that proof of quadratic reciprocity relies is the Fundamental Theorem of Ideal Theory (Theorem 3.16), the result which describes the fundamental algebraic structure of the ideals in the ring R of algebraic integers in an algebraic number field F. As we mentioned in Chap. 3, the Fundamental Theorem of Ideal Theory is due to Richard Dedekind. In order to define and study the zeta function of F, we will need another very important theorem of Dedekind which provides a precise numerical measure of how the ideals of R are distributed in R according to the cardinality of the quotient rings of R modulo the ideals. This result is often called Dedekind's Ideal Distribution Theorem, and the purpose of this section is to develop enough of the theory of ideals in R so that we can state the Ideal Distribution Theorem precisely. All of this information will then be used in the next section to define the zeta function and establish the properties of the zeta function that we will need to prove Theorem 4.12.

Let F denote an algebraic number field of degree n that will remain fixed in the discussion until indicated otherwise, and let R denote the ring of algebraic integers in F. In Sect. 3.11 of Chap. 3, we mentioned that every prime ideal of R is maximal and that the cardinality of the quotient ring R/I of R is finite for all nonzero ideals I of R. Consequently, the ideals of R are exceptionally "large" subsets of R. We begin our discussion here by proving these facts as part of the following proposition.

Proposition 5.1

(*i*) *An ideal of R is prime if and only if it is maximal.*
(*ii*) *If I is a non-zero ideal of R then the cardinality of the quotient ring R/I is finite.*
(*iii*) *If I is a prime ideal of R then there exists a rational prime $q \in \mathbb{Z}$ such that $I \cap \mathbb{Z} = q\mathbb{Z}$. In particular q is the unique rational prime contained in I.*
(*iv*) *If I is a prime ideal of R and q is the rational prime in I then R/I is a finite field of characteristic q, hence there exists a unique positive integer d such that $|R/I| = q^d$.*

Proof The proof of statements (*i*) and (*ii*) of Proposition 5.1 depend on the existence of an integral basis of R. A subset $\{\alpha_1, \ldots, \alpha_k\}$ of R is an *integral basis of R* if for each $\alpha \in R$, there exists a k-tuple $(z_1, \ldots, z_k)$ of integers, *uniquely determined by* α, such that

$$\alpha = \sum_{i=1}^{k} z_i \alpha_i.$$

It is an immediate consequence of the definition that an integral basis $\{\alpha_1, \ldots, \alpha_k\}$ is linearly independent over $\mathbb{Z}$, i.e., if $(z_1, \ldots, z_k)$ is a k-tuple of integers such that $\sum_{i=1}^{k} z_i\alpha_i = 0$ then $z_i = 0$ for $i = 1, \ldots, k$. R always has an integral basis (the interested reader may consult Hecke [27], Sect. 22, Theorem 64, for a proof of this), and it is not difficult to prove that every integral basis of R is a basis of F as a vector space over $\mathbb{Q}$; consequently, all integral bases of R contain exactly n elements.

Now for the proof of (i). Let I be a prime ideal of R: we need to prove that I is a maximal ideal, i.e., we take an ideal J of R which properly contains I and show that $J = R$.

Toward that end, let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis of R, and let $0 \neq \beta \in I$. If

$$x^m + \sum_{i=0}^{m-1} z_i x^i$$

is the minimal polynomial of β over Q then $z_0 \neq 0$ (otherwise, β is the root of a nonzero polynomial over Q of degree less that m) and

$$z_0 = -\beta^m - \sum_{1}^{m-1} z_i\beta^i \in I,$$

hence $\pm z_0 \in I$, and so I contains a positive integer a. We claim that each element of R can be expressed in the form

$$a\gamma + \sum_{1}^{n} r_i\alpha_i,$$

where $\gamma \in R,\ r_i \in [0, a-1], i = 1, \ldots, n$.

Assume this for now, and let $\alpha \in J \setminus I$. Then for each $k \in [1, \infty)$,

$$\alpha^k = a\gamma_k + \sum_{1}^{n} r_{ik}\alpha_i,\ \gamma_k \in R,\ r_{ik} \in [0, a-1],\ i = 1, \ldots, n,$$

hence the sequence $(\alpha^k - a\gamma_k : k \in [1, \infty))$ has only finitely many values; consequently there exist positive integers $l < k$ such that

$$\alpha^l - a\gamma_l = \alpha^k - a\gamma_k.$$

Hence

$$\alpha^l(\alpha^{k-l} - 1) = \alpha^k - \alpha^l = a(\gamma_k - \gamma_l) \in I\ (a \in I\ !).$$

Because I is prime, either $\alpha^l \in I$ or $\alpha^{k-l} - 1 \in I$. However, $\alpha^l \notin I$ because $\alpha \notin I$ and I is prime. Hence

$$\alpha^{k-l} - 1 \in I \subseteq J.$$

But $k - l > 0$ and $\alpha \in J$ (by the choice of α), and so $-1 \in J$. As J is an ideal, this implies that $J = R$.

Our claim must now be verified. Let $\alpha \in R$, and find $z_i \in \mathbb{Z}$ such that

$$\alpha = \sum_{i=1}^{n} z_i \alpha_i.$$

The division algorithm in $\mathbb{Z}$ implies that there exist $m_i \in \mathbb{Z}$, $r_i \in [1, a-1]$, $i = 1, \ldots, n$, such that $z_i = m_i a + r_i$, $i = 1, \ldots, n$. Thus

$$\alpha = a \sum_i m_i \alpha_i + \sum_i r_i \alpha_i = a\gamma + \sum_i r_i \alpha_i,$$

with $\gamma \in R$.

We verify (ii) next. Let $L \neq \{0\}$ be an ideal of R. We wish to show that $|R/L|$ is finite. A propos of that, choose $a \in L \cap \mathbb{Z}$ with $a > 0$ (that such an a exists follows from the previous proof of statement (i)). Then $aR \subseteq L$, hence there is a surjection of R/aR onto R/L, whence it suffices to show that $|R/aR|$ is finite.

We will in fact prove that $|R/aR| = a^n$. Consider for this the set

$$S = \Big\{ \sum_i z_i \alpha_i : z_i \in [0, a-1] \Big\}.$$

We show that S is a set of coset representatives of R/aR; if this is true then clearly $|R/aR| = |S| = a^n$. Thus, let $\alpha = \sum_i z_i \alpha_i \in R$. Then there exist $m_i \in \mathbb{Z}$, $r_i \in [0, a-1]$, $i = 1, \ldots, n$, such that $z_i = m_i a + r_i$, $i = 1, \ldots, n$. Hence

$$\alpha - \sum_i r_i \alpha_i = \Big(\sum_i m_i \Big) a \in aR \text{ and } \sum_i r_i \alpha_i \in S,$$

and so each coset of R/aR contains an element of S.

Let $\sum_i a_i \alpha_i, \sum_i a_i' \alpha_i$ be elements of S in the same coset. Then

$$\sum_i (a_i - a_i')\alpha_i = a\alpha, \text{ for some } \alpha \in R.$$

Hence there exists $m_i \in \mathbb{Z}$ such that

$$\sum_i (a_i - a_i')\alpha_i = \sum_i m_i a \alpha_i,$$

and so the linear independence (over $\mathbb{Z}$) of $\{\alpha_1, \ldots, \alpha_n\}$ implies that

$$a_i - a_i' = m_i a, \ i = 1, \ldots, n$$

i.e., a divides $a_i - a_i'$ in $\mathbb{Z}$. Because $|a_i - a_i'| < a$ for all i, it follows that $a_i - a_i' = 0$ for all i. Hence each coset of R/aR contains exactly one element of S.

In order to verify (iii), note first that the proof of statement (i) implies that $I \cap \mathbb{Z} \neq \{0\}$ and $I \cap \mathbb{Z} \neq \mathbb{Z}$ because $1 \notin I$. Hence $I \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, and is hence generated in $\mathbb{Z}$ by a unique prime number q.

Finally, we prove (iv) by concluding from Proposition 5.1(i) that I is a maximal ideal of R: a standard result in elementary ring theory asserts that if M is a maximal ideal in a commutative ring A with identity then the quotient ring A/M is a field (Hungerford [29], Theorem III.2.20), hence R/I is a field, and is finite by Proposition 5.1(ii).

To see that R/I has characteristic q, note first that $I \cap \mathbb{Z} = q\mathbb{Z}$, and so there is a natural isomorphism of the field $\mathbb{Z}/q\mathbb{Z}$ into R/I such that the identity in $\mathbb{Z}/q\mathbb{Z}$ is mapped onto the identity of R/I. Because $\mathbb{Z}/q\mathbb{Z}$ has characteristic q, it follows that if $\bar{1}$ is the identity in R/I then $q\bar{1} = 0$ in R/I, and q is the least positive integer n such that $n\bar{1} = 0$ in R/I. Hence R/I has characteristic q. QED

Remark It is a consequence of Theorem 3.16 and Proposition 5.1 that R contains infinitely many prime ideals.

It follows from Proposition 5.1(ii) that if $I \neq \{0\}$ is an ideal of R then $|R/I|$ is finite. We set

$$N(I) = |R/I|,$$

and call this the *norm of* I (we defined the norm of an ideal in this way already in Sect. 3.11 of Chap. 3 for ideals in a quadratic number field). The norm function N on nonzero ideals is multiplicative with respect to the ideal product, i.e., we have

Proposition 5.2 *If I and J are (not necessarily distinct) nonzero ideals of R then*

$$N(IJ) = N(I)N(J).$$

Proof Hecke [27], Sect. 27, Theorem 79. QED

The multiplicativity of the norm function on ideals will play a crucial role in the derivation of a very important product expansion formula for the zeta function that will be done in the next section.

Now, let

$$\mathcal{I} = \text{ the set of all nonzero ideals of } R.$$

If $n \in [1, \infty)$, let

$$Z(n) = |\{I \in \mathcal{I} : N(I) \leq n\}|.$$

The following proposition states a very important fact about the parameters $Z(n)$!

Proposition 5.3 *$Z(n) < +\infty$, for all $n \in [1, \infty)$.*

As a result of Proposition 5.3, $(Z(1), Z(2), Z(3) \dots)$ is a sequence of positive integers whose behavior determines how the ideals of R are distributed throughout R in accordance with the cardinality of the quotient rings of R. Useful information about the behavior of this sequence can hence be converted into useful information about the distribution of the ideals in R, and, as we shall see shortly, the Ideal Distribution Theorem gives very useful information about the behavior of this sequence. We turn now to the

Proof of Proposition 5.3 Perhaps the most elegant way to verify Proposition 5.3 is to make use of the ideal class group of R. We defined this group in Sect. 3.11 of Chap. 3, and for the benefit of the reader, we will recall how that goes. First declare that the ideals I and J of R are equivalent if there exist nonzero elements α and β of R such that $\alpha I = \beta J$. This defines an equivalence relation on the set of all ideals of R, and the corresponding equivalence classes are the ideal classes of R. If we let $[I]$ denote the ideal class which contains the ideal I then we define a multiplication on the set of ideal classes by declaring that the product of $[I]$ and $[J]$ is $[IJ]$. It can be shown that when endowed with this product (which is well-defined), the ideal classes of R form an abelian group, called the ideal-class group of R. It is easy to see that the set of all principal ideals of R is an ideal class, called the principal class, and one can prove that the principal class is the identity element of the ideal-class group. The ideal-class group is always finite, and the order of the ideal-class group of R is called the class number of R.

We begin the proof of Proposition 5.3 by letting C be an ideal class of R and for each $n \in [1, \infty)$, letting $\mathcal{Z}_C(n)$ denote the set

$$\{I \in C \cap \mathcal{I} : N(I) \leq n\}.$$

We claim that $|\mathcal{Z}_C(n)|$ is finite. In order to verify this, let J be a fixed nonzero ideal in C^{-1} (the inverse of C in the ideal-class group), and let

$0 \neq \alpha \in J$. Then there is a unique ideal I such that $\alpha R = IJ$, and since $[I] = C[IJ] = C[\alpha R] = C$, it follows that $I \in C \cap \mathcal{I}$. Moreover, the map $\alpha R \to I$ is a bijection of the set of all nonzero principal ideals contained in J onto $C \cap \mathcal{I}$. Proposition 5.2 implies that

$$N(\alpha R) = N(I)N(J),$$

hence

$$N(I) \leq n \text{ if and only if } N(\alpha R) \leq nN(J).$$

Hence there is a bijection of $\mathcal{Z}_C(n)$ onto the set

$$\mathcal{J} = \{\{0\} \neq \alpha R \subseteq J : N(\alpha R) \leq nN(J)\},$$

and so it suffices to show that $\mathcal{J}$ is a finite set.

That $|\mathcal{J}|$ is finite will follow if we prove that there is only a finite number of principal ideals of R whose norms do not exceed a fixed constant. Suppose that this latter statement is false, i.e., there are infinitely many elements $\alpha_1, \alpha_2, \dots$ of R such that the principal ideals $\alpha_i R, i = 1, 2, \dots$ are distinct and $(N(\alpha_1 R), N(\alpha_2 R), \dots)$ is a bounded sequence. As all of the numbers $N(\alpha_i R)$ are positive integers, we may suppose with no loss of generality that $N(\alpha_i R)$ all have the same value z.

We now wish to locate z in each ideal $\alpha_i R$. Toward that end, use the Primitive Element Theorem (Hecke [27], Sect. 19, Theorem 52) to find $\theta \in F$, of degree n over $\mathbb{Q}$, such that for each element ν of F, there is a unique polynomial $f \in \mathbb{Q}[x]$ such that $\nu = f(\theta)$ and the degree of f does not exceed $n-1$. For each i, we hence find $f_i \in \mathbb{Q}[x]$ of degree no larger than $n-1$ and for which $\alpha_i = f_i(\theta)$. If $\theta_1, \dots, \theta_n$, with $\theta_1 = \theta$, are the roots of the minimal polynomial of θ over $\mathbb{Q}$, then one can show that

$$N(\alpha_i R) = \Big| \prod_{k=1}^{n} f_i(\theta_k) \Big|$$

(Hecke [27], Sect. 27, Theorem 76). Moreover, the degree d_i of α_i over $\mathbb{Q}$ divides n in $\mathbb{Z}$, and if $\alpha_i^{(1)}, \dots, \alpha_i^{(d_i)}$, with $\alpha_i^{(1)} = \alpha_i$, denote the roots of the minimal polynomial of α_i over Q, then the numbers on the list $f_i(\theta_k), k = 1, \dots, n$, are obtained by repeating each $\alpha_i^{(j)}$ n/d_i times (Hecke [27], Sect. 19, Theorem 54). If c_0 denotes the constant term of the minimal polynomial of α_i over Q, it follows that

$$\prod_{k=1}^{n} f_i(\theta_k) = \Big(\prod_{k=1}^{d_i} \alpha_i^{(k)} \Big)^{n/d_i} = ((-1)^{d_i} c_0)^{n/d_i} \in \mathbb{Z}.$$

Because $f_i(\theta_k)$ is an algebraic integer for all i and k, it hence follows that

$$\frac{z}{\alpha_i} = \pm \prod_{k=2}^{n} f_i(\theta_k) \in \mathcal{R} \cap F = R,$$

whence $z \in \alpha_i R$, for all i.

If we now let $\{\beta_1, \ldots, \beta_n\}$ be an integral basis of R then the claim in the proof of Proposition 5.1(i) shows that for each i there exists $\gamma_i \in R$ and $z_{ij} \in [0, z-1], j = 1, \ldots, n$, such that

$$\alpha_i = z\gamma_i + \sum_{1}^{n} z_{ij}\beta_j.$$

Because $z \in \alpha_i R$, it follows that

$$\alpha_i R = zR + \Big(\sum_{1}^{n} z_{ij}\beta_j\Big)R, \text{ for all } i.$$

However, the sum $\sum_1^n z_{ij}\beta_j$ can have only finitely many values; we conclude that the ideals $\alpha_i R, i = 1, 2, \ldots$ cannot all be distinct, contrary to their choice.

We now have what we need to easily prove that $Z(n)$ is finite. Let $C_1, \ldots, C_h$ denote the distinct ideal classes of R. The set of all the ideals of R is the (pairwise disjoint) union of the C_i's hence $\{I \in \mathcal{I} : N(I) \leq n\}$ is the union of $\mathcal{J}_{C_1}(n), \ldots, \mathcal{J}_{C_h}(n)$. Because each set $\mathcal{J}_{C_i}(n)$ is finite, so therefore is $|\{I \in \mathcal{I} : N(I) \leq n\}| = Z(n)$. QED

We can now state the main result of this section:

Theorem 5.4 (Dedekind's Ideal Distribution Theorem) *The limit*

$$\lim_{n\to\infty} \frac{Z(n)}{n} = \lambda$$

exists, is positive, and its value is given by the formula

$$\lambda = \frac{2^{r+1}\pi^e \rho}{w\sqrt{|d|}} h,$$

where

$$\begin{aligned} d &= \text{ discriminant of } F, \\ e &= \frac{1}{2}(\text{number of complex embeddings of } F \text{ over } \mathbb{Q}), \end{aligned}$$

$$\begin{aligned} h &= \text{ class number of } R, \\ r &= \text{ unital rank of } R, \\ \rho &= \text{ regulator of } F, \\ w &= \text{ order of the group of roots of unity in } R. \end{aligned}$$

Thus the number of nonzero ideals of R whose norms do not exceed n is asymptotic to λn as $n \to +\infty$.

The establishment of Theorem 5.4 calls for several results from the theory of algebraic numbers whose exposition would take us too far from what we wish to do here, so we omit the proof and instead refer the interested reader to Hecke [27], Sect. 42, Theorem 122. Although we will make no further use of them, readers who are also interested in the definition of the discriminant of F and the regulator of F, should see, respectively, the definition on p. 73 and the definition on p. 116 of Hecke [27]. We will define the parameter e and the unital rank of R in the two paragraphs after the next one. The integers d, e, h, r, w, and the real number ρ are fundamental parameters associated with F which govern many aspects of the arithmetic and algebraic structure of F and R; Theorem 5.4 is a remarkable example of how these parameters work in concert to do that.

Although the parameters which are used in the formula for the value of the limit $\lambda = \lim_{n\to\infty} Z(n)/n$ are rather complicated to define for an arbitrary algebraic number field, they are much simpler to describe for a quadratic number field, so as to gain a better idea of how they determine the asymptotic behavior of the sequence $Z(1), Z(2), \ldots$, we will take a closer look at what they are for quadratic fields. Thus, let $\mathbb{Q}(\sqrt{m})$ be the quadratic number field determined by the square-free integer $m \neq 0$ or 1. As we pointed out in Sect. 3.11 of Chap. 3, the discriminant of $\mathbb{Q}(\sqrt{m})$ is either m or $4m$, if m is, or respectively, is not, congruent to 1 mod 4.

In order to calculate the parameter e in Theorem 5.4, one needs to consider the *embeddings* of an algebraic number field, i.e., the ring isomorphisms of the field into the set of complex numbers which fixes each element of $\mathbb{Q}$. An embedding is said to be *real* if its range is a subset of the real numbers, otherwise, the embedding is said to be *complex*. It can be shown that the number of embeddings is equal to the degree of the field and that the number of complex embeddings is even, and so e is well-defined in Theorem 5.4. It follows that the quadratic field $\mathbb{Q}(\sqrt{m})$ has precisely two embeddings: one is the trivial embedding which maps each element of $\mathbb{Q}(\sqrt{m})$ to itself, and the other is the mapping on $\mathbb{Q}(\sqrt{m})$ induced by the algebraic conjugate of $\sqrt{m}$ which sends the element $q + r\sqrt{m}$ for $(q, r) \in \mathbb{Q} \times \mathbb{Q}$ to the element $q - r\sqrt{m}$. It follows that if $m > 0$ then there are no complex embeddings of $\mathbb{Q}(\sqrt{m})$ and if $m < 0$ then there are exactly 2 complex embeddings. Thus if $m > 0$ then $e = 0$ and if $m < 0$ then $e = 1$.

We have already defined the class number h, and so we turn next to the unital rank r. This parameter is determined by the structure of the group of

units in an algebraic number field. It can be shown that the group of units in the ring of algebraic integers R in the algebraic number field F is isomorphic to the direct sum of the finite cyclic group of roots of unity that are contained in F and a free abelian group of finite rank r (Hecke [27], Sect. 34, Theorem 100). The rank r of this free-abelian summand is by definition the *unital rank* of R. When we now let $F = \mathbb{Q}(\sqrt{m})$, it can be shown that if $m < 0$ then the group of units of $\mathbb{Q}(\sqrt{m})$ has no free-abelian summand, and so $r = 0$ in this case. On the other hand, if $m > 0$ then there is a unit ϖ of R in the group of units $U(R)$ such that $U(R) = \{\pm\varpi^n : n \in \mathbb{Z}\}$. If ϖ is chosen to exceed 1 then it is uniquely determined as a generator of $U(R)$ in this way and is called the *fundamental unit of* R. It follows that when $m > 0$, the group of units of R is isomorphic to the direct sum of the cyclic group of order 2 and the free abelian group $\mathbb{Z}$, hence the unital rank r is 1 in this case.

The regulator ρ of an algebraic number field F is also determined by the group of units of R by means of a rather complicated formula that uses a determinant that is calculated from a basis of the free-abelian summand of the group of units. For a quadratic number field $\mathbb{Q}(\sqrt{m})$ with $m < 0$, whose group of units has no free-abelian summand, the regulator is taken to be 1, and if $m > 0$ then the regulator of $\mathbb{Q}(\sqrt{m})$ turns out to be $\log \varpi$, where ϖ is the fundamental unit of R.

If $m > 0$ then the group of roots of unity in $\mathbb{Q}(\sqrt{m})$ is simply $\{-1, 1\}$, and so the order w of the group of roots of unity is 2. If $m < 0$ then it can be shown that w is 2 when $m < -4$, it is 6 when $m = -3$, and it is 4 when $m = -1$.

Taking all of this information into account, we see that for the quadratic number field $\mathbb{Q}(\sqrt{m})$, the conclusion of Theorem 5.4 can be stated as follows: if $m > 0$ and ϖ is the fundamental unit in $R = \mathcal{R} \cap \mathbb{Q}(\sqrt{m})$ then

$$\lim_{n\to\infty} \frac{Z(n)}{n} = \begin{cases} \dfrac{2\log\varpi}{\sqrt{m}}h, \text{ if } m \equiv 1 \bmod 4, \\ \\ \dfrac{\log\varpi}{\sqrt{m}}h, \text{ if } m \not\equiv 1 \bmod 4, \end{cases}$$

and if $m < 0$ then

$$\lim_{n\to\infty} \frac{Z(n)}{n} = \begin{cases} \dfrac{2\pi}{w\sqrt{|m|}}h, \text{ if } m \equiv 1 \bmod 4, \\ \\ \dfrac{\pi}{w\sqrt{|m|}}h, \text{ if } m \not\equiv 1 \bmod 4, \end{cases}$$

where w is 2 when $m < -4$, 6 when $m = -3$, and 4 when $m = -1$. The Ideal Distribution Theorem for quadratic number fields is in fact due to Dirichlet; after a careful study of Dirichlet's result, Dedekind generalized it to arbitrary algebraic number fields.

5.2 The Zeta Function of an Algebraic Number Field

We are now in a position to define and study the zeta function. Let F be an algebraic number field of degree n and let R denote the ring of algebraic integers in F, as before. Consider next the set $\mathcal{I}$ of all nonzero ideals of R. It is a consequence of Proposition 5.3 that $\mathcal{I}$ is countable, and so if $s \in \mathbf{C}$ then the formal series

$$\sum_{I \in \mathcal{I}} \frac{1}{N(I)^s} \qquad (*)$$

is defined, relative to some fixed enumeration of $\mathcal{I}$. As we shall see, the zeta function of F will be defined by this series. However, in order to do that precisely and rigorously, a careful examination of the convergence of this series must be done first. That is what we will do next.

If we let

$$L(n) = |\{I \in \mathcal{I} : N(I) = n\}|, \ \ n \in [1, \infty),$$

then by formal rearrangement of its terms, we can write the series $(*)$ as

$$\sum_{n=1}^{\infty} \frac{L(n)}{n^s}. \qquad (**)$$

The series $(**)$ is a *Dirichlet series*, i.e., a series of the form

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

where (a_n) is a given sequence of complex numbers. The L-function of a Dirichlet character is another very important example of a Dirichlet series.

We will determine the convergence of the series $(*)$ by studying the convergence of the Dirichlet series $(**)$. This will be done by way of the following proposition, which describes how a Dirichlet series converges.

Proposition 5.5 *Let (a_n) be sequence of complex numbers, let*

$$S(n) = \sum_{k=1}^{n} a_k,$$

and suppose that there exits $\sigma \geq 0, C > 0$ such that

$$\left| \frac{S(n)}{n^\sigma} \right| \leq C, \ \textit{for all } n \textit{ sufficiently large.}$$

Then the Dirichlet series

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

converges in the half-plane $\operatorname{Re}\ s > \sigma$ *and uniformly in each closed and bounded subset of this half-plane. Moreover, if*

$$\lim_{n\to\infty} \frac{S(n)}{n} = d$$

then

$$\lim_{s\to 1^+} (s-1) \sum_{n=1}^{\infty} \frac{a_n}{n^s} = d.$$

*Proof (*according to Hecke [27], Sect. 42, Lemmas (a), (b), (c)*)* Let m and h be integers, with $m > 0$ and $h \geq 0$, and let $K \subseteq \{s : \operatorname{Re}\ s > \sigma\}$ be a compact (closed and bounded) set. Then

$$\begin{aligned}
\sum_{n=m}^{m+h} \frac{a_n}{n^s} &= \sum_{n=m}^{m+h} \frac{S(n) - S(n-1)}{n^s} \\
&= \frac{S(m+h)}{(m+h)^s} - \frac{S(m-1)}{m^s} + \sum_{n=m}^{m+h-1} S(n)\Big(\frac{1}{n^s} - \frac{1}{(n+1)^s}\Big) \\
&= \frac{S(m+h)}{(m+h)^s} - \frac{S(m-1)}{m^s} + s \sum_{n=m}^{m+h-1} S(n) \int_n^{n+1} \frac{dx}{x^{s+1}}.
\end{aligned}$$

If we now use the stipulated bound on the quotients $S(n)/n^\sigma$, it follows that

$$\begin{aligned}
\Big|\sum_{n=m}^{m+h} \frac{a_n}{n^s}\Big| &\leq \frac{2C}{m^{\operatorname{Re}\ s-\sigma}} + C|s| \int_m^{\infty} \frac{dx}{x^{\operatorname{Re}\ s-\sigma+1}} \\
&= \frac{2C}{m^{\operatorname{Re}\ s-\sigma}} + \frac{C|s|}{\operatorname{Re}\ s-\sigma}\ \frac{1}{m^{\operatorname{Re}\ s-\sigma}}.
\end{aligned}$$

Because K is a compact subset of $\operatorname{Re}\ s > \sigma$, it is bounded and lies at a positive distance δ from $\operatorname{Re}\ s = \sigma$, i.e., there is a positive constant C' such that

$$\operatorname{Re}\ s - \sigma \geq \delta \text{ and } |s| \leq C', \text{ for all } s \in K.$$

Hence there is a positive constant C'', independent of m and h, such that

$$\Big|\sum_{n=m}^{m+h}\frac{a_n}{n^s}\Big| \le C''\Big(1+\frac{1}{\delta}\Big)\frac{1}{m^\delta}\ , \text{ for all } s\in K.$$

As m and h are chosen arbitrarily and δ depends on neither m nor h, this estimate implies that the Dirichlet series converges uniformly on K, and as K is also chosen arbitrarily, it follows that the series converges to a function continuous in Re $s > \sigma$.

We now assume that

$$\lim_{n\to\infty}\frac{S(n)}{n} = d;$$

we wish to verify that

$$\lim_{s\to 1^+}(s-1)\sum_{n=1}^{\infty}\frac{a_n}{n^s} = d.$$

From what we have just shown, it follows that the Dirichlet series now converges for $s > 1$. Let

$$S(n) = dn + \varepsilon_n n, \text{ where } \lim_{n\to\infty}\varepsilon_n = 0,$$

$$\varphi(s) = \sum_{n=1}^{\infty}\frac{a_n}{n^s},\ s > 1.$$

Then for $s > 1$, we have that

$$\begin{aligned}|\varphi(s) - d\zeta(s)| &= s\Big|\sum_{n=1}^{\infty} n\varepsilon_n\int_n^{n+1}\frac{dx}{x^{s+1}}\Big| \\ &< s\sum_{n=1}^{\infty}|\varepsilon_n|\int_n^{n+1}\frac{dx}{x^s}.\end{aligned}$$

Let $\epsilon > 0$, and choose an integer N and a positive constant A such that $|\varepsilon_n| < \epsilon$, for all $n \ge N$, and $|\varepsilon_n| \le A$, for all n. Then

$$\begin{aligned}&|(s-1)\varphi(s) - d(s-1)\zeta(s)| \\ &\quad< As(s-1)\sum_{n=1}^{N-1}\int_n^{n+1}\frac{dx}{x} + \epsilon s(s-1) + \sum_{n=N}^{\infty}\int_n^{n+1}\frac{dx}{x^s} \\ &\quad= As(s-1)\log N + \epsilon s(s-1)\int_N^{\infty}\frac{dx}{x^s}.\end{aligned}$$

Because the last expression has limit ϵ as $s \to 1$, it follows that

$$\lim_{s \to 1^+} \big((s-1)\varphi(s) - d(s-1)\zeta(s)\big) = 0.$$

We now claim that

$$\lim_{s \to 1^+} (s-1)\zeta(s) = 1;$$

if this is so, then

$$\lim_{s \to 1^+} (s-1)\varphi(s) = d,$$

as desired. This claim can be verified upon noting that

$$\int_n^{n+1} \frac{dx}{x^s} < \frac{1}{n^s} < \int_{n-1}^{n} \frac{dx}{x^s}\ , \text{ for all } n \in [2, \infty) \text{ and for all } s > 1.$$

Hence

$$\frac{1}{s-1} = \int_1^{\infty} \frac{dx}{x^s} < \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s) < 1 + \int_1^{\infty} \frac{dx}{x^s} = \frac{s}{s-1},$$

and so

$$1 < (s-1)\zeta(s) < s, \text{ for all } s > 1,$$

from which the claim follows immediately. QED

Because each function a_n/n^s is an entire function of s, a Dirichlet series which satisfies the hypotheses of Proposition 5.5 is a series of functions each term of which is analytic in Re $s > \sigma$ and which also converges uniformly on every compact subset of Re $s > \sigma$. Hence the sum of the series is analytic in Re $s > \sigma$.

We wish to apply Proposition 5.5 to the series (**), and so we must study the behavior of the sequence

$$Z(n) = \sum_{k=1}^{n} L(k).$$

It is here that we make use of Theorem 5.4; it follows from that theorem that there is a positive constant λ such that

$$\lim_{n \to \infty} \frac{Z(n)}{n} = \lambda,$$

whence the sequence $(Z(n)/n)_{n=1}^{\infty}$ is bounded. Therefore the hypotheses of Proposition 5.5 are satisfied for $a_n = L(n)$ with $\sigma = 1$, hence the series (∗∗) converges to a function analytic in Re $s > 1$.

We now let $s > 1$. Because $L(n) \geq 0$ for all n, the convergence of (∗∗) is absolute for $s > 1$, hence we can rearrange the terms of (∗∗) in any order without changing its value. It follows that the value of the series

$$\sum_{I \in \mathcal{I}} \frac{1}{N(I)^s}$$

for $s > 1$ is finite, is independent of the enumeration of $\mathcal{I}$ used to define the series, and is given by the value of the Dirichlet series (∗∗).

Definition The *(Dedekind-Dirichlet) zeta function of* F is the function $\zeta_F(s)$ defined for $s > 1$ by

$$\zeta_F(s) = \sum_{I \in \mathcal{I}} \frac{1}{N(I)^s}.$$

Remark One can show without difficulty that if $\sum_n a_n/n^s$ is a Dirichlet series which satisfies the hypotheses of Proposition 5.5 then $\sum_n a_n/n^s$ converges absolutely in Re $s > 1 + \sigma$. If we apply this fact to the series (∗∗), it follows that (∗∗) converges absolutely in Re $s > 2$. Hence the value of the series

$$\sum_{I \in \mathcal{I}} \frac{1}{N(I)^s}$$

for Re $s > 2$ is finite, is independent of the enumeration of $\mathcal{I}$ used to define the series, and is given by the value of the series (∗∗). Although we will make no use of this fact, it follows that the zeta function of F can be defined by the series (∗∗) not only for $s > 1$, but also for Re $s > 1$, and when so defined, is analytic in that half-plane.

For emphasis, we record in the following proposition the observation that we made about the value of the zeta function of F in the paragraph which immediately preceded its definition:

Proposition 5.6 *If*

$$L(n) = |\{I \in \mathcal{I} : N(I) = n\}|, \ \ n \in [1, \infty),$$

then

$$\zeta_F(s) = \sum_{n=1}^{\infty} \frac{L(n)}{n^s}.$$

For future reference, we also observe that Proposition 5.5 and Theorem 5.4 imply

Lemma 5.7 *If $\zeta_F(s)$ is the zeta function of F and λ is the positive constant in the conclusion of Theorem 5.4 then*

$$\lim_{s\to 1^+}(s-1)\zeta_F(s)=\lambda.$$

If $F=\mathbb{Q}$ then $R=\mathcal{R}\cap\mathbb{Q}=\mathbb{Z}$, hence the nonzero ideals of R in this case are the principal ideals $n\mathbb{Z}, n\in[1,\infty)$. Then

$$N(n\mathbb{Z})=|\mathbb{Z}/n\mathbb{Z}|=n,$$

and so

$$\{I\in\mathcal{I}:|N(I)|=n\}=\{n\mathbb{Z}\}.$$

Hence the zeta function of $\mathbb{Q}$ is

$$\zeta_{\mathbb{Q}}(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},$$

the Riemann zeta function.

The next theorem gives a product formula for $\zeta_F(s)$ that is reminiscent of the product formula for the Dirichlet L-function of a Dirichlet character that we pointed out in Sect. 4.4 of Chap. 4. It is a very useful tool for analyzing certain features of the behavior of $\zeta_F(s)$ and will play a key role in our proof of Theorem 4.12.

Theorem 5.8 (Euler-Dedekind Product Formula for ζ_F) *Let $\mathcal{Q}$ denote the set of all prime ideals of R. Then*

$$\zeta_F(s)=\prod_{I\in\mathcal{Q}}\frac{1}{1-N(I)^{-s}}\ ,\ s>1. \tag{5.1}$$

Proof Note that because a prime ideal I of R is proper, $N(I)>1$, and so each term of this product is defined for $s>1$. In order to prove the theorem we will need some standard facts about the convergence of infinite products, which we record in the following definitions and Proposition 5.9.

Definitions Let (a_n) be a sequence of complex numbers such that $a_n\neq -1$, for all n. The infinite product

$$\prod_{1}^{\infty}(1+a_n)$$

converges if

$$\lim_{n\to\infty} \prod_{1}^{n} (1 + a_k)$$

exists and is finite, and it *converges absolutely* if

$$\prod_{1}^{\infty} (1 + |a_n|)$$

converges.

Proposition 5.9

(*i*) $\prod_n (1 + a_n)$ *converges absolutely if and only if the series* $\sum_n |a_n|$ *converges.*

(*ii*) *The limit of an absolutely convergent infinite product is not changed by any rearrangement of the factors.*

Proof See Nevanlinna and Paatero [42], Sects. 13.1, 13.2. QED

Returning to the proof of Theorem 5.8, we next consider the product on the right-hand side of (5.1). Because $N(I) \geq 2$ for all $I \in \mathcal{Q}$ it follows that for $s > 1$,

$$0 < \frac{1}{1 - N(I)^{-s}} - 1 = \frac{N(I)^{-s}}{1 - N(I)^{-s}} \leq 2N(I)^{-s},$$

hence

$$\sum_{I\in\mathcal{Q}} \left(\frac{1}{1 - N(I)^{-s}} - 1 \right) \leq 2 \sum_{I\in\mathcal{Q}} N(I)^{-s} < +\infty$$

and so by Proposition 5.9, the product on the right-hand side of (5.1) converges absolutely for $s > 1$ and its value is independent of the order of the factors.

The next step is to prove that this product converges to $\zeta_F(s)$ for $s > 1$. Let

$$\Pi(x) = \prod_{I\in\mathcal{Q}:N(I)\leq x} \frac{1}{1 - N(I)^{-s}};$$

this product has only a finite number of factors by Proposition 5.3 and

$$\lim_{x\to+\infty} \Pi(x) = \prod_{I\in\mathcal{Q}} \frac{1}{1 - N(I)^{-s}}.$$

We have that

$$\frac{1}{1-N(I)^{-s}} = \sum_{n=0}^{\infty} \frac{1}{N(I)^{ns}},$$

hence $\Pi(x)$ is a finite product of absolutely convergent series, which we can hence multiply together and, in the resulting sum, rearrange terms in any order without altering the value of the sum. Proposition 5.2 implies that each term of this sum is either 1 or of the form

$$N(I_1^{\alpha_1} \cdots I_r^{\alpha_r})^{-s},$$

where $(\alpha_1, \ldots, \alpha_r)$ is an r-tuple of positive integers, I_i is a prime ideal for which $N(I_i) \leq x, i = 1, \ldots, r$, and all products of powers of prime ideals I with $N(I) \leq x$ of this form occur exactly once. Hence

$$\Pi(x) = 1 + \sum \frac{1}{N(I)^s},$$

where the sum here is taken over all ideals I of R such that all prime ideal factors of I have norm no greater than x. Now the Fundamental Theorem of Ideal Theory (Theorem 3.16) implies that all nonzero ideals of R have a unique prime ideal factorization, hence

$$\zeta_F(s) - \Pi(x) = \sum \frac{1}{N(I)^s},$$

where the sum here is taken over all ideals $I \neq \{0\}$ of R such that at least one prime ideal factor of I has norm greater than x. Hence this sum does not exceed

$$\sum_{n>x} \frac{L(n)}{n^s},$$

and so

$$\lim_{x\to+\infty} (\zeta_F(s) - \Pi(x)) = \lim_{x\to+\infty} \sum_{n>x} \frac{L(n)}{n^s} = 0.$$

QED

If $F = \mathbb{Q}$ then the prime ideals of $R = \mathbb{Z}$ are the principal ideals generated by the rational primes $q \in \mathbb{Z}$, and so it follows from Theorem 5.8 that

$$\zeta(s) = \prod_q \frac{1}{1-q^{-s}}, \quad s > 1, \tag{5.2}$$

the Euler-product expansion of Riemann's zeta.

We are now going to use Theorem 5.8 to obtain a factorization of ζ_F over rational primes that is the analog of the product expansion (5.2) of the Riemann zeta function. In order to derive it, we first recall from Proposition 5.1(*iii*) and (*iv*) that if I is a prime ideal of R then I contains a unique rational prime q and there is a unique positive integer d such that $N(I)$ is q^d. The integer d is called the *degree of* I and we will denote it by $\deg I$. We can now state and prove

Theorem 5.10 *If $\mathcal{Q}$ denotes the set of all prime ideals of R then the zeta function $\zeta_F(s)$ of F has a product expansion given by*

$$\zeta_F(s) = \prod_{q \text{ a rational prime}} \Big(\prod_{I \in \mathcal{Q}: q \in I} \frac{1}{1 - q^{-(\deg I)s}} \Big), \quad s > 1. \tag{5.3}$$

Proof If $n \in \mathbb{Z}$ then the ideal nR is contained in a prime ideal of R (Theorem 3.16) and so Proposition 5.1(*iii*) implies that $\mathcal{Q}$ can be expressed as the pairwise disjoint union

$$\bigcup_{q \text{ a rational prime}} \{I \in \mathcal{Q} : q \in I\}.$$

Hence as a consequence of Theorem 5.8 and Proposition 5.9(*ii*), we can rearrange the factors in (5.1) so as to derive the expansion (5.3) for $\zeta_F(s)$. QED

The ideal qR of R is contained in only finitely many prime ideals (because of Theorem 3.16) and so each product inside the parentheses in (5.3) has only a finite number of factors; these finite products are called the *elementary factors of* ζ_F.

5.3 The Zeta Function of a Quadratic Number Field

As has been the case frequently in much of our previous work, quadratic number fields provide interesting and important examples of various phenomena of great interest and importance in algebraic number theory, and zeta functions are no exception to this rule. In this section we will illustrate how the decomposition law for the rational primes in a quadratic number field, Proposition 3.17 from Sect. 3.11 of Chap. 3, and Theorem 5.10 can be used to derive a very useful product expansion for the zeta function of a quadratic number field. It is precisely this result that will be used to prove Theorem 4.12 in the next section.

For a square-free integer $m \neq 1$, let $F = \mathbb{Q}(\sqrt{m}), R = \mathcal{R} \cap F$. We recall for our convenience what the decomposition law for the rational primes in R says. First, let p be an odd prime. Then

(*i*) If $\chi_p(m) = 1$ then pR factors into the product of two distinct prime ideals, each of degree 1.
(*ii*) If $\chi_p(m) = 0$ then pR is the square of a prime ideal I, and the degree of I is 1.
(*iii*) If $\chi_p(m) = -1$ then pR is prime in R of degree 2.

The decomposition of the prime 2 in R occurs as follows:

(*iv*) If $m \equiv 1 \bmod 8$ then $2R$ factors into the product of two distinct prime ideals, each of degree 1.
(*v*) If $m \equiv 2$ or $3 \bmod 4$ then $2R$ is the square of a prime ideal I, and the degree of I is 1.
(*vi*) If $m \equiv 5 \bmod 8$ then $2R$ is prime in R of degree 2.

It follows from (*i*)–(*vi*) that if p is an odd prime in $\mathbb{Z}$ then the corresponding elementary factor of ζ_F is

$$\frac{1}{(1-p^{-s})^2}\ ,\ \text{if } \chi_p(m) = 1,$$
$$\frac{1}{1-p^{-s}}\ ,\ \text{if } \chi_p(m) = 0,$$
$$\frac{1}{1-p^{-2s}}\ ,\ \text{if } \chi_p(m) = -1,$$

and the elementary factor corresponding to 2 is

$$\frac{1}{(1-2^{-s})^2}\ ,\ \text{if } m \equiv 1 \bmod 8,$$
$$\frac{1}{1-2^{-s}}\ ,\ \text{if } m \equiv 2 \text{ or } 3 \bmod 4,$$
$$\frac{1}{1-2^{-2s}}\ ,\ \text{if } m \equiv 5 \bmod 8.$$

Observe next that each of the elementary factors corresponding to p can be expressed as

$$\frac{1}{1-p^{-s}}\,\frac{1}{1-\chi_p(d)p^{-s}}.$$

Hence from the product expansion (5.2) of the Riemann zeta function and the product expansion (5.3) of $\zeta_F(s)$ we deduce

Proposition 5.11 *The zeta function of* $\mathbb{Q}(\sqrt{m})$ *has the product expansion*

$$\zeta_{\mathbb{Q}(\sqrt{m})}(s) = \theta(s)\zeta(s)\prod_p \frac{1}{1-\chi_p(m)p^{-s}}, \ s > 1, \tag{5.4}$$

where

$$\theta(s) = \begin{cases} \dfrac{1}{1-2^{-s}} \text{ , if } m \equiv 1 \bmod 8, \\ 1 \text{ , if } m \equiv 2 \text{ or } 3 \bmod 4, \\ \dfrac{1}{1+2^{-s}} \text{ , if } m \equiv 5 \bmod 8. \end{cases}$$

We will use this factorization of $\zeta_{\mathbb{Q}(\sqrt{m})}(s)$ to prove, in due course, the following lemma, the crucial fact that we will need to prove Theorem 4.12.

Lemma 5.12 *If* $a \in \mathbb{Z}$ *is not a square then*

$$\sum_p \chi_p(a)p^{-s}$$

remains bounded as $s \to 1^+$.

Note that Lemma 5.12 is very similar in form and spirit to the hypothesis of Lemma 4.7, which was a key step in Dirichlet's proof of Theorem 4.5. We will eventually see that this is no accident!

5.4 Proof of Theorem 4.12 and Related Results

We now have assembled all of the ingredients necessary for a proof of Theorem 4.12. As we have already verified the "only if" implication in Theorem 4.12, we hence let S be a nonempty finite subset of $[1, \infty)$ and suppose that for each subset T of S such that $|T|$ is odd,

$$\prod_{i \in T} i \text{ is not a square.}$$

Let

$$X = \{p : \chi_p \equiv -1 \text{ on } S\}.$$

We must prove that X has infinite cardinality.

Consider the sum

$$\Sigma(s) = \sum_{(p)} \Big(\prod_{i \in S} \big(1 - \chi_p(i)\big) \Big) \cdot \frac{1}{p^s}, \ s > 1, \tag{5.5}$$

where (p) means that the summation is over all primes p such that p divides no element of S. Then

$$\Sigma(s) = 2^{|S|} \sum_{p \in X} \frac{1}{p^s}, \ s > 1,$$

hence if we can show that

$$\lim_{s \to 1^+} \Sigma(s) = +\infty, \tag{5.6}$$

then the cardinality of X will be infinite.

In order to get (5.6), we first calculate that

$$\prod_{i \in S} \big(1 - \chi_p(i)\big) = 1 + \sum_{\emptyset \neq T \subseteq S} (-1)^{|T|} \chi_p\Big(\prod_{i \in T} i \Big),$$

substitute this into (5.5) and interchange the order of summation to obtain

$$\Sigma(s) = \sum_{(p)} \frac{1}{p^s} + \sum_{\emptyset \neq T \subseteq S} (-1)^{|T|} \Big(\sum_{(p)} \chi_p\Big(\prod_{i \in T} i \Big) \cdot \frac{1}{p^s} \Big).$$

Now divide $\{ T : \emptyset \neq T \subseteq S \}$ into $U \cup V \cup W$, where

$$U = \Big\{ \emptyset \neq T \subseteq S : |T| \text{ is even and } \prod_{i \in T} i \text{ is a square} \Big\},$$

$$V = \Big\{ \emptyset \neq T \subseteq S : |T| \text{ is even and } \prod_{i \in T} i \text{ is not a square } \Big\},$$

$$W = \{ T \subseteq S : |T| \text{ is odd} \}.$$

Then

$$\begin{aligned} \Sigma(s) &= (1 + |U|) \sum_{(p)} \frac{1}{p^s} + \sum_{T \in V} \Big(\sum_{(p)} \chi_p\Big(\prod_{i \in T} i \Big) \cdot \frac{1}{p^s} \Big) \\ &\quad - \sum_{T \in W} \Big(\sum_{(p)} \chi_p\Big(\prod_{i \in T} i \Big) \cdot \frac{1}{p^s} \Big) \\ &= \Sigma_1(s) + \Sigma_2(s) - \Sigma_3(s). \end{aligned}$$

Because the range of the summation here is over all but finitely many primes, Lemma 5.12, the definition of V and the hypothesis on S imply that $\Sigma_2(s)$ and $\Sigma_3(s)$ remain bounded as $s \to 1^+$, and so (5.6) will follow once we prove Lemma 5.12 and verify that

$$\lim_{s\to 1^+} \sum_{(p)} \frac{1}{p^s} = +\infty. \tag{5.7}$$

We check (5.7) first. Because the summation range in (5.7) is over all but finitely many primes, we need only show that

$$\lim_{s\to 1^+} \sum_{p} \frac{1}{p^s} = +\infty. \tag{5.8}$$

To see (5.8), recall from the proof of Proposition 5.5 that

$$\lim_{s\to 1^+} (s-1)\zeta(s) = 1,$$

hence

$$\lim_{s\to 1^+} \log \zeta(s) = \lim_{s\to 1^+} \log \frac{1}{s-1} + \lim_{s\to 1^+} \log(s-1)\zeta(s) = +\infty. \tag{5.9}$$

Now let $s > 1$. The mean value theorem implies that

$$|\log(1+x)| \le 2|x| \text{ for } |x| \le \frac{1}{2},$$

and so

$$|\log(1-q^{-s})| \le 2q^{-s}, \text{ for all } q \in P.$$

Because $\sum_q q^{-s} < \sum_{n=1}^{\infty} n^{-s} < \infty$ it follows that the series

$$\sum_q \log(1-q^{-s})$$

is absolutely convergent. Hence

$$\begin{aligned} \log \zeta(s) &= \log\Big(\prod_q \frac{1}{1-q^{-s}}\Big) \text{ (from (5.2))} \\ &= -\sum_q \log(1-q^{-s}) \end{aligned}$$

$$= \sum_q \frac{1}{q^s} + \sum_q \Big(-\log(1-q^{-s}) - \frac{1}{q^s} \Big)$$
$$= \sum_q \frac{1}{q^s} + \sum_q \Big(\sum_{n\geq 2} \frac{1}{nq^{ns}} \Big),$$

where we use the series expansion $\log(1-x) = -\sum_1^\infty x^n/n, |x| < 1$, to obtain the last equation. Then

$$0 < \sum_{n\geq 2} \frac{1}{nq^{ns}} = \frac{1}{q^{2s}} \Big(\sum_{n=0}^{\infty} \frac{1}{(n+2)q^{ns}} \Big)$$
$$\leq \frac{1}{q^{2s}} \sum_{n=0}^{\infty} q^{-ns}$$
$$= \frac{1}{q^{2s}} \frac{1}{1-q^{-s}}$$
$$< \frac{2}{q^2}, \text{ for all } q \geq 2 \text{ and for all } s \geq 1.$$

and so

$$0 < \sum_q \Big(\sum_{n\geq 2} \frac{1}{nq^{ns}} \Big) < 2 \sum_q \frac{1}{q^2} < +\infty \text{ for all } s \geq 1.$$

It follows that

$$\sum_q \frac{1}{q^s} = \log \zeta(s) + H(s), \ H(s) \text{ bounded on } s > 1,$$

hence this equation and (5.9) imply (5.8).

It remains only to prove Lemma 5.12. Let $d \neq 1$ be a square-free integer. Then it is a consequence of the factorization (5.4) of $\zeta_F, F = \mathbb{Q}(\sqrt{d})$ in Proposition 5.11 that

$$\zeta_F(s) = \theta(s)\zeta(s)L(s), \text{ where } L(s) = \prod_p \frac{1}{1-\chi_p(d)p^{-s}}.$$

By virtue of Lemma 5.7,

$$\lim_{s\to 1^+} (s-1)\zeta_F(s) = \lambda > 0,$$

hence

$$\lim_{s\to 1^+} L(s) = \lim_{s\to 1^+} \frac{1}{\theta(s)} \frac{(s-1)\zeta_F(s)}{(s-1)\zeta(s)}$$
$$= \frac{\lambda}{\theta(1)} > 0,$$

and so

$$\lim_{s\to 1^+} \log L(s) \text{ is finite.} \tag{5.10}$$

Now let $s > 1$. Then

$$\log L(s) = -\sum_p \log(1 - \chi_p(d)p^{-s}) \tag{5.11}$$
$$= \sum_p \sum_{n=1}^{\infty} \frac{\chi_p(d)^n}{np^{ns}}$$
$$= \sum_p \chi_p(d)p^{-s} + \sum_p \sum_{n=2}^{\infty} \frac{\chi_p(d)^n}{np^{ns}}.$$

Because

$$\left| \sum_p \sum_{n=2}^{\infty} \frac{\chi_p(d)^n}{np^{ns}} \right| \le \sum_p \sum_{n\ge 2} \frac{1}{np^{ns}},$$

the second term on the right-hand side of the last equation in (5.11) can be estimated as before to verify that it is bounded on $s > 1$. Hence (5.10) and (5.11) imply that

$$\sum_p \chi_p(d)p^{-s} \text{ is bounded as } s \to 1^+. \tag{5.12}$$

The integer d here can be any integer $\neq 1$ that is square-free, but every integer is the product of a square and a square-free integer, hence (5.12) remains valid if d is replaced by any integer which is not a square. QED

The technique used in the proof of Theorem 4.12 can also be used to obtain an interesting generalization of Basic Lemma 4.4 which answers the following question: if S is a nonempty, finite subset of $[1, \infty)$ and $\varepsilon : S \to \{-1, 1\}$ is a given function, when does there exist infinitely many primes p such that $\chi_p \equiv \varepsilon$ on S? There is a natural obstruction to S having this property very similar to the obstruction that prevents the conclusion of Theorem 4.12 from

being true for S. Suppose that there exists a subset $T \neq \emptyset$ of S such that $\prod_{i\in T} i$ is a square. If we choose $i_0 \in T$ and define

$$\varepsilon(i) = \begin{cases} -1, \text{ if } i = i_0, \\ 1, \text{ if } i \in S \setminus \{i_0\}, \end{cases}$$

then $\chi_p \not\equiv \varepsilon$ on S for all sufficiently large p: otherwise there exits a p exceeding all prime factors of the elements of T such that

$$-1 = \prod_{i\in T} \varepsilon(i) = \chi_p\Big(\prod_{i\in T} i\Big) = 1.$$

By tweaking the proof of Theorem 4.12, we will show that this is the only obstruction to S having this property.

Theorem 5.13 *Let S be a nonempty finite subset of $[1,\infty)$. The following statements are equivalent:*

(*i*) *The product of all the elements in each nonempty subset of S is not a square;*
(*ii*) *If $\varepsilon : S \to \{-1,1\}$ is a fixed but arbitrary function, then there exist infinitely many primes p such that $\chi_p \equiv \varepsilon$ on S.*

Proof We have already observed that (*i*) follows from (*ii*), hence suppose that S satisfies (*i*) and let $\varepsilon : S \to \{-1,1\}$ be a fixed function. Consider the sum

$$\Sigma_\varepsilon(s) = \sum_{(p)} \Big(\prod_{i\in S} \big(1 + \varepsilon(i)\chi_p(i)\big)\Big) \cdot \frac{1}{p^s}, \ s > 1.$$

If

$$X_\varepsilon = \{p : \chi_p \equiv \varepsilon \text{ on } S\}$$

then

$$\Sigma_\varepsilon(s) = 2^{|S|} \sum_{p\in X_\varepsilon} \frac{1}{p^s}\ .$$

Also,

$$\Sigma_\varepsilon(s) = \sum_{(p)} \frac{1}{p^s} + \sum_{\emptyset\neq T\subseteq S} \prod_{i\in T} \varepsilon(i) \ \Big(\sum_{(p)} \chi_p\Big(\prod_{i\in T} i\Big) \cdot \frac{1}{p^s}\Big).$$

Lemma 5.12 and the hypotheses on S imply that the second term on the right-hand side of this equation is bounded as $s \to 1^+$, hence from (5.7) we conclude that

$$\lim_{s \to 1^+} \Sigma_\varepsilon(s) = +\infty,$$

and so X_ε is infinite. QED

Definition Any set S satisfying statement (ii) of Theorem 5.13 will be said to *support all patterns*.

Remark The proof of Theorems 4.12 and 5.13 follows exactly the same strategy as Dirichlet's proof of Theorem 4.5. One wants to show that a set X of primes with a certain property is infinite. Hence take $s > 1$, attach a weight of p^{-s} to each prime p in X and then attempt to prove that the weighted sum

$$\sum_{p \in X} \frac{1}{p^s}$$

of the elements of X is unbounded as $s \to 1^+$. In order to achieve this (using ingenious methods!), one writes this weighted sum as $\sum_p 1/p^s$ plus a term that is bounded as $s \to 1^+$. The similarity of all of these arguments is no accident; Theorem 5.13 is in fact also due to Dirichlet, and appeared in his great memoir [11], *Recherches sur diverses applications de l'analyse infinitésimal à la théorie des nombres*, of 1839–40, which together with [10] founded modern analytic number theory. The proof of Theorem 5.13 given here is a variation on Dirichlet's original argument due to Hilbert [28], Sect. 80, Theorem 111.

A straightforward modification of the proof of Theorem 4.9 can now be used to establish

Theorem 5.14 *If S is a nonempty, finite subset of $[1, \infty)$ such that for all subsets T of S of odd cardinality, $\prod_{i \in T} i$ is not a square, $\mathcal{S}$ and $v : 2^S \to F^n$ are defined by S as in the statement of Theorem* 4.9*, and d is the dimension of the linear span of $v(\mathcal{S})$ in F^n, then the density of the set $\{p : \chi_p \equiv -1$ on $S\}$ is 2^{-d}.*

If $p < q < r < s$ are distinct primes and we let, for example, $S_1 = \{p, pq, qr, rs\}$ and $S_2 = \{p, ps, pqr, pqrs\}$, then it follows from Theorem 5.14 and the row reduction of the incidence matrices of S_1 and S_2 that we performed in Sect. 4.6 of Chap. 4 that the density of $\{p : \chi_p \equiv -1$ on $S_1\}$ is 2^{-4} and the density of $\{p : \chi_p \equiv -1$ on $S_2\}$ is 2^{-3}. As we pointed out in Sect. 4.6 of Chap. 4, a 2-dimensional subspace of F^4 contains only 3 nonzero vectors, and so if S is a set of 4 nontrivial square-free integers such that S

is supported on 4 primes then the density of $\{p : \chi_p \equiv -1 \text{ on } S\}$ cannot be 2^{-2}. But it is also true that all of the vectors in a 2-dimensional subspace of F^4 must sum to 0 and so if S is a set of 3 nontrivial square-free integers such that S is supported on 4 primes then $\{p : \chi_p \equiv -1 \text{ on } S\}$ is in fact empty. In order to get a set S from p, q, r, and s such that the density of $\{p : \chi_p \equiv -1 \text{ on } S\}$ is 2^{-2}, S has to have 2 elements, and it follows easily from Theorem 5.14 that $S = \{pq, qrs\}$ is one of many examples for which the density of $\{p : \chi_p \equiv -1 \text{ on } S\}$ is 2^{-2}.

A straightforward modification of the proof of Lemma 4.10 can also be used to establish

Theorem 5.15 (*Filaseta and Richman* [18], *Theorem* 2) *If S is a nonempty, finite subset of $[1, \infty)$ such that the product of all the elements in each nonempty subset of S is not a square and $\varepsilon : S \to \{-1, 1\}$ is a fixed but arbitrary function, then the density of the set $\{p : \chi_p \equiv \varepsilon \text{ on } S\}$ is $2^{-|S|}$.*

5.5 Proof of the Fundamental Theorem of Ideal Theory

Because the Fundamental Theorem of Ideal Theory was used at its full strength in the proof of the Euler-Dedekind product expansion of the zeta function (Theorem 5.8), and also because of the important role that it played (although not at full strength) in the results on the factorization of ideals in a quadratic number field from Chap. 3, we will present a proof of it in this final section of Chap. 5. Our account follows the outline given by Ore in [43].

Let F be an algebraic number field of degree n and let R be the ring of algebraic integers in F. We want to prove that every nonzero proper ideal of R is a product of a finite number of prime ideals and also that this factorization is unique up to the order of the prime-ideal factors. The strategy of our argument is to prove first that each nonzero proper ideal of R *contains* a finite product of prime ideals. We hence chose for each nonzero proper ideal I a product of prime ideals with the smallest number of factors that is contained in I, and then by use of appropriate mathematical technology that we will develop, proceed by induction on this smallest number of prime-ideal factors to prove that I is in fact *equal* to a product of prime ideals. Uniqueness will then follow by further use of the mathematical technology that we will have at our disposal. We proceed to implement this strategy.

Let I be an ideal of R, $\{0\} \neq I \neq R$.

Lemma 5.16 *There exists a sequence of prime ideals $P_1, \ldots, P_s$ of R such that $I \subseteq P_i$, for all i and $P_1 \cdots P_s \subseteq I$.*

Proof If I is prime then we are done, with $s = 1$, hence suppose that I is not prime. Then there exists a product $\beta\gamma$ of elements of R which is in I and $\beta \notin I,\ \gamma \notin I$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis of I, and set

$$J = (\alpha_1, \ldots, \alpha_n, \beta),\ K = (\alpha_1, \ldots, \alpha_n, \gamma).$$

Then

$$JK \subseteq I,\ I \subsetneqq J,\ I \subsetneqq K.$$

If J, K are both prime then we are done, with $s = 2$. Otherwise apply this procedure to each nonprime ideal that occurs, and continue in this way as long as the procedure produces nonprime ideals. Note that after each step of the procedure,

(i) the product of all the ideals obtained in that step is contained in I,
(ii) I is contained in each ideal obtained in that step, and
(iii) each ideal obtained in that step is properly contained in an ideal from the immediately preceding step.

Claim: this procedure terminates after finitely many steps.

If this is true then each ideal obtained in the final step is prime; otherwise the procedure would continue by applying it to a nonprime ideal. If $P_1, \ldots, P_s$ are the prime ideals obtained in the final step then this sequence of ideals satisfies Lemma 5.16 by virtue of (i) and (ii) above.

Proof of the claim Suppose this is false. Then (ii) and (iii) above imply that the procedure produces an infinite sequence of ideals $J_0, J_1, \ldots, J_n, \ldots$ such that $J_0 = I$ and $J_i \subsetneqq J_{i+1}$, for all i. We will now prove that I is contained in only finitely many ideals, hence no such sequence of ideals is possible.

The proof of Proposition 5.1(i) implies that I contains a positive rational integer a. We show that a belongs to only finitely many ideals.

Suppose that J is an ideal, with integral basis $\{\beta_1, \ldots, \beta_n\}$, and $a \in J$. Then we also have that

$$J = (\beta_1, \ldots, \beta_n, a).$$

By the claim in the proof of Proposition 5.1(i), for each i, there is $\gamma_i, \delta_i \in R$ such that $\beta_i = a\gamma_i + \delta_i$, and δ_i can take on only at most an values. But then

$$J = (a\gamma_1 + \delta_1, \ldots, a\gamma_n + \delta_s) = (\delta_1, \ldots, \delta_n, a).$$

Because each δ_i assumes at most an values, it follows that J is one of only at most an^2 ideals. QED

The statement of the next lemma requires the following definition:

Definition If J is an ideal of R then

$$J^{-1} = \{\alpha \in F : \alpha\beta \in R, \quad \text{for all } \beta \in J\}.$$

Lemma 5.17 *If P is a prime ideal of R then P^{-1} contains an element of $F \setminus R$.*

Proof Let $x \in P$. Lemma 5.16 implies that (x) contains a product $P_1 \cdots P_s$ of prime ideals. Choose a product with the smallest number s of factors.

Suppose that $s = 1$. Then $P_1 \subseteq (x) \subseteq P$. P_1 maximal (Proposition 5.1(i)) implies that $P = P_1 = (x)$. Hence $1/x \in P^{-1}$. Also, $1/x \notin R$; otherwise, $1 = x \cdot 1/x \in P$, contrary to the fact that P is proper.

Suppose that $s > 1$. Then $P_1 \cdots P_s \subseteq (x) \subseteq P$, and so the fact that P is prime implies that P contains a P_i, say P_1. P_1 maximal implies that $P = P_1$. $P_2 \cdots P_s \nsubseteq (x)$ by minimality of s, hence there exits $\alpha \in P_2 \cdots P_s$ such that $\alpha \notin (x)$, and so $\alpha/x \notin R$.

Claim: $\alpha/x \in P^{-1}$.

Let $\beta \in P$. We must prove that $\beta(\alpha/x) \in R$. To do that, observe that

$$(\alpha)P \subseteq P_2 \cdots P_s P = P_1 \cdots P_s \subseteq (x),$$

and so there is a $\gamma \in R$ such that $\alpha\beta = x\gamma$, i.e., $\beta(\alpha/x) = \gamma$. QED

The next lemma is the key technical tool that allows us to prove the Fundamental Theorem of Ideal Theory; it will be used to factor an ideal into a product of prime ideals and to show that this factorization is unique up to the order of the factors. In order to state it, we need to extend the definition of products of ideals to products of arbitrary subsets of R like so:

Definition If S and T are subsets of R then the *product ST of S and T* is the set consisting of all sums of the form $\sum_i s_i t_i$, where $(s_i, t_i) \in S \times T$ for all i.

This product is clearly commutative and associative, and it agrees with the product defined before when S and T are ideals of R.

Lemma 5.18 *If P is a prime ideal of R and I is an ideal of R then $P^{-1}PI = I$.*

Proof It suffices to show that $P^{-1}P = (1)$. It is straightforward to show that $J = P^{-1}P$ is an ideal of R. As $1 \in P^{-1}$, it follows that $P \subseteq J$ and so P maximal implies that $P = J$ or $J = (1)$.

Suppose that $J = P$. Let $\{\alpha_1, \ldots, \alpha_n\}$ be an integral basis of P, and use Lemma 5.17 to find $\gamma \in P^{-1}$, $\gamma \notin R$. Then $\gamma\alpha_i \in P$, for all i, and so

$$\gamma\alpha_i = \sum_j a_{ij}\alpha_j, \text{ where } a_{ij} \in \mathbb{Z} \text{ for all } i, j.$$

As a consequence of these equations, γ is an eigenvalue of the matrix $[a_{ij}]$, hence it is a root of the characteristic polynomial of $[a_{ij}]$, and this characteristic polynomial is a monic polynomial in $\mathbb{Z}[x]$. As we showed in the proof of Theorem 3.11, this implies that γ is an algebraic integer, contrary to its choice. Hence $P \neq J$, and so $J = (1)$. QED

The Fundamental Theorem of Ideal Theory is now a consequence of the next two lemmas.

Lemma 5.19 *Every nonzero proper ideal of R is a product of prime ideals.*

Proof Lemma 5.16 implies that every nonzero proper ideal of R contains a product $P_1 \cdots P_r$ of prime ideals, where we choose a product with the smallest number r of factors. The argument now proceeds by induction on r.

Let $\{0\} \neq I \neq R$ be an ideal with $r = 1$, i.e., I contains a prime ideal P. P maximal implies that $I = P$, and we are done.

Assume now that $r > 1$ and every nonzero, proper ideal that contains a product of fewer than r prime ideals is a product of prime ideals.

Let $\{0\} \neq I \neq R$ be an ideal that contains a product $P_1 \cdots P_r$ of prime ideals, with r the smallest number of prime ideals with this property. Lemma 5.16 implies that I is contained in a prime ideal Q. Hence $P_1 \cdots P_r \subseteq Q$, and so Q contains a P_i, say P_1. P_1 maximal implies that $Q = P_1$. Hence $I \subseteq P_1$. Then IP_1^{-1} is an ideal of R; $I \subseteq IP_1^{-1}$ $(1 \in P^{-1})$, and so $IP_1^{-1} \neq \{0\}$. $IP_1^{-1} \neq R$; otherwise, $P_1 \subseteq I$, hence $I = P_1$, contrary to the fact that $r > 1$. Lemma 5.18 implies that

$$P_2 \cdots P_r = P_1^{-1}P_1 \cdots P_r \subseteq IP_1^{-1},$$

hence by the induction hypothesis, IP_1^{-1} is a product $P_1' \cdots P_k'$ of prime ideals, and so by Lemma 5.18 again,

$$I = (IP_1^{-1})P_1 = P_1' \cdots P_k'P_1$$

is a product of prime ideals. QED

Lemma 5.20 *Factorization as a product of prime ideals is unique up to the order of the factors.*

Proof Suppose that $P_1 \cdots P_r = Q_1 \cdots Q_s$ are products of prime ideals, with $r \leq s$, say. $Q_1 \cdots Q_s \subseteq Q_1$, hence $P_1 \cdots P_r \subseteq Q_1$ and so the fact that Q_1 is a prime ideal and the maximality of the P_i's imply, after reindexing one of the

P_i's, that $Q_1 = P_1$. Then Lemma 5.18 implies that

$$P_2 \cdots P_r = P_1^{-1} P_1 \cdots P_r = Q_1^{-1} Q_1 \cdots Q_s = Q_2 \cdots Q_s.$$

Continuing in this way, we deduce, upon reindexing of the P_i's, that $P_i = Q_i$, $i = 1, \ldots r$, and also, if $r < s$, that

$$(1) = Q_{r+1} \cdots Q_s.$$

But this equation implies that $R = (1) \subseteq Q_{r+1}$, which is impossible as Q_{r+1} is a proper ideal. Hence $r = s$. QED

Dedekind's own proof of The Fundamental Theorem of Ideal Theory in [8], Chap. 4, Sect. 25, is a model of clarity and insight which amply repays careful study. We strongly encourage the reader to take a look at it.