Unique Factorization of Ideals in $\mathfrak{O}_K$

Yi Guo

September 13, 2015

Contents

Abstract

Let K be a number field and $\mathfrak{O}_K$ be the ring of algebraic integers. We discuss the unique factorization of elements of $\mathfrak{O}_K$ into irreducibles and its use in solving Diophantine equations. We then proceed to prove the existence of the unique factorization of ideals of $\mathfrak{O}_K$ into prime ideals.

1 Introduction

Historically, the intuitive, though not always correct, idea of unique factorization had often been employed to solve Diophantine equations, i.e. polynomial equations in which only integer solutions are allowed. Using this idea without checking whether it is true in the field we are working in may cause problems. An example of such danger can be found in the following proof of a statement of Fermat:

The only integer solutions of $y^2 + 2 = x^3$ *is* $y = \pm 5$ *and* $x = 3$.

A brilliant idea in this proof is to adjoin $\sqrt{-2}$ to $\mathbb{Z}$ so that the equation factors as

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3$$

in $\mathbb{Z}[\sqrt{-2}]$. The ring $\mathbb{Z}[\sqrt{-2}]$ is what is called the *ring of algebraic integers* of the *number field* $\mathbb{Q}(\sqrt{-2})$. Arguing that $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are relatively prime in $\mathbb{Z}[\sqrt{-2}]$, we

get that each factor must be a cube of an element of $\mathbb{Z}[\sqrt{-2}]$. In other words, we must have

$$y + \sqrt{-2} = (a + b\sqrt{-2})^3 \quad \text{for some } a, b \in \mathbb{Z}$$

Expanding and comparing coefficients we can solve for a, b and hence x, y.

In the above "proof", when arguing that $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ must be cubes in $\mathbb{Z}[\sqrt{-2}]$, we have implicitly assumed that $\mathbb{Z}[\sqrt{-2}]$ has unique factorization into irreducibles. Given elements in $\mathbb{Z}$ has the unique factorization, can we elements in $\mathbb{Z}[\sqrt{-2}]$ In this paper, we will give a rigorous formulation of the theory of factorization of elements as well as ideals in rings of algebraic integers of number fields.

2 Preliminaries

Definition 2.1. An *algebraic number* is the root of a polynomial in $\mathbb{Q}[x]$. The algebraic numbers form a ring, which is denoted by $\overline{\mathbb{Q}}$.

Definition 2.2. A *number field* K is a subfield of $\mathbb{Q}$ of finite degree.

Theorem 2.3 (Primitive Element Theorem)**.** K is a number field iff $K = \mathbb{Q}(\alpha)$ for some algebraic number α.

Definition 2.4. An *algebraic integer* is the root of a monic polynomial in $\mathbb{Z}[x]$. The algebraic integers form a ring, which is denoted by $\overline{\mathcal{B}}$.

Definition 2.5. Let K be a number field. The *ring of algebraic integers* of K is defined to be

$$\mathfrak{O}_K = \overline{\mathcal{B}} \cap K.$$

Theorem 2.6 (Ring of Integers of Quadratic Fields)**.** Let $K = \mathbb{Q}[\sqrt{d}]$ for some squarefree integer d. Then $O_K = \{a + \omega b \mid a, b \in \mathbb{Z}\}$ where

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \pmod 4; \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Theorem 2.7 (Existence and uniqueness of the minimal polynomial)**.** If $\alpha \in K$ and K is a number field, then there exists a polynomial $m_{K/\mathbb{Q}}(\alpha)(t) \in \mathbb{Q}[t]$ of minimal degree having α as a root. This polynomial is unique and is called the *minimal polynomial* of α.

Proof. • Existence.

The set which contains all $\{\deg p \mid p \in \mathbb{Q}[t], \text{monic},\ p(\alpha) = 0\} \subset \mathbb{N}$ is not empty. By applying the well-ordering principle to $\mathbb{N}$, it must have a minimal element. Therefore the minimal polynomial must exist.

- Uniqueness.
  Suppose p and q are minimal polynomials having α as a root. Suppose $n = \deg p = \deg q$. Let $r = p - q$. Since p and q are monic, r has degree strictly less than n. Polynomial r also has α as a root, but r has degree less than n. By minimality of n, we must have $r = 0$. Thus $p = q$.

□

Definition 2.8. *A*n Euclidean Domain is a domain D with a *Euclidean function* ϕ, which is by definition a function from $D\backslash\{0\}$ to $\mathbb{N}$ such that for all $x, y \in D\backslash\{0\}$

- if $x|y$ then $\phi(x) \leq \phi(y)$;
- there exist q, $r \in D$ such that $x = qy + r$ and either $r = 0$ or $\phi(r) < \phi(y)$.

It turns out that $\mathbb{Q}[x]$ is a Euclidean domain with Euclidean function being the degree function.

Theorem 2.9. If $\alpha \in K$ and $p(\alpha) = 0$ and $p \in Q[x]$, then $m_\alpha \mid p$ in $\mathbb{Q}[x]$. In particular, m_α is irreducible over $\mathbb{Q}$.

Proof. There must exist polynominals $q(x)$ and $r(x)$ such that

$$p(x) = q(x)m_\alpha(x) + r(x)$$

where either $r = 0$ or r has degree strictly less than m_α. Suppose r is not zero. Then α is a root of p and m_α, so $r(\alpha) = 0$, contradicting the fact that p is the minimal polynomial of α. Therefore, $m_\alpha \mid p$ in $\mathbb{Q}[x]$. □

Corollary 2.9.1. Let α be an algebraic number. If $p \in \mathbb{Q}[x]$, $p(\alpha) = 0$ and p is irreducible, then $p = m_\alpha$.

Definition 2.10. Let K_1 and K_2 be two field extensions of $\mathbb{Q}$. A field homomorphism $f : K_1 \to K_2$ is called a $\mathbb{Q}$-*homomorphism* if $f(x) = x$ for all $x \in \mathbb{Q}$.

Lemma 2.11. Let $f : K_1 \to K_2$ be a $\mathbb{Q}$-homomorphism and let $m_\alpha \in \mathbb{Q}[x]$ be the minimal polynomial over $\mathbb{Q}$ of an algebraic integer $\alpha \in K_1$. Then $f(\alpha)$ is another root of m_α.

Proof. Suppose $m_\alpha(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then

$$m_\alpha(f(\alpha)) = f(\alpha^n) + f(a_{n-1}\alpha^{n-1}) + \cdots + a_0.$$

Since f is an $\mathbb{Q}$-homomorphism, we have

$$f(\alpha^n) + f(a_{n-1}\alpha^{n-1}) + \cdots + a_0 = f(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0) = 0.$$

Since α is a root of m_α, $f(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_0) = 0$. Hence, $m_\alpha(f(\alpha)) = 0$ and $f(\alpha)$ is a root of m_α. □

Definition 2.12. Suppose $\sigma_1, \cdots, \sigma_n$ are all $\mathbb{Q}$-homomorphisms from K to $\mathbb{C}$. Then the $K/\mathbb{Q}$-*norm* of α, denoted by $N_{K/\mathbb{Q}}(\alpha)$, is defined to be $\prod_{i=1}^{n} \sigma_i(\alpha)$.

It is easy to see that the norm function is multiplicative.

Lemma 2.13. Let $K = \mathbb{Q}[\sqrt{-2}]$. Then $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-2}]$ and for all $\alpha = (a + b\sqrt{-2}) \in O_K$ we have

$$N(a + b\sqrt{-2}) = a^2 - 2b^2.$$

Proof. We have $\mathfrak{O}_K = \mathbb{Z}[\sqrt{-2}]$ by Theorem 2.6. The minimal polynomial of $\sqrt{-2}$ over $\mathbb{Q}$ is $f(x) = x^2 + 2$. So by Lemma 2.11 we have two embeddings from K to $\mathbb{C}$

$$\sigma_1 : \sqrt{-2} \mapsto \sqrt{-2}$$
$$\sigma_2 : \sqrt{-2} \mapsto -\sqrt{-2}.$$

□

3 Factorization into Irreducibles

Integers in $\mathbb{Z}$ can be factorized into prime numbers and such a factorization is unique up to the order of factors. However, this notion of unique factorization generally does not carry over to all rings of integers. The reason is in the definition of prime numbers. There are two distinct properties which can serve as definitions of prime number.

(a) If p is prime then $p = ab$ implies either a or b must be a unit.

(b) If p is prime then $p|ab$ implies either $p|a$ or $p|b$.

The only units in $\mathbb{Z}$ are ± 1, which makes property (a) and (b) equivalent. This equivalence relationship holds even in algebraic number rings. But it is not true in all cases. Property (b) generally implies (a), but the converse is not true. Moreover, property (b) guarantees unique factorization into irreducibles.

In order to distinguish property (a) and (b), we call an element p an *irreducible* if p satisfies property (a), and call it a *prime* if p satisfies property (b). In fact, if factorization into primes is possible, then it can be shown that the factorization is unique. In contrast, factorization into irreducibles may not be unique even if it is possible. For example, in $\mathbb{Z}[\sqrt{-6}]$. There are two factorizations of 6: $6 = 2 \cdot 3$ and $6 = \sqrt{-6} \cdot \sqrt{-6}$. Elements 2, 3 and $\sqrt{-6}$ are all irreducible in $\mathbb{Z}[\sqrt{-6}]$; however, they are not prime.

In general a factorization into irreducibles may not be possible. In order to factor an element x in a domain D, naturally we look for proper factors a, b, such that $x = ab$, where neither a nor b is a unit. If either of these factor is reducible, we again factor it. By induction we get a factorization $x = a_1 a_2 \cdots a_n$ such that no factors can be further reduced. However, in some domains (e.g. $\mathcal{B}$) this procedure may not stop, in which case factorization into irreducibles becomes impossible. But in a ring $\mathfrak{O}_K$ of integers of any number field K,

factorization into irreducibles is always possible. We prove this fact later by introducing the notion of Noetherian rings. Every ring of integers $\mathfrak{O}_K$ is Noetherian and in a Noetherian ring, factorization into irreducibles is always possible.

Definition 3.1. An integral domain D is *Noetherian*, if every ideal in D is finitely generated.

Proposition 3.2. The following conditions are equivalent for an integral domain D:

(i) D is Noetherian;

(ii) (Ascending chain condition) Every ascending chain of ideals in D stops;

(iii) (Maximality condition) Every non-empty set of ideals in D has a maximal element.

Proof. (i) $\Longrightarrow$ (ii)

Assume D is Noetherian. Consider an ascending chain of ideals:

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots .$$

Let I be the union of all the elements in the chain, i.e., $I = \bigcup_{i=1}^{\infty} I_i$. Then I is a finitely generated ideal, since every ideal in D is finitely generated. Suppose $I = (x_1, \cdots, x_m)$. Each x_i is an element of some $I_{n(i)}$. Let M be the union of such $I_{n(i)}$'s. Then M contains $x_1, \cdots, x_m$, which implies that $M = I$. Thus the ascending chain stops.

(ii) $\Longrightarrow$ (iii)

Suppose every ascending chain of ideals in D stops. Then consider a non-empty subset $\mathfrak{S}$ of ideals in D. Suppose the set $\mathfrak{S}$ has no maximal elements. We can pick I_0 from $\mathfrak{S}$, and find I_1 such that $I_0 \subsetneqq I_1$. Inductively, if we have I_n, then we can find I_{n+1} such that $I_n \subsetneqq I_{n+1}$. Then we construct an ascending chain $I_0 \subsetneqq I_1 \subsetneqq \cdots \subsetneqq I_n \subsetneqq I_{n+1} \subsetneqq \cdots$, which never stops. This contradicts our assumption.

(iii) $\Longrightarrow$ (i)

Suppose any non-empty subset of ideals of D has a maximal element. Let I be any ideal of D and $\mathfrak{S}$ be the set of all finitely generated ideals in I. The set $\mathfrak{S}$ is not empty, since $(0) \in \mathfrak{S}$. Hence, by our assumption, $\mathfrak{S}$ has a maximal element J. If $J \neq I$, then we can find an element $x \in I \setminus J$. Then $J \subsetneqq (J, x)$ and (J, x) is also finitely generated. This contradicts the maximality of J. Therefore, $I = J$ and all ideals in D are finitely generated. □

Theorem 3.3. If a domain D is Noetherian, then factorization into irreducibles is possible in D.

Proof. Let $\mathfrak{S} = \{\langle x \rangle \mid 0 \neq x \in D, x \text{ cannot be factored into irreducibles}\}$. Suppose $\mathfrak{S}$ is nonempty. Since $\mathfrak{S}$ is a nonempty subset of the Noetherian domain D, there exists a maximal element, $\langle x \rangle$, in $\mathfrak{S}$.

This $\langle x \rangle$ itself cannot be irreducible, so we can write $x = yz$, where neither y nor z is a unit. Then $\langle x \rangle \subset \langle y \rangle$. If $\langle x \rangle = \langle y \rangle$, then $x|y$ and $y|x$. This would imply that x and y

are associates and z is a unit, which is a contradiction. Therefore, $\langle x\rangle \subsetneqq \langle y\rangle$. By the same reasoning, we have $\langle x\rangle \subsetneqq \langle z\rangle$. By maximality of $\langle x\rangle$, we have

$$y = p_1 \cdots p_r,$$

$$z = q_1 \cdots q_s,$$

where each p_i and q_j is irreducible. Then $x = yz = p_1 \cdots p_r \cdot q_1 \cdots q_s$, which is a contradiction to our condition on x. Therefore factorization into irreducibles is always possible in a Noetherian domain D. □

Now, fix a number field K. We want to show that the ring of algebraic integers $\mathfrak{O}_K$ is Noetherian and therefore has unique factorization into irreducibles. To this end, we need to use the following two theorems.

Theorem 3.4. The additive group of $\mathfrak{O}_K$ is free abelian.

Theorem 3.5. Every subgroup H of a free abelian group G of rank n is free of rank $s \leqslant n$. Moreover there exists a basis $u_1, \cdots, u_n$ for G and positive integers $\alpha_1, \cdots, \alpha_s$ such that $\alpha_1 u_1, \cdots \alpha_2 u_2, \cdots \alpha_s u_s$ is a basis for H.

Theorem 3.6. The ring of integers $\mathfrak{O}_K$ in a number field K is Noetherian. Consequently, factorization into irreducibles is possible in $\mathfrak{O}_K$.

Proof. From the above two theorems, we have that for every ideal I of $\mathfrak{O}_K$, $(I, +)$ is free abelian. If $\{x_1, \cdots, x_s\}$ is a $\mathbb{Z}$-basis for $(I, +)$, then clearly $\langle x_1, \cdots, x_s\rangle = I$, so I is finitely generated and hence $\mathfrak{O}_K$ is Noetherian. □

Remember the key step in the "proof" of Fermat's statement in the Introduction is the claim that if, in $\mathbb{Z}[\sqrt{-2}]$, the product of two relatively elements is a cube, then each is a cube. This presumes the *uniqueness* of factorization into irreducibles in $\mathbb{Z}[\sqrt{-2}]$. Thus, a natural question we should ask is: Is factorization into irreducibles in $\mathfrak{O}_K$ unique? The answer is that this is not true in general. However, it is true in the case where $\mathfrak{O}_K$ is a Euclidean domain.

The following gives a criterion for a domain to have unique factorization into irreducibles.

Theorem 3.7. In a domain in which factorization into irreducibles is possible, factorization is unique iff every irreducible is prime. In that case, the domain is called a *Unique Factorization Domain* (UFD).

Since in a UFD, all irreducibles are prime, so we may refer to a factorization into irreducibles as a "prime factorization". It turns out that every Euclidean Domain (ED) is a Principal Ideal Domain (PID) and every PID is a UFD. It turns out that $\mathbb{Z}[\sqrt{-2}] = \mathfrak{O}_K$ for $K = \mathbb{Q}[\sqrt{-2}]$ is a ED with Euclidean function $\phi(x) = |N_{K/\mathbb{Q}}(x)|$. Thus $\mathbb{Z}[\sqrt{-2}]$ is a UFD. We can now give a proof of Fermat's statement.

Lemma 3.8. A Statement of Fermat. The only integer solutions of $y^2 + 2 = x^3$ are $y = \pm 5$ and $x = 3$.[1]

Proof. First of all, y cannot be an even number, otherwise the left hand side is even which forces the right hand side to be even and x to be even. Then 8 divides the right hand side but the highest power of 2 dividing the left hand side is 1, which is a contradiction.

Factoring the equation in the ring $\mathbb{Z}[\sqrt{-2}]$, we get

$$(y + \sqrt{-2})(y - \sqrt{-2}) = x^3.$$

We claim that $(y+\sqrt{-2})$ and $(y-\sqrt{-2})$ are coprime in $\mathbb{Z}[\sqrt{-2}]$. Indeed, suppose $c+d\sqrt{-2}$, where c and $d \in \mathbb{Z}$, is a common divisor of $(y+\sqrt{-2})$ and $(y-\sqrt{-2})$, then $c+d\sqrt{-2}$ divides their sum $2y$ and their difference $2\sqrt{-2}$ as well. Taking norms on both sum and difference, we have $(c^2 + 2d) \mid 4y^2$ and $(c^2 + 2d) \mid 8$. The only solutions are $c = \pm 1$, $d = 0$, or $c = 0$, $d = \pm 1$, or $c = \pm 2$, $d = 0$. But none of these solutions are factors of $(y + \sqrt{-2})$. Hence, $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are coprime. Since $\mathbb{Z}[\sqrt{-2}]$ is an ED and hence a UFD, we must conclude that $(y + \sqrt{-2})$ and $(y - \sqrt{-2})$ are cubes. Thus for some integers a, b, we have

$$y - \sqrt{-2} = ((a + b\sqrt{-2}))^3.$$

Expanding the right hand side and comparing the coefficient of $\sqrt{-2}$ gives

$$1 = b(3a^2 - 2b^2).$$

The only solutions for this equation are $b = 1$, $a = \pm 1$. Plugging this into $y - \sqrt{-2} = ((a + b\sqrt{-2}))^3$, we have $y = \pm 5$. This gives $x = 3$. □

4 Unique Factorization of Ideals in $\mathfrak{O}_K$

The theory of unique factorization into irreducibles in the previous section, though useful, is not often applicable as not all rings of algebraic integers are ED. However, if we change the perspective from factorization of *algebraic integers* to factorization of *ideals*, then we get the following beautiful theorem. To prove this theorem, we make use of the fact that in $\mathfrak{O}_K$, every prime ideal is maximal.

Theorem 4.1. Every non-zero proper ideal $\mathfrak{a}$ of $\mathfrak{O}_K$ admits a factorization,

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

where each $\mathfrak{p}_i$ is a prime ideal, unique up to the order of factors.[2]

Proof. Before showing the existence of factorization into prime ideals in $\mathfrak{O}_K$, we want to show that at least if $\mathfrak{a}$ is a non-zero ideal of $\mathfrak{O}$, then there exist some non-zero prime ideals $\mathfrak{p}_i$'s such that $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subseteq \mathfrak{a}$.

Let $\mathfrak{S}$ be the set of all the ideals not containing any product of non-zero prime ideals. Suppose $\mathfrak{S}$ is not empty. As $\mathfrak{O}_K$ is Noetherian, $\mathfrak{S}$ has a maximal element, say $\mathfrak{a}$. The element $\mathfrak{a}$ cannot be prime, otherwise $\mathfrak{a}$ contains the prime ideal $\mathfrak{a}$. Thus there exist ideals $\mathfrak{b}$, $\mathfrak{c}$ of $\mathfrak{O}_k$ such that $\mathfrak{bc} \subseteq \mathfrak{a}$, $\mathfrak{b} \nsubseteq \mathfrak{a}$ and $\mathfrak{c} \nsubseteq \mathfrak{a}$. Let

$$\mathfrak{a}_1 = \mathfrak{a} + \mathfrak{b}, \qquad \mathfrak{a}_2 = \mathfrak{a} + \mathfrak{c}.$$

Then $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$ because $\mathfrak{a}$ is properly contained in $\mathfrak{a}_1$ and $\mathfrak{a}_2$. By maximality of $\mathfrak{a}$, $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are not in $\mathfrak{S}$. Hence, there exist $\mathfrak{p}_1, \cdots, \mathfrak{p}_t, \mathfrak{p}_{t+1}, \cdots, \mathfrak{p}_r$ such that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_t \subseteq \mathfrak{a}_1, \qquad \mathfrak{p}_{t+1} \cdots \mathfrak{p}_r \subseteq \mathfrak{a}_2.$$

Therefore

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}$$

contrary to the choice of $\mathfrak{a}$. Thus we have shown that every non-zero ideal of $\mathfrak{O}_K$ contains a product of non-zero prime ideals.

For every non-zero ideal $\mathfrak{a}$ of $\mathfrak{O}_K$, define

$$\mathfrak{a}^{-1} = \{x \in K | x\mathfrak{a} \subseteq \mathfrak{O}_K\}.$$

Next we show: (1) if $\mathfrak{a}$ is a proper ideal of $\mathfrak{O}_K$, then $\mathfrak{O}_K \subsetneqq \mathfrak{a}^{-1}$ and (2) for every non-zero ideal $\mathfrak{a}$ and every prime ideal $\mathfrak{p}$, we have $\mathfrak{a} \subsetneqq \mathfrak{a}\mathfrak{p}^{-1}$.

(1) It is clear that $\mathfrak{O}_K$ is contained in $\mathfrak{a}^{-1}$. Thus it suffices to show that there exists an element that is in $\mathfrak{a}^{-1}$ but not in $\mathfrak{O}_K$. We are going to construct such element.

We have $\mathfrak{a} \subseteq \mathfrak{q}$ for some maximal ideal $\mathfrak{q}$. Pick an element $a \in \mathfrak{q}$, such that $a \neq 0$. Let r be the smallest number such that there exist prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$, satisfying $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq (a) \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime, we must have $\mathfrak{p} | \mathfrak{p}_i$ for some i. Without loss of generality, suppose $\mathfrak{p}_i = \mathfrak{p}_1$. Because $\mathfrak{O}_K$ is a Dedekind ring, every non-zero prime ideal of $\mathfrak{O}_K$ is maximal. Hence $\mathfrak{p}_1 = \mathfrak{p}$. By the minimality of r, we have

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \nsubseteq (a).$$

Therefore we can find $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_r \setminus (a)$. So $b \notin a\mathfrak{O}_K$, which means $ba^{-1} \notin \mathfrak{O}_K$. But $b\mathfrak{p} \subseteq (a)$, i.e., $ba^{-1}\mathfrak{p} \subseteq \mathfrak{O}_K$ and thus $ba^{-1} \in \mathfrak{p}^{-1}$. Hence, $\mathfrak{O}_K \subsetneqq \mathfrak{p}^{-1}$.

(2) Let $\mathfrak{a} \neq 0$ be an ideal. As $\mathfrak{O}_K$ is Noetherian, we must have $\mathfrak{a} = (a_1, \cdots, a_m)$ for some a_i's. Let $\mathfrak{p}$ be a prime ideal. Suppose that $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{a}$, then for every $y \in \mathfrak{p}^{-1}$, for some $b_{ij} \in \mathfrak{O}_K$,

$$ya_i = \sum_j b_{ij} a_j.$$

Writing B for the matrix $(y\delta_{ij} - b_{ij})$, we have $x = (a_1, \cdots, a_m)$ is a solution to the equation $Bx = 0$. On the other hand, we have $B^*B = \det(B)I$ so multiplying B^* on both sides of $Bx = 0$, gives $\det(B)x = 0$ so $\det B = 0$. Thus y is a root of the monic polynomial

$f(X) = \det(X\delta_{ij} - b_{ij}) \in \mathfrak{O}_K[X]$. This implies $y \in \mathfrak{O}_K$. Therefore, $p^{-1} = \mathfrak{O}_K$. This is a contradiction to (1).

Now we want to use (1) and (2) to prove that every non-zero proper ideal of $\mathfrak{O}_K$ can be factored into a product of prime ideals. Suppose not every non-zero proper ideal has a factorization. Let σ be the set of non-zero proper ideals of $\mathfrak{O}_K$ which cannot factored into prime ideals. Then σ is not empty. Since $\mathfrak{O}_K$ is Noetherian, σ has a maximal element $\mathfrak{a}$. The ideal $\mathfrak{a}$ cannot be prime. Let $\mathfrak{p}$ be a prime ideal such that $\mathfrak{a} \subseteq \mathfrak{p}$. Then by (2), we have

$$\mathfrak{a} \subsetneqq \mathfrak{a}\mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{O}_K.$$

Since $\mathfrak{a}$ is the maximal element in σ, $\mathfrak{a}\mathfrak{p}^{-1}$ is not in the set. So there exist prime ideals $\mathfrak{p}_2, \cdots, \mathfrak{p}_r$ such that

$$\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Multiplying $\mathfrak{p}$ on both sides, we have

$$\mathfrak{a} = \mathfrak{p}\mathfrak{p}_2 \cdots \mathfrak{p}_r,$$

contrary to the choice of $\mathfrak{a}$.

Finally, we want to show that the factorization of $\mathfrak{a}$ into non-zero prime ideals is unique up to reordering. Suppose we have

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

for some prime ideals p_i's and q_i's. Since $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are prime for all i and j, then $\mathfrak{p}_1$ divides some factor $\mathfrak{q}_i$. Since every prime ideal in $\mathfrak{O}_K$ is maximal, by reordering, we can assume $\mathfrak{p}_1 = \mathfrak{q}_1$. Multiplying both sides of the above equation by $\mathfrak{p}_1^{-1}$, we have

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_2 \cdots \mathfrak{q}_s.$$

By induction we can see that $r = s$ and, by rearrangement, $\mathfrak{p}_i = \mathfrak{q}_i$, for all i. Therefore the factorization is unique.

□

References

[1] Ian Stewart and David Tall. *Algebraic Number Theory and Fermat's Last Theorem*. A K Peters, Natick, MA, 2002.

[2] Pierre Samuel. *Algebraic theory of numbers*. Kershaw Pub. Co., London, 1971.