# Algebraic Number Theory

Dr. Anuj Jakhar

Lectures 9-12

Indian Institute of Technology Bhilai

*anujjakhar@iitbhilai.ac.in*

June 25, 2021

# Factorisation into irreducible elements

Definition. Let $R$ be an integral domain. Then we define the following.

- An element $\alpha$ of $R$ is said to be a *unit* of $R$ if there exists $\beta \in R$ such that $\alpha\beta = 1$.
- Two elements $\alpha, \beta$ are said to be *associates* if there exists a unit $\epsilon$ of $R$ such that $\beta = \alpha\epsilon$.
- A non-zero non-unit element $\alpha$ of $R$ is said to be an *irreducible* element of $R$ if whenever $\alpha = \beta\gamma$ with $\beta, \gamma \in R$, then either $\beta$ or $\gamma$ is a unit.
- A non-zero non-unit element $\alpha$ of R is said to be a *prime* element of $R$ if whenever $\alpha | \beta\gamma$ with $\beta, \gamma \in R$, then either $\alpha | \beta$ or $\alpha | \gamma$.

Note: Every prime element is irreducible in an integral domain but the converse is not true in general.

Definitions.

- An integral domain $R$ is said to be a factorization domain if every non-zero non-unit element of $R$ can be expressed as a product of finitely many irreducible elements of $R$.
- A factorization domain $R$ is called a unique factorization domain(UFD) if whenever $p_1p_2\cdots p_r = q_1q_2\cdots q_s$ with every $p_i, q_j$ irreducible in $R$, then $r = s$ and there is a permutation $\sigma$ of $\{1, 2, \ldots, r\}$ such that $p_i$ and $q_{\sigma(i)}$ are associates for all $i = 1, 2, \ldots, r$.
- An integral domain $R$ is said to be a principal ideal domain if every ideal of $R$ is a principal ideal.

---

- Every principal ideal domain is a unique factorization domain but the converse is not true in general.
- However we shall prove in this chapter that the converse is true for the ring of algebraic integers $\mathcal{O}_K$ of an algebraic number field $K$.
- We shall also prove that each $\mathcal{O}_K$ is a factorization domain.

---

The following proposition characterizes the units of $\mathcal{O}_K$ in terms of their norms.

---

Proposition 1. Let $K$ be an algebraic number field. An element $\alpha$ of $\mathcal{O}_K$ is a unit if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

---

Remark: Recall that for an element $\alpha \in \mathcal{O}_K$ by virtue of Theorem 16 of [1-4],

$$N_{K/\mathbb{Q}}(\alpha) = (N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha))^{[K:\mathbb{Q}(\alpha)]}.$$

So by the above proposition implies that $\alpha$ is a unit of $\mathcal{O}_K$ if and only if

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \pm 1.$$

Corollary 2. Let $K$ be an algebraic number field and $\alpha$ be an element of $\mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\alpha)|$ is a prime number, then $\alpha$ is an irreducible element of $\mathcal{O}_K$.

If $\alpha$ is as in the above corollary, then it will be proved in these lectures that $\alpha$ is indeed a prime element of $\mathcal{O}_K$.

Lemma 3. If $\alpha$ is a non-zero algebraic integer belonging to an algebraic number field $K$, then the element $N_{K/\mathbb{Q}}(\alpha)/\alpha$ is an algebraic integer in $K$.

The following theorem says that $\mathcal{O}_K$ is a factorization domain.

Theorem 4. Let $K$ be an algebraic number field. Then any non-zero non-unit element $\alpha$ of $\mathcal{O}_K$ can be written as a product of finitely many irreducible elements of $\mathcal{O}_K$.

Remark. The ring $\mathcal{A}$ consisting of all algebraic integers in $\mathbb{C}$ does not have an irreducible element, because for any $\alpha \in \mathcal{A}$, $\sqrt{\alpha} \in \mathcal{A}$. In particular $\mathcal{A}$ is not a factorization domain.

**Corollary 5.** For an algebraic number field $K, \mathcal{O}_K$ has infinitely many non-associate irreducible elements.

**Note.**

- For an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ with $d$ a negative square free integer, Gauss proved that $\mathcal{O}_K$ is a UFD for $d = -1$, $-2$, $-3$, $-7$, $-11$, $-19$, $-43$, $-67$, $-163$.
- He also conjectured that these are the only nine imaginary quadratic fields $K$ for which $\mathcal{O}_K$ is a UFD. This conjecture remained open until 1966 when it was proved by Baker [Bak] and Stark [Sta].
- Gauss also conjectured that there are infinitely many real quadratic fields whose ring of algebraic integers are unique factorization domains. This conjecture is neither proved nor disproved as yet.

Now we will study properties of ideals of $\mathcal{O}_K$. We first recall some definitions.

Definition. Let $R$ be an integral domain with quotient field $F$. A subset $I$ of $F$ is called a fractional ideal of $R$ if the following three conditions are satisfied:

(i) $I$ is an additive subgroup of $F$.

(ii) For every $a \in I$ and $r \in R$, $ar \in I$.

(iii) There exists $\alpha \neq 0$ in $R$ such that $\alpha I \subseteq R$.

Note. Every ideal of $R$ is a fractional ideal of $R$, but the converse is not true. To be more specific, an ideal of $R$ will sometimes be called an **integral ideal** of $R$.

Notation. If $I, J$ are fractional ideals of $R$, then $IJ$ is defined to be the subset of $F$ consisting of all finite sums of the type $\sum\limits_i a_i b_i$ where $a_i$'s belong to $I$ and $b_i$'s belong to $J$. Note that $IJ$ is a fractional ideal of $R$ and is called the product of $I$ with $J$.

Definition. A non-zero fractional ideal $I$ of $R$ is called invertible if there exists a fractional ideal $J$ of $R$ such that $IJ = R$. Such an ideal $J$ is called (the) inverse of $I$. One can check that if inverse of $I$ exists, then it is unique. We shall denote the inverse of an ideal $I$ by $I^{-1}$.

Note that if a fractional ideal $I$ of an integral domain $R$ with quotient field $F$ is invertible, then

$$I^{-1} = \{\alpha \in F \mid \alpha I \subseteq R\}; \tag{1}$$

this holds because if $I'$ denotes the ideal on the right hand side of (1) and $J$ denotes the inverse of $I$, then clearly $J \subseteq I'$ and $I' = I'(IJ) = (I'I)J \subseteq RJ = J$.

Definition. A fractional ideal $I$ of $R$ is said to be finitely generated if there exist $a_1, \ldots, a_n$ in $I$ such that $I = Ra_1 + \cdots + Ra_n$, i.e., every $\alpha \in I$ can be written as $\alpha = r_1 a_1 + \cdots + r_n a_n$ for some $r_1, \ldots, r_n$ in $R$; in this situation $a_1, \ldots, a_n$ is called a system of generators of $I$ and we sometimes express it by writing $I = \langle a_1, \ldots, a_n \rangle$.
If a fractional ideal is generated by a single element, it is called a principal fractional ideal.

we prove the following slightly more general result of "every ideal of the ring of algebraic integers in an algebraic number field is finitely generated".

Theorem 6. Let $K$ be an algebraic number field of degree $n$. Any non-zero ideal $I$ of $\mathcal{O}_K$ is a free abelian group of rank $n$.

Corollary 7. Let $K$ be an algebraic number field. Then every ideal of $\mathcal{O}_K$ is finitely generated.

The class of commutative rings with identity in which every ideal is finitely generated is of fundamental importance in ring theory. Such rings are called *Noetherian rings* and are named after a great algebraist Emmy Noether who introduced this concept. We now state a basic proposition which gives two more equivalent conditions for a ring to be Noetherian.

**Proposition 8.**

For a commutative ring $R$ with identity, the following conditions are equivalent.

(i) Every ideal of $R$ is finitely generated.

(ii) Every ascending chain of ideals of $R$ is stationary i.e., if $I_1 \subseteq I_2 \subseteq \dots$ are ideals of $R$, then there exists $m$ such that $I_n = I_m$ for every $n \geq m$.

(iii) Every non-empty family $S$ of ideals of $R$ has a maximal element with respect to the inclusion relation i.e., there exist $J \in S$ such that $J$ is not properly contained in any member of $S$.

Recall from algebra.

An ideal $\mathfrak{p} \neq R$ of a ring $R$ is called a *prime ideal* if whenever $\alpha\beta \in \mathfrak{p}$ for $\alpha, \beta \in R$, then either $\alpha \in \mathfrak{p}$ or $\beta \in \mathfrak{p}$. An ideal $\mathfrak{m}$ of $R$ is called *maximal* if $\mathfrak{m} \neq R$ and $\mathfrak{m}$ is not properly contained in any ideal of $R$ except $R$.

Note. It can easily be seen that every maximal ideal of a commutative ring with identity is a prime ideal but the converse is not true.

For example, consider $R = \mathbb{Z}[X]$, then $\langle 2 \rangle$ is a prime ideal of $R$ but it is not maximal as $\langle 2 \rangle \subsetneqq \langle 2, X \rangle \subsetneqq \mathbb{Z}[X]$.

However the following theorem shows that the converse holds for the ring of algebraic integers of an algebraic number field.

Theorem 9. Let $K$ be an algebraic number field. Then every non-zero prime ideal of $\mathcal{O}_K$ is maximal.

Combining Corollary 9 of [1-4], Corollary 7 and the above theorem, we see that $\mathcal{O}_K$ is an integrally closed domain which is Noetherian and in which every non-zero prime ideal is maximal. This leads to the following definition.

Definition. An integral domain $R$ is called a *Dedekind domain* if $R$ is integrally closed Noetherian domain in which every non-zero prime ideal is maximal.

Note. As pointed out above $\mathcal{O}_K$ is a Dedekind domain for each algebraic number field $K$. It can be easily seen that every principal ideal domain is a Dedekind domain.

We now prove a few results regarding the factorization of ideals in a Dedekind domain which will be needed in the sequel.

---

Theorem 10. Every non-zero fractional ideal of a Dedekind domain is invertible.

---

Theorem 11. Let $R$ be a Dedekind domain. Then every non-zero proper ideal of $R$ can be written as a product of prime ideals of $R$ in one and only one way except for the order of factors.

---

Note. The converse of the above two theorems is true.

- If every non-zero fractional ideal of an integral domain $R$ is invertible, then $R$ is a Dedekind domain.
- It is also known that in an integral domain $R$, if every non-zero proper ideal $R$ can be written as a product of prime ideals of $R$, then $R$ is a Dedekind domain; the uniqueness of factorization follows from existence.
- We shall not prove the above mentioned points as these are not needed in the sequel.

We first state three lemmas which are used in the proof of Theorems 10, 11.

Lemma 12. If $R$ is a Noetherian domain and $I$ is a non-zero ideal of $R$ different from $R$, then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $R$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq I \subseteq \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$.

Lemma 13. If $R$ is a Dedekind domain, then every non-zero prime ideal $\mathfrak{p}$ of $R$ is invertible.

Lemma 14. If $R$ is a Dedekind domain, then every non-zero ideal of $R$ except $R$ is a product of prime ideals of $R$.

Now we give some corollaries of Theorems 10 and 11.

Corollary 15. The set of all non-zero fractional ideals of a Dedekind domain $R$ is a group under multiplication of ideals. This group is free abelian generated by all non-zero prime ideals of $R$.

Corollary 16. A Dedekind domain which is a unique factorization domain is a principal ideal domain.

Theorem 11 leads to the notion of the greatest common divisor (gcd) of ideals in Dedekind domains. We first recall the notion of divisibility of ideals.

---

Definition. Let $A$ and $B$ be two ideals of an integral domain $R$. We say that $A$ divides $B$ and write $A|B$ if there is an (integral) ideal $C$ of $R$ such that $B = AC$. Note that if $A$ divides $B$, then $B \subseteq A$. We shall show soon that the converse is true in a Dedekind domain $R$. But the converse is false for a general integral domain $R$ as the following example shows.

---

Example. Consider $R = \mathbb{Z}[X]$, the ring of polynomials in indeterminate $X$ with coefficients from $\mathbb{Z}$. Let $A = \langle 2, X \rangle$ and $B = \langle 2 \rangle$ be ideals of $R$. We show that $A \nmid B$. If $B = AC$ for some ideal $C$ of $R$, then $Xg(X)$ has even coefficients for each $g(X) \in C$ which implies that $g(X)$ has all even coefficients. Hence $C \subseteq 2\mathbb{Z}[X]$. Also $C \supseteq B$. So $B = C = 2\mathbb{Z}[X]$. Multiplying the equation $B = AC$ on both sides by $\langle 2 \rangle^{-1}$, we see that $R = A = \langle 2, X \rangle$ which is not so.

---

Definition. Let $A$ and $B$ be two non-zero ideals in an integral domain $R$. We say that an ideal D is the greatest common divisor (gcd) of $A$ and $B$ if $D|A$ , $D|B$ and whenever an ideal $C|A$ and $C|B$, then $C|D$. Similarly one can define the least common multiple (lcm) of ideals. Two ideals are said to be relatively prime or coprime if their gcd is $R$.

Note. gcd and lcm of two non-zero ideals always exist in a Dedekind domain in view of Theorem 11. However gcd or lcm of two non-zero elements may not exist in a Dedekind domain. Consider $R = \mathbb{Z}[\sqrt{-5}]$. It can be easily seen that $6, 3(1+\sqrt{-5})$ do not have a gcd and $2, 1+\sqrt{-5}$ have no lcm.

Theorem 17. Let $R$ be a Dedekind domain. The following hold:

(i) For fractional ideals $A, B$ of $R$, $A \subseteq B$ if and only if $A = BC$ for some integral ideal $C$ of $R$.

(ii) If $A$ and $B$ are relatively prime ideals in $R$, then $AB = A \cap B$.

(iii) If $A$ and $B$ are ideals in $R$, then $\gcd(A, B) = A + B$.

(iv) If $A$ and $B$ are ideals in $R$, then $lcm(A, B) = A \cap B$.

Definition. Let $I$ be a non-zero ideal of $R$ and $a, b$ be elements of $R$. We say that $a$ is congruent to $b$ modulo $I$ and write $a \equiv b \pmod{I}$ if $I|(a-b)R, i.e.,$ if $a - b \in I$.

**Proposition 18.** Let $R$ be a Dedekind domain and $I$ be a non-zero ideal of $R$. Let $a, b \in R$ with $a \neq 0$. Then the congruence $aX \equiv b \pmod{I}$ is solvable in $R$ if and only if $\gcd(aR, I)|bR$, which is so if and only if $b \in aR + I$.

**Proof.** In view of Theorem 17, $\gcd(aR, I)|bR$ if and only if $aR + I \supseteq bR$, which is so if and only if $b \in aR + I$. So it is enough to prove the equivalence of the first and the last assertions of the proposition, which can be easily verified.

**Corollary 19.** Let $\mathfrak{p}$ be a non-zero prime ideal in a Dedekind domain $R$. Let $a \in R \setminus \mathfrak{p}$, then for every natural number $n$, the congruence $aX \equiv b \pmod{\mathfrak{p}^n}$ is solvable for each $b$ belonging to $R$.

**Proof.** In view of the above proposition, it is enough to verify that $\gcd(aR, \mathfrak{p}^n) = R$. Clearly $\gcd(aR, \mathfrak{p}^n) = \mathfrak{p}^j$ for some $j, 0 \leq j \leq n$. If $j > 0$, then $\mathfrak{p}^j|aR$. So $\mathfrak{p}^j \supseteq aR$. This implies that $a \in \mathfrak{p}^j \subseteq \mathfrak{p}$ , a contradiction. So $j = 0$ and $\gcd(aR, \mathfrak{p}^n) = R$.

We shall use the following theorem which is named after a classical theorem of elementary number theory.

Theorem 20 (Chinese Remainder Theorem). Let $I_1, \ldots, I_m$ be ideals of a commutative ring $R$ with identity such that $I_i + I_j = R$ for $i \neq j, 1 \leq i, j \leq m$. Then given $x_1, \ldots, x_m$ in $R$, there exists $x \in R$ such that $x \equiv x_j \pmod{I_j}$ for $1 \leq j \leq m$.

Note. In Dedekind domains, Generalized Chinese Remainder Theorem holds which is as follows:
Let $I_1, \ldots, I_m$ be ideals of a Dedekind domain $R$, then for given $x_1, \ldots, x_m$ belonging to $R$, there exists $x \in R$ such that $x \equiv x_i \pmod{I_i}$ for $1 \leq i \leq m$ if and only if $x_i - x_j \in I_i + I_j$ for each pair $i, j$, $1 \leq i, j \leq m$.

The following corollary describes an important property of ideals of a Dedekind domain. It is stronger than saying that every non-zero ideal is invertible. Corollary 21. If $I$ and $J$ are non-zero ideals of a Dedekind domain $R$, then there exists an ideal $A$ of $R$ such that $\gcd(A, IJ) = R$ and $AI$ is principal.

The following corollary sharpens the fact that every Dedekind domain is Noetherian.

Corollary 22. Let $I$ be an ideal of a Dedekind domain $R$. Given any non-zero $x \in I$, there exists $y \in I$ such that $I$ is the ideal generated by $x$ and $y$.

# Norm of an ideal

We now introduce the notion of norm of non-zero ideals in a Dedekind domain.

Definition. Let $R$ be a Dedekind domain and $I$ be a non-zero ideal in $R$. The number of elements of $R/I$ is called the norm of $I$ and is denoted by $N(I)$. A Dedekind domain $R$ is said to have finite norm property if $R/I$ is a finite ring for every non-zero ideal $I$ of $R$.

Example. If $K$ is an algebraic number field, then $\mathcal{O}_K$ has finite norm property in view of Theorem 6 and Lemma 10.

Example. For any infinite field $F$, the ring $F[X]$ of polynomials in an indeterminate $X$ (which is a PID and hence a Dedekind domain) does not have finite norm property.

**Lemma 23.** Let $R$ be a Dedekind domain and $I$ be a non-zero ideal in $R$. Write $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$ as a product of powers of distinct prime ideals, then the factor ring $R/I$ is isomorphic to $R/\mathfrak{p}_1^{a_1} \oplus \cdots \oplus R/\mathfrak{p}_r^{a_r}$.

We shall now prove that norm is multiplicative.

**Lemma 24.** If $\mathfrak{p}$ is a non-zero prime ideal in a Dedekind domain $R$, then $R/\mathfrak{p}$ is isomorphic to $\mathfrak{p}^m/\mathfrak{p}^{m+1}$ as an additive group for $m \geq 1$.

**Theorem 25.** For a Dedekind domain $R$ with finite norm property, the following hold :

(i) If $I, J$ are non-zero ideals of $R$, then $N(IJ) = N(I)N(J)$.

(ii) For a given positive integer $t$, the number of ideals $I$ of $R$ satisfying $N(I) \leq t$ is finite.

Definition. Let $R$ be Dedekind domain with finite norm property and $I$ be a non-zero fractional ideal of $R$. Suppose that $I = AB^{-1}$, where $A, B$ are (integral) ideals, we define $N(I) = N(A)/N(B)$.
This is well defined, because if $I = AB^{-1} = A_1 B_1^{-1}$, then $AB_1 = A_1 B$ and hence $N(A)N(B_1) = N(A_1)N(B)$.

Using the notion of norm of ideals, we now prove the analogues of Fermat's little theorem and Euler's theorem for Dedekind domains with finite norm property.

Generalized Fermat's Theorem. Let $R$ be a Dedekind domain with finite norm property. If $\mathfrak{p}$ is a non-zero prime ideal in $R$, then $x^{N(\mathfrak{p})} \equiv x \pmod{\mathfrak{p}}$ for every $x$ belonging to $R$. Moreover $N(\mathfrak{p})$ is the smallest positive integer amongst integers $n \geq 2$ such that $x^n \equiv x \pmod{\mathfrak{p}}$ for every $x \in R$.

Generalized Euler's Theorem. Let $R$ be a Dedekind domain with finite norm property. For any non-zero ideal $I$ of $R$, let $\phi(I)$ denote the number of invertible elements of the ring $R/I$. Then $\phi(I) = N(I) \prod_{\mathfrak{p}|I} \left(1 - \frac{1}{N(\mathfrak{p})}\right)$, where the product extends over all prime ideals dividing $I$.

Lemma 26. Let $\mathfrak{p}$ be a non-zero prime ideal of a Dedekind domain $R$, then $R/\mathfrak{p}^{n-1}$ and $\mathfrak{p}/\mathfrak{p}^n$ are isomorphic as additive groups for $n \geq 2$.

Corollary 27. If $I$ and $J$ are coprime ideals of a Dedekind domain $R$, then $\phi(IJ) = \phi(I)\phi(J)$.

The following proposition describes the norm of principal ideals of $\mathcal{O}_K$.

Proposition 27. Let $K$ be an algebraic number field. For any non-zero element $\alpha$ of $K$, $N(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$.

By virtue of the fact that if norm of an ideal $I$ is a prime number, then $I$ is a prime ideal, the following corollary is an immediate consequence of the above proposition.

---

Corollary 28. Let $\alpha$ be an algebraic integer belonging to an algebraic number field $K$ such that $|N_{K/\mathbb{Q}}(\alpha)|$ is a prime number, then $\alpha$ is a prime element of $\mathcal{O}_K$.

---

In view of the above corollary, it can be easily seen that $1-\omega$ and $1+2\omega$ are prime elements in the ring $\mathbb{Z}[\omega]$, where $\omega = (-1+\sqrt{-3})/2$.

---

# Examples.

1. Let $K = \mathbb{Q}(\sqrt{-5})$. Then the element $\alpha := 1 + \sqrt{-5}$ can not be a prime element of $\mathcal{O}_K$.

- For otherwise $\alpha\mathcal{O}_K$ would be a prime ideal and hence its norm will be a prime power which is not so, because in view of Proposition 27, $N(\alpha\mathcal{O}_K) = 6$.
- However $\alpha$ is an irreducible element of $\mathcal{O}_K$.
- If $\alpha = \beta\gamma$ with $\beta, \gamma$ non-units of $\mathcal{O}_K$, then either $\beta$ or $\gamma$ has norm 2.
- So there exist $a, b \in \mathbb{Z}$ such that $a^2 + 5b^2 = 2$ which is impossible.

2. We show that the ideal $I = \langle 1+\sqrt{-5}, 1-\sqrt{-5}\rangle$ is a maximal ideal of the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$ and is not principal.

- As $(1+\sqrt{-5}) \in I$, so $I$ divides $\langle 1+\sqrt{-5}\rangle$ and hence by virtue of Proposition 27, $N(I)$ divides $N_{K/\mathbb{Q}}(1+\sqrt{-5}) = 6$, where $K = \mathbb{Q}(\sqrt{-5})$.
- Similarly keeping in view that $2 \in I$, we see that $N(I)$ divides 4. Hence $N(I)$ divides 2.
- We will show that $I \neq \mathbb{Z}[\sqrt{-5}]$. This will prove that $N(I) = 2$ and consequently $I$ will be a prime and hence maximal ideal of $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. If $I = \mathcal{O}_K$, then there exist $a, b, c, d$ in $\mathbb{Z}$ such that $1 = (1+\sqrt{-5})(a+b\sqrt{-5}) + (1-\sqrt{-5})(c+d\sqrt{-5})$.
- Separating the real and imaginary parts, the above equation gives
$$1 = a - 5b + c + 5d, \quad 0 = a + b - c + d.$$
- On adding these equations, we obtain $1 = 2a - 4b + 6d$, which leads to a contradiction. Hence $I \neq \mathcal{O}_K$.
- If $I$ is a principal ideal generated by an element $\alpha = a + b\sqrt{-5}$ of $\mathbb{Z}[\sqrt{-5}]$, then by Proposition 27, $2 = N(I) = N_{K/\mathbb{Q}}(\alpha) = a^2 + 5b^2$, which is not possible.

3. Let $I = \left\langle 3, 1+2\sqrt{-5} \right\rangle$ be the ideal of $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-5})$. As in the above example, it can be shown that $I$ is a maximal ideal of $\mathcal{O}_K$. We compute the inverse of the ideal $I$.

- In view of (1),

$$I^{-1} = \{\alpha \in K \mid \alpha I \subseteq \mathcal{O}_K\} = \{\alpha \in K \mid 3\alpha \in \mathcal{O}_K, (1+2\sqrt{-5})\alpha \in \mathcal{O}_K\}.$$

- Let $a + b\sqrt{-5}$ be an element of $K$ with $a, b \in \mathbb{Q}$. It can be easily seen that $3(a + b\sqrt{-5}) \in \mathcal{O}_K$ if and only if $3a, 3b \in \mathbb{Z}$. Further $(1 + 2\sqrt{-5})(a + b\sqrt{-5}) \in \mathcal{O}_K$ if and only if $a - 10b, 2a + b$ are in $\mathbb{Z}$.
- On writing $a = a'/3$ and $b = b'/3$ with $a', b' \in \mathbb{Z}$, we see that $a - 10b$ and $2a + b$ are in $\mathbb{Z}$ if and only if $a' \equiv b' \pmod 3$. So $I^{-1} = \{(a' + b'\sqrt{-5})/3 \mid a', b' \in \mathbb{Z}, a' \equiv b' \pmod 3\}$.

# Exercises

- Determine the inverse of ideal $\langle 1+\sqrt{-5}, 1-\sqrt{-5}\rangle$ of $\mathcal{O}_K$, where $K=\mathbb{Q}(\sqrt{-5})$.
- (True/False) If $I$ is a non-zero ideal of $\mathcal{O}_K$ with $N(I)$ a prime number, then $I$ is a prime ideal. Justify your answer.
- Let $I$ be a non-zero ideal of $\mathcal{O}_K$. Prove that $I$ contains $N(I)$ and if $m$ is the least positive integer in $I$, then $m$ divides $N(I)$.
- Prove that the ideal $\left\langle 1+\sqrt{-5}, 1-\sqrt{-5}\right\rangle$ is prime ideal in $\mathbb{Z}[\sqrt{-5}]$.
- Let $K=\mathbb{Q}(\theta)$, where $\theta^3-\theta-1=0$. Prove that the ideal $\langle 23, 3-\theta\rangle$ is a prime ideal in $\mathcal{O}_K$.
- Find a solution of the congruence $(\sqrt{-5})x \equiv 3 \pmod{I}$ in $\mathbb{Z}[\sqrt{-5}]$, where $I=\langle 3, 1+\sqrt{-5}\rangle$.
- (Generalized Wilson Theorem) Let $K$ be an algebraic number field. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$ and $\{\xi_1,\dots,\xi_s\}$ be a system of representatives of all non-zero distinct elements of $\mathcal{O}_K/\mathfrak{p}$. Prove that $\prod\limits_{i=1}^{s}\xi_i \equiv -1 \mod \mathfrak{p}$.