CHAPTER 3

Ideal Theory

3.1. Introduction

Let us examine the ring of integers in the algebraic number field $\mathbb{Q}(\sqrt{15})$. This is simply $\mathbb{Z}[\sqrt{15}]$ by Theorem 2.24. Consider, in particular, the two factorizations of the algebraic integer 10 into products of primes, given by

$$10 = 2 \cdot 5 = (5 + \sqrt{15})(5 - \sqrt{15}).$$

Clearly we do not have uniqueness of factorization into products of primes in this algebraic number field.

The numbers $\sqrt{5}$ and $\sqrt{3}$ are not in the algebraic number field $\mathbb{Q}(\sqrt{15})$, but let us introduce these numbers into the argument nevertheless. Then

$$5 + \sqrt{15} = \sqrt{5}(\sqrt{5} + \sqrt{3}) \quad \text{and} \quad 5 - \sqrt{15} = \sqrt{5}(\sqrt{5} - \sqrt{3}),$$

and note that

$$2 = (\sqrt{5} + \sqrt{3})(\sqrt{5} - \sqrt{3}).$$

Hence the two factorizations of the algebraic integer 10 are obtained by grouping the terms in the "factorization"

$$10 = \sqrt{5}\sqrt{5}(\sqrt{5} + \sqrt{3})(\sqrt{5} - \sqrt{3})$$

in two different ways. It therefore appears that in the algebraic number field $\mathbb{Q}(\sqrt{15})$, the primes are not necessarily the "building blocks". It seems necessary to enlarge the field $\mathbb{Q}(\sqrt{15})$ to perhaps $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ in order to include "ideal numbers" such as $\sqrt{5} \pm \sqrt{3}$.

Our hope is then the following: Suppose that there is no uniqueness of factorization of algebraic integers into products of primes in an algebraic number field K. Is it then possible to extend K to an algebraic number field L such that the algebraic integers in K factorize in some unique way into products of algebraic integers in L? But then how do we attempt to find such an algebraic number field L, if it exists? Or, returning to our example, what numbers should we add to $\mathbb{Q}(\sqrt{15})$?

Let K be a given algebraic number field. Suppose that ξ is a "common factor" to two relatively prime algebraic integers in K. Let $\mathfrak{a}$ denote the set of all algebraic integers in K that are "divisible" by ξ. If $\alpha, \beta \in \mathfrak{a}$, then clearly $\lambda\alpha + \mu\beta \in \mathfrak{a}$ for all algebraic integers λ and μ in K. But this is precisely the definition of an ideal in the ring of integers $\mathfrak{O}$ of the algebraic number field K.

Let us consider an ideal $\mathfrak{a}$ in an algebraic number field K. Suppose that we can find an algebraic integer ξ, not necessarily in K, such that $\mathfrak{a}$ is the set of all algebraic integers in K which are "divisible" by ξ, and that ξ is in some sense unique, then we have characterized the missing algebraic integers in K by means of ideals. In this case, the problem of factorization of algebraic integers then becomes the problem of factorization of ideals. Our aim is to show that there is a satisfactory solution to the latter. This is known as Kummer theory.

REMARKS. (i) The origin of Kummer theory goes back to the famous Fermat's last theorem, that for all natural numbers $n > 2$, the diophantine equation

$$x^n + y^n = z^n$$

has no solutions in non-zero integers x, y and z.

(ii) The problem can be simplified somewhat. First of all, we may restrict the solutions to pairwise coprime non-zero integers x, y and z. Secondly, it clearly suffices to study the problem when the exponent n is equal to 4 or is an odd prime.

(iii) When $n = 2$, the solutions of the equation $x^2 + y^2 = z^2$ with pairwise coprime integers x, y and z are given parametrically by

$$\pm x = r^2 - s^2, \quad \pm y = 2rs, \quad \pm z = r^2 + s^2,$$

or with x and y interchanged, where r and s are coprime integers and exactly one of them is odd. Clearly it is sufficient to consider positive x, y and z, and not all three of them can be odd. Since they are pairwise coprime, exactly one of them is even. This cannot be z, for otherwise

$$2 \equiv x^2 + y^2 = z^2 \equiv 0 \bmod 4.$$

We may therefore assume that y is even, and that x and z are odd. In this case,

$$y^2 = z^2 - x^2 = (z + x)(z - x), \tag{3.1}$$

where y, $z - x$ and $z + x$ are all even and positive. Writing $y = 2u$, $z + x = 2v$ and $z - x = 2w$, we then have $u^2 = vw$. It is not difficult to see that v and w are coprime, so factorizing u, v and w into prime factors, it is easily seen that both v and w are squares. Let $v = r^2$ and $w = s^2$. Then r and s are coprime, and

$$z = v + w = r^2 + s^2, \quad x = v - w = r^2 - s^2.$$

Furthermore, since both x and z are odd, precisely one of r and s is odd. Finally, it follows from (3.1) that $y^2 = (r^2 + s^2)^2 - (r^2 - s^2)^2 = 4r^2s^2$, so that $y = 2rs$.

(iv) The case $n = 4$ of the problem can now be handled relatively easily by showing that the equation

$$x^4 + y^4 = z^2$$

has no solutions in non-zero integers x, y and z. Suppose on the contrary that such a solution exists. We may assume that x, y and z are all positive, and that z is minimal among all such solutions. Then x, y and z are coprime. In view of (iii) above, there exist coprime r and s, precisely one of which is even and such that

$$x^2 = r^2 - s^2, \quad y^2 = 2rs, \quad z = r^2 + s^2.$$

Furthermore, x and z are odd and y is even. Clearly

$$x^2 + s^2 = r^2,$$

where x and s are coprime. In view of (iii) above, there exist coprime a and b, precisely one of which is even and such that

$$x = a^2 - b^2, \quad s = 2ab, \quad r = a^2 + b^2.$$

Substitution gives $y^2 = 4ab(a^2 + b^2)$. On writing $y = 2k$, we have

$$k^2 = ab(a^2 + b^2).$$

It is not difficult to see that a, b and $a^2 + b^2$ are pairwise coprime. Hence there exist u, v and w such that $a = u^2$, $b = v^2$ and $a^2 + b^2 = w^2$, so that

$$u^4 + v^4 = w^2.$$

Now $w \leqslant a^2 + b^2 = r < z$, contradicting the minimality of z.

(v) Summarizing the above, it now follows that Fermat's last theorem is reduced to showing that the diophantine equation

$$x^p + y^p = z^p \tag{3.2}$$

for any fixed odd prime p has no solutions in pairwise coprime non-zero integers x, y and z. Suppose on the contrary that such a solution to the equation (3.2) exists. Writing $\zeta = \mathrm{e}^{2\pi \mathrm{i}/p}$ for a primitive p-th root of unity, we obtain

$$(x+y)(x+\zeta y)\dots(x+\zeta^{p-1}y) = z^n, \tag{3.3}$$

and factorization takes place in the cyclotomic number field $\mathbb{Q}(\zeta)$. If x and y are coprime, then the factors on the left hand side of (3.3) have no common factors, and so "must" each be a p-th power. However, this last step assumes uniqueness of factorization in a subtle way!

(vi) In Chapter 5, we establish a special case of Fermat's last theorem due to Kummer – for primes p which are "regular".

(vii) The proof of Fermat's last theorem in 1994 is due to Wiles with assistence from Taylor.

3.2. Ideals in an Algebraic Number Field

Let K be an algebraic number field, with ring of integers $\mathfrak{O}$. A subset $\mathfrak{a}$ of $\mathfrak{O}$ is an ideal in K if the following condition is satisfied: If $\alpha, \beta \in \mathfrak{a}$, then $\lambda\alpha + \mu\beta \in \mathfrak{a}$ for every $\lambda, \mu \in \mathfrak{O}$.

We denote by $\langle 0 \rangle = \{0\}$ the zero ideal.

The following result can be considered a generalization of Theorem 2.22.

THEOREM 3.1. *Suppose that K is an algebraic number field of degree n, with ring of integers $\mathfrak{O}$. Then every non-zero ideal $\mathfrak{a}$ in K has a $\mathbb{Z}$-basis $\{\alpha_1, \dots, \alpha_n\}$.*

PROOF. We first of all show that if $\mathfrak{a}$ has a $\mathbb{Z}$-basis $\{\alpha_1, \dots, \alpha_r\}$, then we must have $r = n$. Clearly $r \leqslant n$. On the other hand, let $\{\beta_1, \dots, \beta_n\}$ be an integral basis for $\mathfrak{O}$. If $\alpha \in \mathfrak{a}$ is non-zero, then $\alpha\beta_1, \dots, \alpha\beta_n \in \mathfrak{a}$ and are linearly independent over $\mathbb{Q}$, and hence also over $\mathbb{Z}$. It follows that we must have $r = n$. It remains to prove that $\mathfrak{a}$ has a $\mathbb{Z}$-basis. To do this, we imitate the proof of Theorem 2.22. Let $\mathcal{L}$ be the set of all bases of K whose elements are all in $\mathfrak{a}$. Then $\mathcal{L} \neq \emptyset$, for $\{\alpha\beta_1, \dots, \alpha\beta_n\} \in \mathcal{L}$. By Theorem 2.21, $\Delta[\alpha_1, \dots, \alpha_n] \in \mathbb{Z} \setminus \{0\}$ for every element $\{\alpha_1, \dots, \alpha_n\} \in \mathcal{L}$, and so there exists $\{\alpha_1, \dots, \alpha_n\} \in \mathcal{L}$ for which $|\Delta[\alpha_1, \dots, \alpha_n]|$ is minimal. This is a $\mathbb{Z}$-basis for $\mathfrak{a}$ by similar arguments as in the proof of Theorem 2.22, and noting that $b_1\alpha_1 + \ldots + b_n\alpha_n \in \mathfrak{a}$ for every $b_1, \dots, b_n \in \mathbb{Z}$. ◯

Before we study some basic properties of ideals, we need to make a few definitions. Throughout, K denotes an algebraic number field, with ring of integers $\mathfrak{O}$.

An ideal $\mathfrak{a}$ in K is said to be generated by $\alpha_1, \dots, \alpha_s$, denoted by $\mathfrak{a} = \langle \alpha_1, \dots, \alpha_s \rangle$, if $\mathfrak{a}$ consists of all sums of the form $\lambda_1\alpha_1 + \ldots + \lambda_s\alpha_s$, where $\lambda_1, \dots, \lambda_s \in \mathfrak{O}$.

Clearly, if $\{\alpha_1, \dots, \alpha_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$, then $\mathfrak{a} = \langle \alpha_1, \dots, \alpha_n \rangle$.

An ideal $\mathfrak{a}$ in K is said to be principal if $\mathfrak{a}$ is generated by a single element; in other words, if $\mathfrak{a} = \{\alpha\}$ for some $\alpha \in \mathfrak{O}$.

Let $\mathfrak{a} = \langle \alpha_1, \dots, \alpha_s \rangle$ and $\mathfrak{b} = \langle \beta_1, \dots, \beta_t \rangle$ be ideals in K. By the product $\mathfrak{ab}$, we mean the ideal $\langle \alpha_1\beta_1, \dots, \alpha_i\beta_j, \dots, \alpha_s\beta_t \rangle$.

Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in K. Then we say that $\mathfrak{a}$ divides $\mathfrak{b}$, denoted by $\mathfrak{a} \mid \mathfrak{b}$, if there exists an ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{ac}$. In this case, we also say that $\mathfrak{a}$ is a factor of $\mathfrak{b}$.

THEOREM 3.2. *Suppose that K is an algebraic number field. Then the following statements hold:*

(i) *If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in K satisfying $\mathfrak{a} \mid \mathfrak{b}$, then $\mathfrak{b} \subseteq \mathfrak{a}$.*
(ii) *A non-zero rational integer belongs to at most a finite number of ideals in K.*
(iii) *Every non-zero ideal in K contains a non-zero rational integer.*
(iv) *A non-zero ideal in K has only a finite number of divisors.*

PROOF. (i) If $\mathfrak{a} \mid \mathfrak{b}$, then $\mathfrak{b} = \mathfrak{ac}$ for some ideal $\mathfrak{c}$ in K. Let $\mathfrak{a} = \langle \alpha_1, \dots, \alpha_s \rangle$ and $\mathfrak{c} = \langle \gamma_1, \dots, \gamma_t \rangle$. Then every $\beta \in \mathfrak{b}$ is of the form

$$\beta = \sum_{i=1}^{s}\sum_{j=1}^{t} \lambda_{ij}\alpha_i\gamma_j = \sum_{i=1}^{s}\left(\sum_{j=1}^{t}\lambda_{ij}\gamma_j\right)\alpha_i,$$

where $\lambda_{ij} \in \mathfrak{O}$ for every $i = 1, \dots, s$ and $j = 1, \dots, t$. Hence $\beta \in \mathfrak{a}$, since clearly

$$\sum_{j=1}^{t}\lambda_{ij}\gamma_j \in \mathfrak{O}, \quad i = 1, \dots, s.$$

(ii) Suppose that a is a non-zero rational integer which belongs to an ideal $\mathfrak{a}$. We may assume, without loss of generality, that $a > 0$. Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis for $\mathfrak{O}$. Then every $\alpha \in \mathfrak{O}$ can be written in the form $\alpha = c_1\omega_1 + \ldots + c_n\omega_n$, where $c_1, \ldots, c_n \in \mathbb{Z}$. For every $i = 1, \ldots, n$, we can write $c_i = aq_i + r_i$, where $q_i, r_i \in \mathbb{Z}$ and $0 \leqslant r_i < a$. Then

$$\alpha = (aq_1 + r_1)\omega_1 + \ldots + (aq_n + r_n)\omega_n = a(q_1\omega_1 + \ldots + q_n\omega_n) + (r_1\omega_1 + \ldots + r_n\omega_n).$$

Clearly $\gamma = q_1\omega_1 + \ldots + q_n\omega_n \in \mathfrak{O}$ and $\beta = r_1\omega_1 + \ldots + r_n\omega_n \in \mathcal{B}$, where $\mathcal{B}$ is a finite set. Suppose now that $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_s \rangle$. Since $a \in \mathfrak{a}$, we can write

$$\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_s, a \rangle.$$

Using the above observation, we can write

$$\mathfrak{a} = \langle a\gamma_1 + \beta_1, \ldots, a\gamma_s + \beta_s, a \rangle,$$

where $\gamma_1, \ldots, \gamma_s \in \mathfrak{O}$ and $\beta_1, \ldots, \beta_s \in \mathcal{B}$. Clearly $\mathfrak{a} = \langle \beta_1, \ldots, \beta_s, a \rangle$, and so the conclusion follows.

(iii) Let $\alpha \in \mathfrak{a}$ be non-zero, and let $\alpha^{(1)}, \ldots, \alpha^{(n)}$ be the K-conjugates of α, with the convention that $\alpha = \alpha^{(1)}$. Then $\alpha^{(2)} \ldots \alpha^{(n)}$ is an algebraic integer and

$$\alpha^{(2)} \ldots \alpha^{(n)} = \frac{N(\alpha)}{\alpha} \in K.$$

Hence $\alpha^{(2)} \ldots \alpha^{(n)} \in \mathfrak{O}$. It now follows that $N(\alpha) = \alpha\alpha^{(2)} \ldots \alpha^{(n)} \in \mathfrak{a}$.

(iv) Let $\alpha \in \mathfrak{a}$ be non-zero. By part (iii), $N(\alpha) \in \mathfrak{a}$. It follows from part (i) that $N(\alpha)$ belongs to any divisor of $\mathfrak{a}$. The conclusion now follows from part (ii). ◯

To establish a theory of factorization, we make the following two definitions.

An ideal $\mathfrak{a}$ in K is said to be maximal if $\mathfrak{a} \neq \mathfrak{O}$ and satisfies the following condition: If $\mathfrak{b}$ is an ideal in K satisfying $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathfrak{O}$, then $\mathfrak{b} = \mathfrak{a}$ or $\mathfrak{b} = \mathfrak{O}$; in other words, there are no ideals in K strictly between $\mathfrak{a}$ and $\mathfrak{O}$.

An ideal $\mathfrak{a}$ in K is said to be prime if $\mathfrak{a} \neq \mathfrak{O}$ and satisfies the following condition: If $\mathfrak{b}$ and $\mathfrak{c}$ are ideals in K satisfying $\mathfrak{bc} \subseteq \mathfrak{a}$, then $\mathfrak{b} \subseteq \mathfrak{a}$ or $\mathfrak{c} \subseteq \mathfrak{a}$.

THEOREM 3.3. *Every maximal ideal in an algebraic number field K is prime.*

PROOF. Suppose that $\mathfrak{a}$ is maximal, and that $\mathfrak{b}$ and $\mathfrak{c}$ are ideals in K satisfying $\mathfrak{bc} \subseteq \mathfrak{a}$. Suppose further that $\mathfrak{b} \not\subseteq \mathfrak{a}$. We need to show that $\mathfrak{c} \subseteq \mathfrak{a}$. Since $\mathfrak{b} \not\subseteq \mathfrak{a}$, there exists $\beta \in \mathfrak{b}$ such that $\beta \notin \mathfrak{a}$. Let $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_s \rangle$. Then $\mathfrak{a} \subsetneqq \langle \alpha_1, \ldots, \alpha_s, \beta \rangle \subseteq \mathfrak{O}$. Since $\mathfrak{a}$ is maximal, it follows that $\langle \alpha_1, \ldots, \alpha_s, \beta \rangle = \mathfrak{O}$, and so there exist $\lambda_1, \ldots, \lambda_s, \mu \in \mathfrak{O}$ such that

$$1 = \lambda_1\alpha_1 + \ldots + \lambda_s\alpha_s + \mu\beta.$$

Hence for every $\gamma \in \mathfrak{c}$, we have

$$\gamma = \gamma 1 = (\gamma\lambda_1)\alpha_1 + \ldots + (\gamma\lambda_s)\alpha_s + \mu(\beta\gamma).$$

Since $\gamma\lambda_1, \ldots, \gamma\lambda_s, \mu \in \mathfrak{O}$ and $\alpha_1, \ldots, \alpha_s, \beta\gamma \in \mathfrak{a}$, it follows that $\gamma \in \mathfrak{a}$. ◯

Our aim in the next two sections is to give two proofs of the following important result.

THEOREM 3.4 (Unique factorization theorem). *Suppose that K is an algebraic number field, with ring of integers $\mathfrak{O}$. Suppose further that $\mathfrak{a}$ is an ideal in K such that $\mathfrak{a} \neq \langle 0 \rangle$ and $\mathfrak{a} \neq \mathfrak{O}$. Then $\mathfrak{a}$ can be written as a product of prime ideals in K, uniquely up to the order of factors.*

In Section 3.3, we give a classical proof based on the ideas of Hurwitz. In Section 3.4, we then give a modern proof based on the ideas of Noether. We emphasize that Section 3.4 does not depend on any result in Section 3.3 not established also within Section 3.4.

3.3. The Classical Proof of the Unique Factorization Theorem

The crucial step in the classical proof of the Unique factorization theorem is summarized by the following result.

THEOREM 3.5. *Suppose that K is an algebraic number field. Then for any non-zero ideal $\mathfrak{a}$ in K, there exists a non-zero ideal $\mathfrak{b}$ in K such that $\mathfrak{ab} = \langle a \rangle$ for some $a \in \mathbb{Z}$.*

An immediate consequence is the following result.

THEOREM 3.6. *Suppose that $\mathfrak{a}$, $\mathfrak{b}$ and $\mathfrak{c}$ are ideals in an algebraic number field K. Then the following statements hold:*

(i) *If $\mathfrak{ab} = \mathfrak{ac}$ and $\mathfrak{a} \neq \langle 0 \rangle$, then $\mathfrak{b} = \mathfrak{c}$.*
(ii) *If $\mathfrak{b} \subseteq \mathfrak{a}$, then $\mathfrak{a} \mid \mathfrak{b}$.*

PROOF. By Theorem 3.5, there exists an ideal $\mathfrak{d}$ in K such that $\mathfrak{ad} = \langle a \rangle$ for some $a \in \mathbb{Z}$.

(i) We have $\mathfrak{abd} = \mathfrak{acd}$, so that $\langle a \rangle \mathfrak{b} = \langle a \rangle \mathfrak{c}$. The conclusion follows easily.

(ii) Since $\mathfrak{b} \subseteq \mathfrak{a}$, we have $\mathfrak{bd} \subseteq \mathfrak{ad}$. Let $\mathfrak{bd} = \langle \beta_1, \ldots, \beta_m \rangle$. Then for every $i = 1, \ldots, m$, we have $\beta_i \in \mathfrak{ad} = \langle a \rangle$, and so $\beta_i = \lambda_i a$ for some $\lambda_i \in \mathfrak{O}$. It follows that $\mathfrak{bd} = \langle a \rangle \langle \lambda_1, \ldots, \lambda_m \rangle = \mathfrak{ad} \langle \lambda_1, \ldots, \lambda_m \rangle$, and so $\mathfrak{b} = \mathfrak{a} \langle \lambda_1, \ldots, \lambda_m \rangle$, in view of part (i). ◯

We postpone the proof of Theorem 3.5 to the latter part of this section. To deduce Theorem 3.4, we also need the following result.

THEOREM 3.7. *Suppose that K is an algebraic number field. Then every ideal $\mathfrak{a}$ in K such that $\mathfrak{a} \neq \mathfrak{O}$ is contained in a maximal ideal in K.*

PROOF. We assume that $\mathfrak{a}$ is non-zero. Then it follows from Theorem 3.2(iv) that $\mathfrak{a}$ has only a finite number of divisors. Clearly any divisor $\mathfrak{b}$ of $\mathfrak{a}$ which is different from $\mathfrak{O}$ has fewer divisors than $\mathfrak{a}$. Among the divisors of $\mathfrak{a}$ which are different from $\mathfrak{O}$, let $\mathfrak{p}$ be one with the smallest number of divisors. We now claim that $\mathfrak{p}$ is maximal in K. Suppose not. Then there exists an ideal $\mathfrak{q}$ in K such that $\mathfrak{p} \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{O}$. It then follows from Theorem 3.6(ii) that $\mathfrak{q} \mid \mathfrak{p}$, and so must have fewer divisors than $\mathfrak{p}$. ◯

PROOF OF THEOREM 3.4. Let $\mathfrak{a}$ be an ideal in K such that $\mathfrak{a} \neq \langle 0 \rangle$ and $\mathfrak{a} \neq \mathfrak{O}$.

We first of all exhibit a factorization of $\mathfrak{a}$ into a product of maximal ideals. This is trivial if $\mathfrak{a}$ is maximal. If $\mathfrak{a}$ is not maximal, then it follows from Theorem 3.7 that $\mathfrak{a} \subseteq \mathfrak{p}_1$ for some maximal ideal $\mathfrak{p}_1$ in K. It then follows from Theorem 3.6(ii) that $\mathfrak{p}_1 \mid \mathfrak{a}$, so that $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{a}_1$ for some ideal $\mathfrak{a}_1$ in K. If $\mathfrak{a}_1$ is maximal, then we stop; otherwise we repeat the process with $\mathfrak{a}$ replaced by $\mathfrak{a}_1$, so that $\mathfrak{a}_1 = \mathfrak{p}_2 \mathfrak{a}_2$, where $\mathfrak{p}_2$ and $\mathfrak{a}_2$ are ideals in K and $\mathfrak{p}_2$ is maximal. If $\mathfrak{a}_2$ is maximal, then we stop; otherwise we repeat the process again, and so on. This process must stop, in view of Theorem 3.2(iv) and the observation that $\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \ldots$. We can therefore conclude that $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_r$, a product of maximal ideals in K. Furthermore, the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are prime, in view of Theorem 3.3.

To prove uniqueness of factorization, suppose that

$$\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_r = \mathfrak{q}_1 \ldots \mathfrak{q}_s,$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are maximal, and hence prime, ideals in K and where $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are prime ideals in K. Clearly $\mathfrak{q}_1 \mid \mathfrak{p}_1 \ldots \mathfrak{p}_r$. It therefore follows from Theorem 3.2(i) that $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{q}_1$. Since $\mathfrak{q}_1$ is prime, there exists some $j = 1, \ldots, r$ such that $\mathfrak{p}_j \subseteq \mathfrak{q}_1$. Renumbering $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ if necessary, we may assume that $\mathfrak{p}_1 \subseteq \mathfrak{q}_1$. Since $\mathfrak{p}_1$ is maximal and $\mathfrak{q}_1$ is prime, we must then have $\mathfrak{p}_1 = \mathfrak{q}_1$. It then follows from Theorem 3.6(i) that $\mathfrak{p}_2 \ldots \mathfrak{p}_r = \mathfrak{q}_2 \ldots \mathfrak{q}_s$. Repeating this argument, we clearly have $r = s$ and uniqueness of factorization. ◯

REMARK. Note that in the proof of Theorem 3.4, we have not used the fact that the ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are maximal, only that they are prime. However, we have used the fact that the ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are maximal. This is clearly possible, since we have first established that the ideal $\mathfrak{a}$ has a factorization into a product of maximal ideals. What we have not studied so far is whether a prime ideal is also maximal. In fact, we can deduce this fact from the proof of Theorem 3.4. Note that if $\mathfrak{p}$ is a prime ideal in K, then $\mathfrak{p} = \mathfrak{p}_1 \ldots \mathfrak{p}_r$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are maximal, and hence prime, ideals in K. Uniqueness of factorization then gives $r = 1$ and $\mathfrak{p} = \mathfrak{p}_1$ is maximal.

Our proof of Theorem 3.5 is based on the following generalization of Gauss's lemma given in Theorem 1.6.

THEOREM 3.8. *Suppose that $p(t) = \alpha_p t^p + \ldots + \alpha_0$ and $q(t) = \beta_q t^q + \ldots + \beta_0$ are polynomials such that $\alpha_p \beta_q \neq 0$ and all coefficients are algebraic integers, and that $r(t) = p(t)q(t) = \gamma_r t^r + \ldots + \gamma_0$. If δ is an algebraic integer such that γ_k/δ is an algebraic integer for every $k = 0, \ldots, r$, then $\alpha_i \beta_j / \delta$ is also an algebraic integer for every $i = 0, \ldots, p$ and $j = 0, \ldots, q$.*

To establish this generalization, we need the following intermediate result.

THEOREM 3.9. *Suppose that $f(t) = \delta_m t^m + \ldots + \delta_0$ is a polynomial such that $\delta_m \neq 0$ and all coefficients are algebraic integers.*

(i) *If $f(\rho) = 0$, then every coefficient of the polynomial $f(t)/(t-\rho)$ is an algebraic integer.*
(ii) *If $f(t) = \delta_m(t-\rho_1)\ldots(t-\rho_m)$, then for every $k = 1, \ldots, m$, $\delta_m\rho_1\ldots\rho_k$ is an algebraic integer.*

PROOF. (i) Clearly $\delta_m\rho$ is an algebraic integer by Theorem 2.18 – why? The result is obvious in the case $m = 1$, so suppose that it is true for all polynomials of degree less than m. Now $g(t) = f(t) - \delta_m t^{m-1}(t-\rho)$ is of degree less than m, and $g(\rho) = 0$. By the induction hypothesis,

$$\frac{g(t)}{t-\rho} = \frac{f(t)}{t-\rho} - \delta_m t^{m-1}$$

is a polynomial all of whose coefficients are algebraic integers. Clearly this is also the case for $f(t)/(t-\rho)$.

(ii) This follows by repeated application of part (i). ◯

PROOF OF THEOREM 3.8. Let us suppose that

$$p(t) = \alpha_p(t-\nu_1)\ldots(t-\nu_p) \quad \text{and} \quad q(t) = \beta_q(t-\omega_1)\ldots(t-\omega_q).$$

Then the coefficients of the polynomial

$$\frac{r(t)}{\delta} = \frac{\alpha_p\beta_q}{\delta}(t-\nu_1)\ldots(t-\nu_p)(t-\omega_1)\ldots(t-\omega_q)$$

are algebraic integers, and so by Theorem 3.9(ii), every product of the form

$$\frac{\alpha_p\beta_q}{\delta}\nu_{m_1}\ldots\nu_{m_i}\omega_{n_1}\ldots\omega_{n_j} \tag{3.4}$$

is an algebraic integer. On the other hand, α_i/α_p and β_j/β_q are elementary symmetric functions in $\nu_1, ldots, \nu_p$ and in $\omega_1, \ldots, \omega_q$ respectively. It follows that

$$\frac{\alpha_i\beta_j}{\delta} = \frac{\alpha_p\beta_q}{\delta}\frac{\alpha_i}{\alpha_p}\frac{\beta_j}{\beta_q}$$

is a sum of terms of the form (3.4), hence an algebraic integer. ◯

PROOF OF THEOREM 3.5. Let $\mathfrak{a} = \langle\alpha_1, \ldots, \alpha_s\rangle$. For each $j = 1, \ldots, s$, let $\alpha_j^{(1)}, \ldots, \alpha_j^{(n)}$ denote the K-conjugates of α_j with $\alpha_j^{(1)} = \alpha_j$. For each $i = 1, \ldots, n$, let $f_i(t) = \alpha_1^{(i)}t + \ldots + \alpha_s^{(i)}t^s$, and write

$$F(t) = f_1(t)\ldots f_n(t) = \sum_k c_k t^k.$$

Now each coefficient c_k is a sum of products of algebraic integers $\alpha_j^{(i)}$, symmetric with respect to permutation of the variable i. Application of Theorem 1.8 shows that each c_k is a rational integer. Furthermore, $F(t) = f_1(t)h(t)$, where $h(t) = f_2(t)\ldots f_n(t)$ has coefficients which are algebraic integers in K. Suppose that $h(t) = \beta_1 t + \ldots + \beta_m t^m$. Now let a be the greatest common divisor of all the c_k, and let $\mathfrak{b} = \langle\beta_1, \ldots, \beta_m\rangle$. We show that $\mathfrak{ab} = \langle a\rangle$. By Theorem 3.8, $\alpha_i\beta_j/a$ is an algebraic integer for every $i = 1, \ldots, s$ and $j = 1, \ldots, m$. Since $\mathfrak{ab} = \langle\alpha_1\beta_1, \ldots, \alpha_i\beta_j, \ldots, \alpha_s\beta_m\rangle$, we must have $\mathfrak{ab} \subseteq \langle a\rangle$. To show that $\langle a\rangle \subseteq \mathfrak{ab}$, note that there exist rational integers x_k such that

$$a = \sum_k x_k c_k.$$

Now each c_k is of the form

$$\sum_{i,j}\lambda_{ijk}\alpha_i\beta_j,$$

where $\lambda_{ijk} \in \{0, 1\}$. Hence a is of the form

$$\sum_{i,j}\left(\sum_k x_k\lambda_{ijk}\right)\alpha_i\beta_j,$$

so that $a \in \mathfrak{ab}$. The result follows. ◯

3.4. The Modern Proof of the Unique Factorization Theorem

We proceed in a sequence of steps.

THEOREM 3.10. *Suppose that $\mathfrak{a}$ is an ideal in an algebraic number field K such that whenever $\beta, \gamma \in \mathfrak{O}$ and $\beta\gamma \in \mathfrak{a}$, we have $\beta \in \mathfrak{a}$ or $\gamma \in \mathfrak{a}$. Then $\mathfrak{a}$ is maximal in K.*

PROOF. Let $\mathfrak{b}$ be an ideal in K such that $\mathfrak{a} \subsetneqq \mathfrak{b}$. We must show that $\mathfrak{b} = \mathfrak{O}$. To do this, it is sufficient to show that $1 \in \mathfrak{b}$. Recall Theorem 3.2(iii), that $\mathfrak{a}$ contains a positive rational integer a. Then, as in the proof of Theorem 3.2(ii), every element of $\mathfrak{O}$ can be written in the form $a\gamma + \beta$, where $\gamma \in \mathfrak{O}$ and $\beta \in \mathcal{B}$, where $\mathcal{B}$ is a finite set. Let $\alpha \in \mathfrak{b}$ such that $\alpha \notin \mathfrak{a}$. Then for every $j \in \mathbb{N}$, we have

$$\alpha^j = a\gamma_j + \beta_j,$$

where $\gamma_j \in \mathfrak{O}$ and $\beta_j \in \mathcal{B}$. Hence $\alpha^j - a\gamma_j \in \mathcal{B}$, and can only have finitely many different values. It follows that there exist $k, \ell \in \mathbb{N}$ such that $k > \ell$ and

$$\alpha^k - a\gamma_k = \alpha^\ell - a\gamma_\ell.$$

Note that $\alpha^\ell(\alpha^{k-\ell} - 1) = \alpha^k - \alpha^\ell = a(\gamma_k - \gamma_\ell) \in \mathfrak{a}$, so that by the hypothesis on $\mathfrak{a}$, either $\alpha^\ell \in \mathfrak{a}$ or $\alpha^{k-\ell} - 1 \in \mathfrak{a}$. Clearly $\alpha^\ell \notin \mathfrak{a}$, for otherwise $\alpha \in \mathfrak{a}$. Hence $\alpha^{k-\ell} - 1 \in \mathfrak{a} \subset \mathfrak{b}$. Since $\alpha \in \mathfrak{b}$, we conclude that $\alpha^{k-\ell} \in \mathfrak{b}$, and so $1 \in \mathfrak{b}$. ◯

THEOREM 3.11. *Suppose that $\mathfrak{a}$ is an ideal in an algebraic number field K such that $\mathfrak{a} \neq \langle 0 \rangle$ and $\mathfrak{a} \neq \mathfrak{O}$. Then there exist maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ in K such that $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{a}$ and $\mathfrak{a} \subseteq \mathfrak{p}_i$ for every $i = 1, \ldots, r$.*

PROOF. If $\mathfrak{a}$ is maximal, then there is nothing to prove. If $\mathfrak{a}$ is not maximal, then it follows from Theorem 3.10 that there exist $\beta, \gamma \in \mathfrak{O}$ such that $\beta \notin \mathfrak{a}$, $\gamma \notin \mathfrak{a}$ and $\beta\gamma \in \mathfrak{a}$. If $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_s \rangle$, let $\mathfrak{b} = \langle \alpha_1, \ldots, \alpha_s, \beta \rangle$ and $\mathfrak{c} = \langle \alpha_1, \ldots, \alpha_s, \gamma \rangle$. Then $\mathfrak{a} \subseteq \mathfrak{b}$, $\mathfrak{a} \subseteq \mathfrak{c}$ and $\mathfrak{bc} \subseteq \mathfrak{a}$. We now repeat this procedure with $\mathfrak{b}$ and $\mathfrak{c}$. By Theorem 3.2, $\mathfrak{a}$ has only a finite number of divisors, and so is contained in at most a finite number of ideals in K. Our procedure must therefore end, so that we end up with maximal ideals. ◯

For an algebraic number field K with ring of integers $\mathfrak{O}$, and for every ideal $\mathfrak{a}$ of K, we define

$$\mathfrak{a}^{-1} = \{\gamma \in K : \gamma\mathfrak{a} \subseteq \mathfrak{O}\}.$$

THEOREM 3.12. *Suppose that $\mathfrak{p}$ is a maximal ideal in an algebraic number field K. Then $\mathfrak{p}^{-1}$ contains a number which is not an algebraic integer.*

PROOF. Let $\alpha \in \mathfrak{p}$, with $\alpha \neq 0$. By Theorem 3.11, we can choose a minimal natural number r subject to the existence of maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ in K such that $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \langle \alpha \rangle \subseteq \mathfrak{p}$. Now $\mathfrak{p}$ is prime by Theorem 3.3, so that $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some $i = 1, \ldots, r$. Without loss of generality, assume that $\mathfrak{p}_1 \subseteq \mathfrak{p}$. Since $\mathfrak{p}_1$ is maximal, we must have $\mathfrak{p}_1 = \mathfrak{p}$. By the minimality of r, we have $\mathfrak{p}_2 \ldots \mathfrak{p}_r \not\subseteq \langle \alpha \rangle$. It follows that there exists $\beta \in \mathfrak{p}_2 \ldots \mathfrak{p}_r \setminus \langle \alpha \rangle$. But $\beta\mathfrak{p} \subseteq \langle \alpha \rangle$, so that $\beta\alpha^{-1}\mathfrak{p} \subseteq \mathfrak{O}$ and so $\beta\alpha^{-1} \in \mathfrak{p}^{-1}$. Since $\beta \notin \langle \alpha \rangle$, we must have $\beta\alpha^{-1} \notin \mathfrak{O}$. ◯

Let A and B be sets. By the product AB, we mean the set of all finite sums of products $\alpha\beta$, where $\alpha \in A$ and $\beta \in B$. Note that this coincides with the definition of the product of two ideals in an algebraic number field.

THEOREM 3.13. *Suppose that $\mathfrak{p}$ is a maximal ideal in an algebraic number field K. Then $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{O}$.*

PROOF. Let $\mathfrak{a} = \mathfrak{p}\mathfrak{p}^{-1}$. Then $\mathfrak{a}$ is an ideal in K – why? Since $1 \in \mathfrak{p}^{-1}$, we have $\mathfrak{p} \subseteq \mathfrak{a} \subseteq \mathfrak{O}$. Since $\mathfrak{p}$ is maximal in K, we must have $\mathfrak{a} = \mathfrak{O}$ or $\mathfrak{a} = \mathfrak{p}$. Suppose on the contrary that $\mathfrak{a} = \mathfrak{p}$. Let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Z}$-basis for $\mathfrak{p}$, and let $\alpha \in \mathfrak{p}^{-1}$ such that $\alpha \notin \mathfrak{O}$, in view of Theorem 3.12. Clearly for each $i = 1, \ldots, n$, the product $\alpha\omega_i \in \mathfrak{a} = \mathfrak{p}$, so that $\alpha\omega_i = a_{i1}\omega_1 + \ldots + a_{in}\omega_n$, where $a_{i1}, \ldots, a_{in} \in \mathbb{Z}$. Then the system of simultaneous linear equations

$$\begin{aligned}
(a_{11} - \alpha)t_1 + \quad & a_{12}t_2 + \ldots + \quad a_{1n}t_n = 0, \\
a_{21}t_1 + (a_{22} - \alpha)t_2 + \ldots + \quad & a_{2n}t_n = 0, \\
& \vdots \\
a_{n1}t_1 + \quad & a_{n2}t_2 + \ldots + (a_{nn} - \alpha)t_n = 0,
\end{aligned}$$

has a non-trivial solution $(\omega_1, \ldots, \omega_n)$, so that the determinant

$$\begin{vmatrix} a_{11}-\alpha & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22}-\alpha & \ldots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn}-\alpha \end{vmatrix} = 0.$$

It follows that α satisfies a monic polynomial equation with integral coefficients, and so is an algebraic integer. This is a contradiction. Hence we must have $\mathfrak{a} = \mathfrak{O}$, and this completes the proof. ◯

PROOF OF THEOREM 3.4. Let $\mathfrak{a}$ be an ideal in an algebraic number field K such that $\mathfrak{a} \neq \langle 0 \rangle$ and $\mathfrak{a} \neq \mathfrak{O}$.

We first of all show that $\mathfrak{a}$ can be written as a product of maximal ideals. By Theorem 3.11, there exist maximal ideals $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ in K, with minimal r, such that $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{a}$ and $\mathfrak{a} \subseteq \mathfrak{p}_i$ for every $i = 1, \ldots, r$. We now proceed by induction on r. If $r = 1$, then $\mathfrak{a} = \mathfrak{p}_1$ and the proof is complete. Suppose now that every ideal in K that satisfies Theorem 3.11 with fewer than r maximal ideals is a product of maximal ideals. Since $\mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq \mathfrak{a}$, we have $\mathfrak{p}_1 \ldots \mathfrak{p}_{r-1} \subseteq \mathfrak{a}\mathfrak{p}_r^{-1}$ by Theorem 3.13. Since $\mathfrak{a} \subseteq \mathfrak{p}_r$, it is not difficult to see that $\mathfrak{a}\mathfrak{p}_r^{-1}$ is an ideal in K. By the induction hypothesis, we have $\mathfrak{a}\mathfrak{p}_r^{-1} = \mathfrak{q}_1 \ldots \mathfrak{q}_k$, where $\mathfrak{q}_1, \ldots, \mathfrak{q}_k$ are maximal ideals in K. By Theorem 3.13 again, we have $\mathfrak{a} = \mathfrak{q}_1 \ldots \mathfrak{q}_k \mathfrak{p}_r$, and the result follows.

The uniqueness of factorization is now established in precisely the same way as in Section 3.3, noting that every maximal ideal in K is prime. ◯

3.5. Consequences of the Unique Factorization Theorem

Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals in an algebraic number field K. Then an ideal $\mathfrak{g}$ in K is said to be a greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$ if

(i) $\mathfrak{g} \mid \mathfrak{a}$ and $\mathfrak{g} \mid \mathfrak{b}$; and
(ii) if $\mathfrak{g}'$ is an ideal in K such that $\mathfrak{g}' \mid \mathfrak{a}$ and $\mathfrak{g}' \mid \mathfrak{b}$, then $\mathfrak{g}' \mid \mathfrak{g}$.

In view of the result below, we write $\mathfrak{g} = (\mathfrak{a}, \mathfrak{b})$.

THEOREM 3.14. *Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are two ideals in an algebraic number field K and not both zero. Then $(\mathfrak{a}, \mathfrak{b})$ exists and is unique.*

PROOF. Suppose that $\mathfrak{a} = \langle \alpha_1, \ldots, \alpha_r \rangle$ and $\mathfrak{b} = \langle \beta_1, \ldots, \beta_s \rangle$. Let us write

$$\mathfrak{g} = \langle \alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \rangle.$$

We claim that $\mathfrak{g} = (\mathfrak{a}, \mathfrak{b})$. Clearly we have $\mathfrak{a} \subseteq \mathfrak{g}$ and $\mathfrak{b} \subseteq \mathfrak{g}$, so that $\mathfrak{g} \mid \mathfrak{a}$ and $\mathfrak{g} \mid \mathfrak{b}$ by Theorem 3.6(ii). Suppose now that $\mathfrak{g}'$ is an ideal in K such that $\mathfrak{g}' \mid \mathfrak{a}$ and $\mathfrak{g}' \mid \mathfrak{b}$. Then $\mathfrak{a} \subseteq \mathfrak{g}'$ and $\mathfrak{b} \subseteq \mathfrak{g}'$ by Theorem 3.2(i), so that $\mathfrak{g} \subseteq \mathfrak{g}'$, whence $\mathfrak{g}' \mid \mathfrak{g}$ by Theorem 3.6(ii). ◯

Recall that any ideal in an algebraic number field can be generated by a finite number of elements, for instance, those in a $\mathbb{Z}$-basis. We now show that, in fact, two generators will suffice.

THEOREM 3.15. *Suppose that K is an algebraic number field. Suppose further that $\mathfrak{a}$ is a non-zero ideal in K, and that $0 \neq \beta \in \mathfrak{a}$. Then there exists $\alpha \in \mathfrak{a}$ such that $\mathfrak{a} = \langle \alpha, \beta \rangle$.*

We deduce this from the following intermediate result.

THEOREM 3.16. *Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are non-zero ideals in an algebraic number field K, with ring of integers $\mathfrak{O}$. Then there exists $\alpha \in \mathfrak{a}$ such that $(\langle \alpha \rangle \mathfrak{a}^{-1}, \mathfrak{b}) = \mathfrak{O}$.*

Note that if $\alpha \in \mathfrak{a}$, then $\langle \alpha \rangle \subseteq \mathfrak{a}$, so that $\mathfrak{a} \mid \langle \alpha \rangle$. It follows that $\langle \alpha \rangle \mathfrak{a}^{-1}$ is the ideal $\mathfrak{x}$ satisfying $\mathfrak{a}\mathfrak{x} = \langle \alpha \rangle$.

PROOF OF THEOREM 3.15. Let $\mathfrak{b} = \langle \beta \rangle \mathfrak{a}^{-1}$. By Theorem 3.16, there exists $\alpha \in \mathfrak{a}$ such that $(\langle \alpha \rangle \mathfrak{a}^{-1}, \langle \beta \rangle \mathfrak{a}^{-1}) = \mathfrak{O}$. Let $\mathfrak{c}$ and $\mathfrak{d}$ be ideals in K such that $\langle \alpha \rangle = \mathfrak{a}\mathfrak{c}$ and $\langle \beta \rangle = \mathfrak{a}\mathfrak{d}$. Then $(\mathfrak{c}, \mathfrak{d}) = \mathfrak{O}$, so that $(\langle \alpha \rangle, \langle \beta \rangle) = \mathfrak{a}$. This gives $\langle \alpha, \beta \rangle = \mathfrak{a}$ – see the proof of Theorem 3.14. ◯

PROOF OF THEOREM 3.16. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the distinct prime ideals dividing $\mathfrak{b}$. Since every prime ideal that divides $\mathfrak{b}$ must also divide at least one of $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, it is sufficient to choose $\alpha \in \mathfrak{a}$ such that $(\alpha \mathfrak{a}^{-1}, \mathfrak{p}_i) = \mathfrak{O}$ for every $i = 1, \ldots, r$. Since each $\mathfrak{p}_i$ is prime in K, it is also maximal in K.

Hence it suffices to choose $\alpha \in \mathfrak{a}$ such that $\alpha\mathfrak{a}^{-1} \neq \mathfrak{p}_i$ for every $i = 1, \ldots, r$. In other words, it suffices to choose $\alpha \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}_i$ for every $i = 1, \ldots, r$. For $r = 1$, this is trivial, for $\mathfrak{a}\mathfrak{p}_1 \subsetneqq \mathfrak{a}$ by uniqueness of factorization. Suppose now that $r > 1$. For every $i = 1, \ldots, r$, let

$$\mathfrak{a}_i = \mathfrak{a}\mathfrak{p}_1 \ldots \mathfrak{p}_{i-1}\mathfrak{p}_{i+1} \ldots \mathfrak{p}_r.$$

Again $\mathfrak{a}_i\mathfrak{p}_i \subsetneqq \mathfrak{a}_i$, so that there exists $\alpha_i \in \mathfrak{a}_i \setminus \mathfrak{a}_i\mathfrak{p}_i$ for every $i = 1, \ldots, r$. Clearly $\alpha_i \in \mathfrak{a}$ for every $i = 1, \ldots, r$, so that $\alpha = \alpha_1 + \ldots + \alpha_r \in \mathfrak{a}$. On the other hand, for every $i = 1, \ldots, r$, we have $\alpha \notin \mathfrak{a}\mathfrak{p}_i$, for otherwise, noting that $\alpha_j \in \mathfrak{a}_j \subseteq \mathfrak{a}\mathfrak{p}_i$ for every $j \neq i$, we would have

$$\alpha_i = \alpha - \alpha_1 - \ldots - \alpha_{i-1} - \alpha_{i+1} - \ldots - \alpha_r \in \mathfrak{a}\mathfrak{p}_i,$$

a contradiction. ◯

We round off this section by establishing a result on the relationship between factorization of elements and factorization of ideals.

THEOREM 3.17. *Suppose that K is an algebraic number field, with ring of integers $\mathfrak{O}$. Then factorization of elements of $\mathfrak{O}$ into primes is unique to within order and units if and only if every ideal in K is principal.*

We need the following intermediate result.

THEOREM 3.18. *Suppose that K is an algebraic number field, with ring of integers $\mathfrak{O}$. Suppose further that γ is a prime in $\mathfrak{O}$.*

(i) *If every ideal in K is principal, then $\langle\gamma\rangle$ is prime.*
(ii) *If factorization of elements of $\mathfrak{O}$ into primes is unique to within order and units, then $\langle\gamma\rangle$ is prime.*

PROOF. (i) Suppose that $\langle\gamma\rangle = \mathfrak{b}_1\mathfrak{b}_2$, where $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are ideals in K. Since $\mathfrak{b}_1$ and $\mathfrak{b}_2$ are both principal, there exist $\beta_1, \beta_2 \in \mathfrak{O}$ such that $\mathfrak{b}_1 = \langle\beta_1\rangle$ and $\mathfrak{b}_2 = \langle\beta_2\rangle$. Then $\langle\beta_1\beta_2\rangle = \langle\gamma\rangle$, so that $\beta_1\beta_2$ and γ are associates. Hence one of β_1 or β_2 is a unit, so that $\mathfrak{b}_1 = \mathfrak{O}$ or $\mathfrak{b}_2 = \mathfrak{O}$.

(ii) We first of all show that if $\gamma \mid \alpha\beta$, then $\gamma \mid \alpha$ or $\gamma \mid \beta$. If $\gamma \mid \alpha\beta$, then there exists $\delta \in \mathfrak{O}$ such that $\gamma\delta = \alpha\beta$. We now factorize each of α, β and δ into a product of primes. Uniqueness of factorization then gives the conclusion that the representation of $\alpha\beta$ as a product of primes contains an associate of γ. This must have come from the factorization of α or that of β, establishing our claim. To show that $\langle\gamma\rangle$ is prime, suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in K such that $\mathfrak{a}\mathfrak{b} \subseteq \langle\gamma\rangle$ and $\mathfrak{a} \not\subset \langle\gamma\rangle$. We must then show that $\mathfrak{b} \subseteq \langle\gamma\rangle$. Since $\mathfrak{a} \not\subset \langle\gamma\rangle$, there exists $\alpha_1 \in \mathfrak{a}$ such that $\alpha_1 \notin \langle\gamma\rangle$, so that $\gamma \nmid \alpha_1$. By Theorem 3.15, we have $\mathfrak{a} = \langle\alpha_1, \alpha_2\rangle$ for some $\alpha_2 \in \mathfrak{a}$. Let $\mathfrak{b} = \langle\beta_1, \ldots, \beta_s\rangle$. Then

$$\mathfrak{a}\mathfrak{b} = \langle\alpha_1\beta_1, \ldots, \alpha_1\beta_s, \alpha_2\beta_1, \ldots, \alpha_2\beta_s\rangle \subseteq \langle\gamma\rangle.$$

It follows that $\gamma \mid \alpha_1\beta_j$ and thus $\gamma \mid \beta_j$ for every $j = 1, \ldots, s$. Hence $\mathfrak{b} \subseteq \langle\gamma\rangle$. ◯

PROOF OF THEOREM 3.17. ($\Leftarrow$) Assume first of all that every ideal in K is principal. Suppose that α is an element of $\mathfrak{O}$, not zero or a unit, and has factorization in primes

$$\alpha = \gamma_1 \ldots \gamma_r = \delta_1 \ldots \delta_s.$$

In view of Theorem 3.18(i), this gives rise to a factorization of $\langle\alpha\rangle$ into prime ideals

$$\langle\alpha\rangle = \langle\gamma_1\rangle \ldots \langle\gamma_r\rangle = \langle\delta_1\rangle \ldots \langle\delta_s\rangle.$$

Uniqueness of factorization of ideals gives $r = s$ and, after a suitable rearrangement, $\langle\gamma_i\rangle = \langle\delta_i\rangle$ for every $i = 1, \ldots, r$. Hence the primes γ_i and δ_i are associates for every $i = 1, \ldots, r$.

($\Rightarrow$) Suppose now that factorization of elements in $\mathfrak{O}$ into primes is unique to within order and units. To prove that every ideal in K is principal, it clearly suffices to prove that every prime ideal in K is principal. Let $\mathfrak{p}$ be a prime ideal in K. By Theorem 3.2(iii), there exists a non-zero rational integer $N \in \mathfrak{p}$. Let $N = \gamma_1 \ldots \gamma_s$, where $\gamma_1, \ldots, \gamma_s$ are primes in $\mathfrak{O}$. Then $\langle N\rangle = \langle\gamma_1\rangle \ldots \langle\gamma_s\rangle \subseteq \mathfrak{p}$. It follows that $\mathfrak{p} \mid \langle\gamma\rangle$ for some γ in $\mathfrak{O}$. By Theorem 3.18(ii), the ideal $\langle\gamma\rangle$ is prime. It follows from the uniqueness of factorization of ideals that $\mathfrak{p} = \langle\gamma\rangle$, so that $\mathfrak{p}$ is principal. ◯

3.6. Norm of an Ideal

Throughout this section, K is an algebraic number field, with ring of integers $\mathfrak{O}$, and $\mathfrak{a}$ is an ideal in K.

We say that two numbers $\alpha, \beta \in \mathfrak{O}$ are congruent modulo $\mathfrak{a}$, written $\alpha \equiv \beta \bmod \mathfrak{a}$, if $\alpha - \beta \in \mathfrak{a}$. It is not difficult to show that congruence modulo $\mathfrak{a}$ is an equivalence relation on $\mathfrak{O}$. The equivalence classes that arise are called residue classes modulo $\mathfrak{a}$.

THEOREM 3.19. *Suppose that $\mathfrak{a}$ is a non-zero ideal in an algebraic number field K. Then the number of distinct residue classes modulo $\mathfrak{a}$ is finite.*

PROOF. We use ideas in the proof of Theorem 3.2. Let $a \in \mathfrak{a}$ be a non-zero rational integer. Since $\langle a \rangle \subseteq \mathfrak{a}$, it follows that for every $\mu, \nu \in \mathfrak{O}$ that satisfy $\mu \equiv \nu \bmod \langle a \rangle$, we must have $\mu \equiv \nu \bmod \mathfrak{a}$. Hence the number of distinct residue classes modulo $\mathfrak{a}$ cannot exceed the number of distinct residue classes modulo $\langle a \rangle$. On the other hand, every $\alpha \in \mathfrak{O}$ can be written in the form $\alpha = a\gamma + \beta$, where $\gamma \in \mathfrak{O}$ and $\beta \in \mathcal{B}$, where $\mathcal{B}$ is a finite set. It follows that the number of distinct residue classes modulo $\langle a \rangle$ is finite. ◯

By the norm of an ideal $\mathfrak{a}$ in an algebraic number field K, denoted by $N(\mathfrak{a})$, we mean the number of distinct residue classes modulo $\mathfrak{a}$. Note that if $\mathfrak{O}$ is the ring of integers in K, then $N(\mathfrak{a}) = |\mathfrak{O}/\mathfrak{a}|$.

By a complete set of residues modulo $\mathfrak{a}$, we mean a set of $N(\mathfrak{a})$ elements in $\mathfrak{O}$ which are pairwise incongruent modulo $\mathfrak{a}$, so that every element in $\mathfrak{O}$ is congruent to precisely one of these modulo $\mathfrak{a}$.

THEOREM 3.20. *Suppose that $\mathfrak{a}$ is a non-zero ideal in an algebraic number field K, and that $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$. Then*

$$N(\mathfrak{a}) = \left| \frac{\Delta[\alpha_1, \ldots, \alpha_n]}{\Delta} \right|^{\frac{1}{2}},$$

where Δ is the discriminant of K, i.e. the discriminat of any integral basis of the ring of integers $\mathfrak{O}$.

To establish Theorem 3.20, we first of all exhibit the existence of a $\mathbb{Z}$-basis for $\mathfrak{a}$ of a particular kind.

THEOREM 3.21. *Suppose that $\{\omega_1, \ldots, \omega_n\}$ is an integral basis for the ring of integers $\mathfrak{O}$ of an algebraic number field K. Then every non-zero ideal $\mathfrak{a}$ of K has a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of the form*

$$\begin{aligned}
\alpha_1 &= a_{11}\omega_1, \\
\alpha_2 &= a_{21}\omega_1 + a_{22}\omega_2, \\
&\vdots \\
\alpha_n &= a_{n1}\omega_1 + a_{n2}\omega_2 + \ldots + a_{nn}\omega_n,
\end{aligned}$$

where the coefficients $a_{ij} \in \mathbb{Z}$ and $a_{ii} > 0$ for every $i = 1, \ldots, n$.

PROOF. Clearly $a\omega_i \in \mathfrak{a}$ for every non-zero rational integer $a \in \mathfrak{a}$ and every $i = 1, \ldots, n$. Let an integer m satisfying $1 \leqslant m \leqslant n$ be fixed. Clearly the set

$$\{a_1\omega_1 + \ldots + a_m\omega_m \in \mathfrak{a} : a_1, \ldots, a_m \in \mathbb{Z},\ a_m > 0\} \tag{3.5}$$

is non-empty, since $\mathfrak{a}$ contains a non-zero rational integer a, and so $a\omega_m$ and $-a\omega_m$ are in $\mathfrak{a}$. Let α_m be the element in the set (3.5) with minimal a_m, and write

$$\alpha_m = a_{m1}\omega_1 + \ldots + a_{mm}\omega_m.$$

We claim that the set $\{\alpha_1, \ldots, \alpha_n\}$ has the required properties. Note, first of all, that $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for K, since the determinant

$$\begin{vmatrix}
a_{11} & & & \\
a_{21} & a_{22} & & \\
\vdots & \vdots & \ddots & \\
a_{n1} & a_{n2} & \ldots & a_{nn}
\end{vmatrix} \neq 0.$$

We now show that $\{\alpha_1, \ldots, \alpha_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a}$. Let $\alpha \in \mathfrak{a}$. Then there exists $b_1, \ldots, b_n \in \mathbb{Z}$ such that $\alpha = b_1\omega_1 + \ldots + b_n\omega_n$. Consider the number b_n. There exist integers h_n and r_n such that $b_n = a_{nn}h_n + r_n$ and $0 \leqslant r_n < a_{nn}$. Then there exist $b'_1, \ldots, b'_{n-1} \in \mathbb{Z}$ such that

$$\alpha - h_n\alpha_n = b'_1\omega_1 + \ldots + b'_{n-1}\omega_{n-1} + r_n\omega_n \in \mathfrak{a}.$$

If $r_n > 0$, then $r_n < a_{nn}$ contradicts the minimality of a_{nn}. It follows that $r_n = 0$, and so

$$\alpha - h_n\alpha_n = b'_1\omega_1 + \ldots + b'_{n-1}\omega_{n-1}.$$

Repeating this procedure, we conclude that there exist $h_{n-1}, b''_1, \ldots, b''_{n-2} \in \mathbb{Z}$ such that

$$\alpha - h_n\alpha_n - h_{n-1}\alpha_{n-1} = b''_1\omega_1 + \ldots + b''_{n-2}\omega_{n-2}.$$

And so on. After finitely many repetitions of this procedure, we conclude that α can be expressed as a linear combination of $\alpha_1, \ldots, \alpha_n$ with rational integer coefficients. This expression is unique, since $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for K. ◯

Proof of Theorem 3.20. Note that a consequence of the proof of Theorem 3.1 is that the discriminant of any $\mathbb{Z}$-basis for $\mathfrak{a}$ is the same, so that we may take $\{\alpha_1, \ldots, \alpha_n\}$ to be defined in Theorem 3.21. Then by Theorem 2.19,

$$\Delta[\alpha_1, \ldots, \alpha_n] = \begin{vmatrix} a_{11} & & & \\ a_{21} & a_{22} & & \\ \vdots & \vdots & \ddots & \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}^2 \Delta[\omega_1, \ldots, \omega_n],$$

so that $\Delta[\alpha_1, \ldots, \alpha_n] = (a_{11} \ldots a_{nn})^2\Delta$. To complete the proof, it is therefore sufficient to show that $N(\mathfrak{a}) = a_{11} \ldots a_{nn}$; in other words, that the number of distinct residue classes modulo $\mathfrak{a}$ is $a_{11} \ldots a_{nn}$. We achieve this by showing that the numbers $r_1\omega_1 + \ldots + r_n\omega_n$, where $r_i \in \mathbb{Z}$ and $0 \leqslant r_i < a_{ii}$ for every $i = 1, \ldots, n$, form a complete set of residues modulo $\mathfrak{a}$. We therefore need to show that (i) they are pairwise incongruent modulo $\mathfrak{a}$; and (ii) every element in $\mathfrak{O}$ is congruent to one of these numbers modulo $\mathfrak{a}$.

(i) Suppose that

$$r'_1\omega_1 + \ldots + r'_n\omega_n \equiv r''_1\omega_1 + \ldots + r''_n\omega_n \bmod \mathfrak{a},$$

where $0 \leqslant r'_i, r''_i < a_{ii}$ for every $i = 1, \ldots, n$. Then

$$(r'_1 - r''_1)\omega_1 + \ldots + (r'_n - r''_n)\omega_n \in \mathfrak{a}.$$

We may assume, without loss of generality, that $r'_n \geqslant r''_n$. Then $0 \leqslant r'_n - r''_n < a_{nn}$, and so $r'_n = r''_n$ in view of the minimality of a_{nn}. Thus

$$(r'_1 - r''_1)\omega_1 + \ldots + (r'_{n-1} - r''_{n-1})\omega_{n-1} \in \mathfrak{a}.$$

Repetition of this argument gives $r'_i = r''_i$ for every $i = 1, \ldots, n$.

(ii) Every number $\alpha \in \mathfrak{O}$ is of the form $\alpha = b_1\omega_1 + \ldots + b_n\omega_n$, where the coefficients $b_1, \ldots, b_n \in \mathbb{Z}$. Let $b_n = a_{nn}h_n + r_n$, where $h_n, r_n \in \mathbb{Z}$ and $0 \leqslant r_n < a_{nn}$. Then there exist $b'_1, \ldots, b'_{n-1} \in \mathbb{Z}$ such that

$$\alpha - h_n\alpha_n = b'_1\omega_1 + \ldots + b'_{n-1}\omega_{n-1} + r_n\omega_n.$$

Repeating this procedure, we conclude that there exist $h_1, \ldots, h_n \in \mathbb{Z}$ such that

$$\alpha - h_n\alpha_n - \ldots - h_1\alpha_1 = r_1\omega_1 + \ldots + r_n\omega_n,$$

where $0 \leqslant r_i < a_{ii}$ for every $i = 1, \ldots, n$. Clearly $\alpha \equiv r_1\omega_1 + \ldots + r_n\omega_n \bmod \mathfrak{a}$. ◯

It is now easy to deduce the following result.

Theorem 3.22. *Suppose that K is an algebraic number field, and that the ideal $\mathfrak{a} = \langle\alpha\rangle \neq \langle 0\rangle$ is principal in K. Then $N(\mathfrak{a}) = |N(\alpha)|$.*

PROOF. Let $\{\omega_1, \ldots, \omega_n\}$ be a $\mathbb{Z}$-basis for $\mathfrak{O}$. Then clearly $\{\alpha\omega_1, \ldots, \alpha\omega_n\}$ is a $\mathbb{Z}$-basis for $\mathfrak{a} = \langle\alpha\rangle$. By Theorem 3.20,

$$N(\mathfrak{a}) = \left|\frac{\Delta[\alpha\omega_1, \ldots, \alpha\omega_n]}{\Delta[\omega_1, \ldots, \omega_n]}\right|^{\frac{1}{2}} = \left|\frac{|(\alpha^{(i)}\omega_j^{(i)})|}{|(\omega_j^{(i)})|}\right| = |\alpha^{(1)} \ldots \alpha^{(n)}|$$

as required. ◯

A useful property of the norm is the following.

THEOREM 3.23. *Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ are non-zero ideals in an algebraic number field K. Then $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

To establish this, we need the following result on congruences.

THEOREM 3.24. *Suppose that $\mathfrak{a}$ is a non-zero ideal in an algebraic number field K, and $\alpha, \beta \in \mathfrak{O}$, the ring of integers in K.*

(i) *Suppose further that $(\langle\alpha\rangle, \mathfrak{a}) = \mathfrak{O}$. Then the congruence $\alpha\xi \equiv \beta \bmod \mathfrak{a}$ has a solution $\xi \in \mathfrak{O}$ which is unique modulo $\mathfrak{a}$.*
(ii) *Suppose further that $(\langle\alpha\rangle, \mathfrak{a}) = \mathfrak{d}$. Then the congruence $\alpha\xi \equiv \beta \bmod \mathfrak{a}$ has a solution $\xi \in \mathfrak{O}$ if and only if $\beta \in \mathfrak{d}$. If there is a solution, then it is unique modulo $\mathfrak{d}^{-1}\mathfrak{a}$.*

PROOF. (i) Let $\{\xi_1, \ldots, \xi_{N(\mathfrak{a})}\}$ be a complete set of residues modulo $\mathfrak{a}$. Since $(\langle\alpha\rangle, \mathfrak{a}) = \mathfrak{O}$, the set $\{\alpha\xi_1, \ldots, \alpha\xi_{N(\mathfrak{a})}\}$ is also a complete set of residues modulo $\mathfrak{a}$. To see this, note that if $\alpha\xi_i \equiv \alpha\xi_j \bmod \mathfrak{a}$, then $\alpha(\xi_i - \xi_j) \in \mathfrak{a}$, so that $\mathfrak{a} \mid \langle\alpha\rangle\langle\xi_i - \xi_j\rangle$. The condition $(\langle\alpha\rangle, \mathfrak{a}) = \mathfrak{O}$ then ensures that $\mathfrak{a} \mid \langle\xi_i - \xi_j\rangle$, so that $\xi_i - \xi_j \in \mathfrak{a}$, whence $\xi_i \equiv \xi_j \bmod \mathfrak{a}$. From the set $\{\alpha\xi_1, \ldots, \alpha\xi_{N(\mathfrak{a})}\}$, clearly precisely one element is congruent to β modulo $\mathfrak{a}$.

(ii) Suppose first of all that $\alpha\xi \equiv \beta \bmod \mathfrak{a}$. Then $\alpha\xi - \beta \in \mathfrak{a} \subseteq \mathfrak{d}$. Since $\mathfrak{d} = (\langle\alpha\rangle, \mathfrak{a})$, we must have $\mathfrak{d} \mid \langle\alpha\rangle$, so that $\alpha \in \mathfrak{d}$, and so $\alpha\xi \in \mathfrak{d}$, whence $\beta \in \mathfrak{d}$. Next, suppose that $\beta \in \mathfrak{d}$. Recall that $\mathfrak{d} = \langle\alpha, \alpha_1, \ldots, \alpha_s\rangle$, where $\langle\alpha_1, \ldots, \alpha_s\rangle = \mathfrak{a}$. It follows that there exists $\alpha\xi \in \langle\alpha\rangle$ and $\lambda \in \mathfrak{a}$ such that $\beta = \alpha\xi + \lambda$. Clearly we have $\alpha\xi \equiv \beta \bmod \mathfrak{a}$. Finally suppose that $\alpha\xi' \equiv \alpha\xi'' \equiv \beta \bmod \mathfrak{a}$. Then $\mathfrak{a} \mid \langle\alpha\rangle\langle\xi' - \xi''\rangle$. If $\mathfrak{a} = \mathfrak{d}\mathfrak{a}_1$ and $\langle\alpha\rangle = \mathfrak{d}\mathfrak{a}_2$, where $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are ideals in K, then $\mathfrak{a}_1 \mid \mathfrak{a}_2\langle\xi' - \xi''\rangle$. Since $(\mathfrak{a}_1, \mathfrak{a}_2) = \mathfrak{O}$, we must have $\mathfrak{a}_1 \mid \langle\xi' - \xi''\rangle$, and so $\xi' \equiv \xi'' \bmod \mathfrak{a}_1$. ◯

PROOF OF THEOREM 3.23. By Theorem 3.16, there exists $\gamma \in \mathfrak{a}$ such that $(\langle\gamma\rangle\mathfrak{a}^{-1}, \mathfrak{b}) = \mathfrak{O}$, so that $(\langle\gamma\rangle, \mathfrak{ab}) = \mathfrak{a}$. Let $\{\alpha_1, \ldots, \alpha_{N(\mathfrak{a})}\}$ and $\{\beta_1, \ldots, \beta_{N(\mathfrak{b})}\}$ be complete sets of residues modulo $\mathfrak{a}$ and $\mathfrak{b}$ respectively. We claim that the numbers $\alpha_i + \gamma\beta_j$, where $i = 1, \ldots, N(\mathfrak{a})$ and $j = 1, \ldots, N(\mathfrak{b})$, form a complete set of residues modulo $\mathfrak{ab}$. We therefore have to show that (i) these numbers are pairwise incongruent modulo $\mathfrak{ab}$; and (ii) every integer in K is congruent to one of these numbers modulo $\mathfrak{ab}$. The proof will then be complete since a complete set of residues modulo $\mathfrak{ab}$ has precisely $N(\mathfrak{ab})$ elements.

(i) Let $\alpha', \alpha'' \in \{\alpha_1, \ldots, \alpha_{N(\mathfrak{a})}\}$ and $\beta', \beta'' \in \{\beta_1, \ldots, \beta_{N(\mathfrak{b})}\}$. Suppose that

$$\alpha' + \gamma\beta' \equiv \alpha'' + \gamma\beta'' \bmod \mathfrak{ab}.$$

Then clearly $\alpha' + \gamma\beta' \equiv \alpha'' + \gamma\beta'' \bmod \mathfrak{a}$. Since $\gamma \in \mathfrak{a}$, we must have $\alpha' \equiv \alpha'' \bmod \mathfrak{a}$, and so $\alpha' = \alpha''$. Then $\gamma\beta' \equiv \gamma\beta'' \bmod \mathfrak{ab}$, so that $\mathfrak{ab} \mid \langle\gamma\rangle\langle\beta' - \beta''\rangle$. Write $\langle\gamma\rangle = \mathfrak{ac}$. Then $\mathfrak{b} \mid \mathfrak{c}\langle\beta' - \beta''\rangle$. Since $(\mathfrak{c}, \mathfrak{b}) = \mathfrak{O}$, it follows that $\mathfrak{b} \mid \langle\beta' - \beta''\rangle$, and so $\beta' \equiv \beta'' \bmod \mathfrak{b}$, whence $\beta' = \beta''$.

(ii) Let α be an integer in K. Choose $\alpha_i \equiv \alpha \bmod \mathfrak{a}$. Then the congruence $\gamma\xi \equiv \alpha - \alpha_i \bmod \mathfrak{ab}$ has a solution ξ by Theorem 3.24(ii). Moreover, ξ can be chosen uniquely modulo $\mathfrak{a}^{-1}\mathfrak{ab}$, so that ξ is one of the β_j. Clearly $\alpha \equiv \alpha_i + \gamma\beta + j \bmod \mathfrak{ab}$. ◯

We complete this chapter by making a few simple deductions from earlier results.

THEOREM 3.25. *Suppose that K is an algebraic number field.*

(i) *If $\mathfrak{a}$ is an ideal in K and $N(\mathfrak{a})$ is prime, then $\mathfrak{a}$ is a prime ideal.*
(ii) *If $\mathfrak{a}$ is a non-zero ideal in K, then $N(\mathfrak{a}) \in \mathfrak{a}$.*
(iii) *There are only a finite number of ideals in K of a given norm.*
(iv) *If $\mathfrak{a}$ is a prime ideal in K, then $\mathfrak{a}$ contains exactly one rational prime p, and $N(\mathfrak{a}) = p^m$ for some natural number $m \leqslant n = [K : \mathbb{Q}]$.*

PROOF. (i) This is obvious from Theorem 3.23.

(ii) If $\{\alpha_1, \ldots, \alpha_{N(\mathfrak{a})}\}$ is a complete set of residues modulo $\mathfrak{a}$, then so is the set $\{\alpha_1+1, \ldots, \alpha_{N(\mathfrak{a})}+1\}$. Then

$$\alpha_1 + \ldots + \alpha_{N(\mathfrak{a})} \equiv (\alpha_1 + 1) + \ldots + (\alpha_{N(\mathfrak{a})} + 1) \bmod \mathfrak{a}.$$

The result follows immediately.

(iii) Note that the norm is a non-zero rational integer and quote Theorem 3.2(ii).

(iv) Note that $N(\mathfrak{a}) \neq 1$, since $\mathfrak{a} \neq \mathfrak{O}$. It follows that $N(a) = p_1^{m_1} \ldots p_r^{m_r}$, where $p_1, \ldots, p_r$ are rational primes and $m_1, \ldots, m_r \in \mathbb{N}$. Since $N(\mathfrak{a}) \in \mathfrak{a}$, we have $\mathfrak{a} \mid \langle p_1 \rangle^{m_1} \ldots \langle p_r \rangle^{m_r}$. We therefore conclude that $\mathfrak{a} \mid \langle p \rangle$ for some rational prime p. Suppose now that p' and p'' are distinct rational primes and $p', p'' \in \mathfrak{a}$. Since there exists rational integers u and v such that $1 = up' + vp'' \in \mathfrak{a}$, it follows that $\mathfrak{a} = \mathfrak{O}$, a contradiction. Hence $\mathfrak{a}$ contains precisely one rational prime p. Since $\langle p \rangle \subseteq \mathfrak{a}$, we must have $N(\mathfrak{a}) \mid N(\langle p \rangle) = p^n$, and the last assertion follows. ◯