This section [1] introduces some of the results in *Algebraic Number Theory* that will be needed in the hardness proof of the ring LWE (RLWE) problem. In RLWE, proofs and computations are conducted in number fields and rings of integers, which are generalizations of the rational field $\mathbb{Q}$ and integers $\mathbb{Z}$. However, unlike elements in $\mathbb{Z}$ that can be uniquely factorized, which is an essential property that guarantees the validity of some hard computational problems such as integer factorization, elements of rings of integers are not necessarily uniquely factorizable in general. Instead we need to work with sets of elements that possess such unique factorization. As we will see in this section, the ideals of these rings of integers are natural candidates for this purpose and we will state some useful properties of the ideals. In particular, the connection with lattice theory comes from a natural mapping between these ideals of a ring of integers to full-ranked lattices that we call ideal lattices.

Algebraic Number Theory is a deep and interesting area and we do not attempt to cover all important results in this compact section. Instead, we cover only those mathematical results that are directly relevant to the future sections. Additional results that may assist the reader to better understand the main content are kept in the appendix. This section is organized as follows:

1. First, we familiarize the reader with algebraic number field, its ring of integers and ideals of the ring of integers including the generalized fractional ideals. The most important observation is that a fractional ideal can be uniquely factorized into prime ideals. This plays a significant part when employing the *Chinese Remainder Theorem* (CRT) for number fields.
2. Second, to build the geometric interpretation of these algebraic objects, we introduce canonical embedding, which maps fractional ideals to special lattices called *ideal lattices*. The embedding allows us to talk about geometric quantities of algebraic objects and enables certain features of ideal lattices that are convenient for the RLWE's proof and computations.
3. Finally, we go through dual lattices in number fields and relate them with fractional ideals.

It's worth noting that many of the concepts covered in this section are used primarily for analysis of the hardness results of the RLWE problem. As such, some readers may find it useful to first skim this section quickly to identify key concepts, and only come back for details as they work through Section **??**. The only computations that are explicitly needed in RLWE-based cryptosystems are Fast Fourier Transform operations to transform polynomials between their natural and canonical embeddings.

0.1 Ring of integers and its ideal

We have seen the LWE problem, which was defined in the integer domain $\mathbb{Z}$ and proved to be hard by reductions from hard lattice problems in the domain in $\mathbb{R}^n$. The drawback of LWE is the large public key that is a matrix of m independent length n columns vectors. The RLWE problem, which greatly reduces the key size, is defined in a more general domain, called *the ring of integers*.

Recall that an algebraic number (integer) is a complex number that is a root of a non-zero polynomial with rational (integer) coefficients. For example, $\sqrt{2}$ is a root of the polynomial $x^2 - 2$, so it is an algebraic integer. Algebraic numbers and algebraic integers generalize rational numbers and rational integers. In addition, they respectively form fields and rings just like the rational field $\mathbb{Q}$ and the integer ring $\mathbb{Z}$.

Number field

Definition 0.1.1. *An **algebraic number field** (or simply **number field**) is a finite extension of the field of rationals by algebraic numbers, i.e., $\mathbb{Q}(r_1, \ldots, r_n)$, where $r_1, \ldots, r_n$ are algebraic numbers.*

Cyclotomic field

In a special case when the element ζ_n adjoins to $\mathbb{Q}$ is an nth root of unity, which is also an algebraic number, the number field $\mathbb{Q}(\zeta_n)$ is also known as the **nth cyclotomic number field** (or **nth cyclotomic field**). This is the primary working domain for RLWE reduction from the search to decision version. In a number field K, the set of all algebraic integers forms a ring under the usual addition and multiplication operations in K. These elements form a ring and is the generalization of the ring of rational integers.

Ring of integers

Definition 0.1.2. *The **ring of integers** of an algebraic number field K, denoted by $\mathcal{O}_K$, is the set of all algebraic integers that lie in the field K.*

[1] This section is part of the work *A Tutorial Introduction to Lattice-based Cryptography and Homomorphic Encryption* by the authors Yang Li, Kee Siong Ng, Michael Purcell from the School of Computing, Australian National University @2022.

Some examples of a number field and its ring of integers are the basic $\mathbb{Q}$ and $\mathbb{Z}$, the quadratic field $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Z}[\sqrt{2}]$, the nth cyclotomic field $\mathbb{Q}(\zeta_n)$ and $\mathbb{Z}[\zeta_n]$. In general, determining the ring of integers is a difficult problem, unless for special cases, see Theorem **??** in Appendix **??**.

$\mathcal{O}_K$ is a free Z-module Basis

Since $\mathbb{Z}$ is contained in $\mathcal{O}_K$, we can also interpret $\mathcal{O}_K$ as a $\mathbb{Z}$-module. In addition, $\mathcal{O}_K$ is a free Z-module, as there always exists a $\mathbb{Z}$-basis $B = \{b_1, \ldots, b_n\} \subseteq \mathcal{O}_K$ such that every element $r \in \mathcal{O}_K$ can be written as $r = \sum_{i=1}^{n} a_i b_i$, where $a_i \in \mathbb{Z}$. The basis B is called an **integral basis** of the number field K and its ring of integers $\mathcal{O}_K$. If the basis can be written as $\{1, r, \ldots, r^{n-1}\}$ the powers of an element $r \in K$, then it is called a **power basis**. A field K always has a power basis by the Primitive Element Theorem (Appendix **??** Theorem **??**). If $K = \mathbb{Q}(\zeta_m)$ is a cyclotomic field, the power basis $\{1, \zeta_m, \ldots, \zeta_m^{\varphi(m)-1}\}$ is also an integral basis of $\mathcal{O}_K$.

0.1.1 Integral ideal

In the applications of this tutorial, we do not work with individual elements in $\mathcal{O}_K$ because they lack the unique factorization property; instead, we work with ideals of $\mathcal{O}_K$. Ideals of a ring are useful for constructing a field, for the same reason they are important in the ring of integers. Since we will generalize ideals of $\mathcal{O}_K$ to fractional ideals, we sometimes call ideals integral ideals to distinguish them.

Integral ideal

Definition 0.1.3. *Given a number field K and its ring of integers $\mathcal{O}_K$, an (**integral**) **ideal** I of $\mathcal{O}_K$ is a non-empty (i.e., $I \neq \emptyset$) and non-trivial (i.e., $I \neq \{0\}$) additive subgroup of $\mathcal{O}_K$ that is closed under multiplication by the elements in $\mathcal{O}_K$, i.e., for any $r \in \mathcal{O}_K$ and any $x \in I$, their product $rx \in I$.*

As $\mathcal{O}_K$ is commutative, we do not differentiate left and right ideals. The definition intentionally excluded the zero ideal $\{0\}$ in order to simplify the work of defining ideal division later. Since $\mathcal{O}_K$ has a $\mathbb{Z}$-basis, its ideals have $\mathbb{Z}$-bases too, which makes ideals of $\mathcal{O}_K$ free $\mathbb{Z}$-modules too. As we will see later, these bases will be mapped to bases of ideal lattices by canonical embeddings.

We now define basic arithmetic of ideals. In particular, we focus on ideal multiplication and division which then lead to prime ideals.

Recall that if I and J are ideals then the set sum $I + J = \{x + y \mid x \in I, y \in J\}$ is also an ideal. The set product $S = \{xy \mid x \in I, y \in J\}$, however, may not be an ideal because it is not necessarily closed under addition. For this reason, the **product of two ideals** I and J is defined as the set of all finite sums of products of two ideal elements:

Ideal product

$$IJ := \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I \text{ and } b_i \in J, n \in \mathbb{N} \right\},$$

By grouping all finite sums of products, the set is closed under addition. Furthermore, it is closed under multiplication by $\mathcal{O}_K$, so the product is also an ideal. Since $\mathcal{O}_K$ is commutative, ideal multiplication is commutative too.

Example 0.1.4. *Given the ring of integers $\mathcal{O}_K = \mathbb{Z}$ and two ideals $I = 2\mathbb{Z} = \{2, 4, 6, 8, \ldots, \}$ and $J = 3\mathbb{Z} = \{3, 6, 9, 12, \ldots, \}$, their product is $IJ = \{2 \cdot 3, 2 \cdot 6, 2 \cdot 3 + 2 \cdot 6, \ldots\}$.*

Since the zero ideal is excluded from the ideal definition, it is convenient to define ideal division. The intuition is the same as non-zero integer division.

Ideal division

Definition 0.1.5. *Let I and J be two ideals of $\mathcal{O}_K$. We say J **divides** I, denoted $J \mid I$, if there is another ideal $M \subseteq \mathcal{O}_K$ such that $I = JM$.*

The following theorem gives a more intuitive way of thinking about ideal division by relating division with containment.

Theorem 0.1.6. *Let I and J be two ideals of $\mathcal{O}_K$. Then $J \mid I$ if and only if $I \subseteq J$.*

The intuition of divisibility implies containment is that if $J \mid I$ then $I = JM \subseteq J$, so $I \subseteq J$. The converse may not be true in general, but is certainly true in the context of $\mathcal{O}_K$.

The standard definition of a prime ideal $I \subseteq \mathcal{O}_K$ is that it is a proper ideal such that if $xy \in I$, then either $x \in I$ or $y \in I$. The next lemma gives an alternative definition in terms of ideal containment.

Lemma 0.1.7. *An ideal I of $\mathcal{O}_K$ is prime if and only if for ideals J and K of $\mathcal{O}_K$, whenever $JK \subseteq I$, either $J \subseteq I$ or $K \subseteq I$.*

By this lemma and Theorem 0.1.6, we can define a prime ideal in analogy to a prime number.

Prime ideal **Definition 0.1.8.** *A proper ideal $I \subsetneq \mathcal{O}_K$ is **prime** if whenever $I \mid JK$, either $I \mid J$ or $I \mid K$.*

Principal ideals and maximal ideals are defined in the same way as that in general rings. An important observation is that in $\mathcal{O}_K$, prime ideals are also maximal.

Lemma 0.1.9. *All prime ideals in $\mathcal{O}_K$ are maximal.*

The proof relies on the results that the quotient of a commutative ring by a prime ideal gives an integral domain, and the quotient by a maximal ideal gives a field. See Lemma **??** in Appendix **??**. The importance of this lemma is that when working in $\mathcal{O}_K/I$, the quotient ring by a prime ideal I is a field, as implied by Proposition **??** in Appendix **??**.

The most important result of this subsection, which is also one of the main theorems in *Algebraic Number Theory*, is that ideals of $\mathcal{O}_K$ can be uniquely factorized into prime ideals. Alternatively, we say the ideals of $\mathcal{O}_K$ form a unique factorization domain.

Definition 0.1.10. *An integral domain D is a **unique factorization domain (UFD)** if every non-zero non-unit element $x \in D$ can be written as a product*

$$x = p_1 \cdots p_n$$

of finitely many irreducible elements $p_i \in D$ uniquely up to reordering of the irreducible elements.

We know $\mathbb{Z}$ is a UFD, because every integer can be uniquely factored into a prouct of prime numbers. But the extension $\mathbb{Z}(\sqrt{5})$ is not a UFD, because not every element has a unique factorization, for example $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, which can be factored in two ways. To avoid such issues, we do not work with the individual elements in $\mathcal{O}_K$, but study the ideals of $\mathcal{O}_K$, which do form a UFD because $\mathcal{O}_K$ is a Dedekind domain. (See Appendix **??** for more detail about Dedekind domain.)

UFD **Theorem 0.1.11.** *For an algebraic number field K, every proper ideal I of $\mathcal{O}_K$ admits a unique factorization*

$$I = \mathfrak{q}_1 \cdots \mathfrak{q}_k, \tag{1}$$

into prime ideals $\mathfrak{q}_i$ of $\mathcal{O}_K$.

Example 0.1.12. *When working in the 5th cyclotomic field $K = \mathbb{F}_{11}(\zeta_5)$ and $\mathcal{O}_K = \mathbb{Z}_{11}[\zeta_5]$, the ideal $I = (11)$ of $\mathcal{O}_K$ can be uniquely factorized into the product of these four prime ideals:*

$$(11) = (11, \zeta_5 - 3)(11, \zeta_5 - 9)(11, \zeta_5 - 5)(11, \zeta_5 - 4).$$

The detailed derivation is given in Example 0.1.26.

The usefulness of UFD in our context is that it gives a unique isomorphism between a quotient ring $\mathcal{O}_K/I$ and its Chinese Remainder Theorem (CRT) representation. To generalize CRT to the ring of integers $\mathcal{O}_K$, we first define coprime ideals in $\mathcal{O}_K$. Since ideals in $\mathcal{O}_K$ can be uniquely factorized, it makes sense to talk about coprimality. The standard definition is similar to coprime integers, which do not share a common divisor.

Ideal GCD **Definition 0.1.13.** *Let I and J be integral ideals of $\mathcal{O}_K$, their **greatest common divisor (GCD)** $\gcd(I, J) = I + J$.*

Coprime **Definition 0.1.14.** *Two ideals I and J in $\mathcal{O}_K$ are **coprime** if $I + J = \mathcal{O}_K$.*

In other words, two integral ideals are coprime if their sum is the entire ring of integers. For example, the integral ideals (2) and (3) in $\mathbb{Z}$ are coprime because $(2) + (3) = (1) = \mathbb{Z}$. But the integral ideals (2) and (4) are not coprime because $(2) + (4) = (2) \neq \mathbb{Z}$.

CRT in $\mathcal{O}_K$ **Theorem 0.1.15.** *Let $I_1, \ldots, I_k$ be pairwise coprime ideals in a ring of integers $\mathcal{O}_K$ and $I = \prod_{i=1}^k I_i$. Then the map*

$$\mathcal{O}_K \to (\mathcal{O}_K/I_1, \ldots, \mathcal{O}_K/I_k)$$

induces an isomorphism

$$\mathcal{O}_K/I \cong \mathcal{O}_K/I_1 \times \cdots \times \mathcal{O}_K/I_k.$$

The core element of the proof of CRT in $\mathcal{O}_K$ is to show that the kernel of the map is $I_1 \cap \cdots \cap I_k$, which is identical to $\prod_{i=1}^k I_i$ under the assumption that the ideals are pairwise coprime. The result then follows from the First Isomorphism Theorem.

By CRT in $\mathcal{O}_K$, the factorization (1) yields the isomorphism

$$\mathcal{O}_K/I \cong \mathcal{O}_K/\mathfrak{q}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{q}_k. \tag{2}$$

This isomorphism is essential for the hardness proof of RLWE. If the factorization is not unique, the same proof will not follow through. We will discuss more detail of the proof in Section **??**.

0.1.2 Fractional ideal

As briefly mentioned earlier, fractional ideals are generalizations of integral ideals and they are one of the main ingredients in the hardness proof of RLWE. On the one hand, fractional ideals share some common properties with integral ideals including the important unique factorization characteristic. On the other hand, they are neither ideals of the ring of integers $\mathcal{O}_K$ nor ideals of the number field K as we will see soon.

Fractional ideal

Definition 0.1.16. *Let K be a number field and $\mathcal{O}_K$ be its ring of integers. A **fractional ideal** I of $\mathcal{O}_K$ is a set such that $dI \subseteq \mathcal{O}_K$ is an integral ideal for a non-zero $d \in \mathcal{O}_K$.*

Given an integral ideal $J \subseteq \mathcal{O}_K$ and an invertible element $x \in K$, the corresponding fractional ideal I can be expressed as

$$I = x^{-1}J := \{x^{-1}a \mid a \in J\} \subseteq K.$$

From this expression, it is clearer that the non-zero element $d \in K$ in the above definitions is for cancelling the denominator x of elements in the fractional ideal. When $x = 1$, it entails the integral ideals of $\mathcal{O}_K$ including $\mathcal{O}_K$ itself are all fractional ideals. This is also why fractional ideals are generalizations of them. Since an integral ideal is a free $\mathbb{Z}$-module and a fractional ideal is related to an integral ideal by an invertible element, it follows that a fractional ideal is a free $\mathbb{Z}$-module too with a $\mathbb{Z}$-basis.

It can be seen that a fractional ideal is closed under addition and multiplication by the elements in $\mathcal{O}_K$, but it is NOT an ideal of $\mathcal{O}_K$, because it is not necessarily a subset of $\mathcal{O}_K$. Neither it is an ideal of the number field K, because a field has only zero and itself as ideals.

Example 0.1.17. *Let $K = \mathbb{Q}$ and $\mathcal{O}_K = \mathbb{Z}$. Given the integral ideal $5\mathbb{Z}$ and $x = 4 \in \mathbb{Q}$, whose inverse is $\frac{1}{4}$, the corresponding fractional ideal in $\mathbb{Q}$ is $\frac{5}{4}\mathbb{Z}$.*

Frac ideal product

The product of two fractional ideals can be defined analogous to the product of two integral ideals. That is, for fractional ideals I and J,

$$IJ := \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in I \text{ and } b_i \in J, n \in \mathbb{N} \right\}.$$

It is also easy to check that the product of two fractional ideals is still a fractional ideal.

The fractional ideals in a number field K form a multiplicative group. To see this, we have demonstrated that they are closed under multiplication and the unit ideal $(1) = \mathcal{O}_K$ is the multiplicative identity in the group. It remains to show that every fractional ideal has an inverse in the group. This is done via the following two lemmas. The first lemma states that every prime ideal of $\mathcal{O}_K$ has an inverse. The second lemma states that every non-zero integral ideal of $\mathcal{O}_K$ has an inverse, which uses the result of the first lemma and the fact that every prime ideal in $\mathcal{O}_K$ is also maximal. See Appendix **??** for the proofs of these two lemmas.

Lemma 0.1.18. *If P is a prime ideal in $\mathcal{O}_K$, then P has an inverse $P^{-1} = \{a \in K \mid aP \subseteq \mathcal{O}_K\}$ that is a fractional ideal.*

Lemma 0.1.19. *Every non-zero integral ideal of $\mathcal{O}_K$ has an inverse.*

Frac ideal inverse

The two lemmas combined prove that a fractional ideal has an inverse. For more detail of the proof, see Theorem 3.1.8 (Stein, 2012). To be more precise, the inverse of a fractional ideal I has the form

$$I^{-1} = \{x \in K \mid xI \subseteq \mathcal{O}_K\}. \tag{3}$$

In the special case when the product of two fractional ideals is a principal fractional ideal $IJ = (x)$, the inverse has the form $I^{-1} = \frac{1}{x}J$.

Multiplicative group

Theorem 0.1.20. *The set of fractional ideals in a number field K is an abelian group under multiplication with the identity element $\mathcal{O}_K$.*

A key result of this subsection is that a fractional ideal can also be uniquely factorized into a product of prime ideals.

UFD **Theorem 0.1.21.** *Let K be a number field. If I is a fractional ideal in K, then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ in $\mathcal{O}_K$, unique up to ordering, such that*

$$I = (\mathfrak{p}_1 \cdots \mathfrak{p}_n)(\mathfrak{q}_1 \cdots \mathfrak{q}_m)^{-1}.$$

The theorem follows from the fact that a fractional ideal has the form $I = \frac{1}{a}J$, where J is an integral ideal and $a \in \mathcal{O}_K$. Since both J and (a) are integral ideals of $\mathcal{O}_K$, Theorem 0.1.11 implies they have unique prime ideal factorization.

0.1.3 Applications in Ring LWE

As we will see in Section **??**, when working on the hardness proof of the ring LWE problem, it is easier to view the underlying ring $\mathbb{Z}[x]/(\Phi_m(x))$ as a ring of integers in a cyclotomic number field, as opposed to the (more direct) interpretation of a ring of polynomials. This perspective change in interpretation is supported by the following two results.

Theorem 0.1.22. *The ring of integers in $\mathbb{Q}(\zeta_m)$ is generated by ζ_m:*

$$\mathcal{O}_{\mathbb{Q}(\zeta_m)} = \mathbb{Z}[\zeta_m].$$

Theorem 0.1.23. *For all $m \in \mathbb{N}$, we have*

$$\mathbb{Z}[x]/(\Phi_m(x)) \cong \mathcal{O}_{\mathbb{Q}(\zeta_m)}$$

Proof. This is a direct consequence of Theorems 0.1.22 and **??**. □

We state here two technical lemmas that will be needed in the RLWE result. The first lemma shows that given two ideals $I, J \subseteq R$ of a Dedekind domain R (e.g., a ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain), it is possible to construct another ideal that is coprime with either one of them.

Lemma 0.1.24. *If I and J are non-zero integral ideals of a Dedekind domain R, then there exists an element $a \in I$ such that $(a)I^{-1} \subseteq R$ is an integral ideal coprime to J.*

Proof. Since $a \in I$, the principal ideal $(a) \subseteq I$. By Theorem 0.1.6, we have $I \mid (a)$, that is, there is an ideal $M \subseteq R$ such that $IM = (a)$, so $M = (a)I^{-1} \subseteq R$ is an ideal of R. We skip the proof of coprimality. See Lemma 5.5.2 in Stein (2012). □

The element $a \in I$ can be efficiently computable using CRT in $\mathcal{O}_K$. Hence, given two ideals in R, we can efficiently construct another one that is coprime with either one of them. This corresponds to Lemma 2.14 in Lyubashevsky et al. (2010). The next lemma is essential in the reduction from K-BDD problem to RLWE.

Lemma 0.1.25. *Let I and J be ideals in a Dedekind domain R and M be a fractional ideal in the number field K. Then there is an isomorphism*

$$M/JM \cong IM/IJM.$$

Proof. Given ideals $I, J \subseteq R$, by Lemma 0.1.24 we have $tI^{-1} \subseteq R$ is coprime to J for an element $t \in I$. Then we can define a map

$$\begin{aligned} \theta_t : K &\to K \\ u &\mapsto tu. \end{aligned}$$

This map induces a homomorphism

$$\theta_t : M \to IM/IJM.$$

First, show $ker(\theta_t) = JM$. Since $\theta_t(JM) = tJM \subseteq IJM$, then $\theta_t(JM) = 0$. Next, show any other element $u \in M$ that maps to 0 is in JM. To see this, if $\theta_t(u) = tu = 0$, then $tu \in IJM$. To use Lemma 0.1.24, we re-write it as $(tI^{-1})(uM^{-1}) \subseteq J$. Since tI^{-1} and M are coprime, we have $uM^{-1} \subseteq J$, which implies $u \subseteq JM$. Therefore, $ker(\theta_t) = JM$ and

$$\theta_t : M/JM \to IM/IJM$$

is injective.

Second, show the map is surjective. That is, for any $v \in IM$, its reduction $v \mod IJM$ has a preimage in M/JM. Since tI^{-1} and J are coprime, by CRT we can compute an element $c \in tI^{-1}$ such that $c \equiv 1 \mod J$. Let $a = cv \in tM$, then $a - v = cv - v = v(c-1) \in IJM$. Let $w = a/t \in M$, then $\theta_t(w) = t(a/t) = a \equiv v \mod IJM$. Hence, any arbitrary element $v \in IM$ satisfies the preimage of $v \mod IJM$ is $w \mod IM$. □

In the hardness proof of RLWE as will be shown in Section **??**, we can use Lemma 0.1.25 to show that for $R = \mathbb{Z}[x]/(\Phi_m(x))$, an ideal I and a prime integer q,

$$R/(q)R \cong I/(q)I$$
$$I^\vee/(q)I^\vee \cong R^\vee/(q)R^\vee,$$

where $R^\vee$ denotes the dual of R that we will define later in Section 0.3.

We end this subsection by looking at the (unique) factorisation of the ideal (q) in the ring of integers $R_q = \mathbb{Z}_q[x]/(\Phi_m(x))$. Since q is prime, the principal ideal generated by it can be split into prime ideals $\mathfrak{q}_i$ as follows:

$$(q) = \prod_{i=1}^{n/(ef)} \mathfrak{q}_i^e = \prod_{i=1}^{n/(ef)} (q, F_i(\zeta_m))^e,$$

where $n = \varphi(m)$, $e = \varphi(q')$ is the Euler totient function of q', the largest power of q that divides m, f is the multiplicative order of q modulo m/q', i.e., $q^f \equiv 1 \mod (m/q')$, and each $\mathfrak{q}_i$ is generated by two elements, the prime number q and the monic irreducible factor $F_i(x)$ of the cyclotomic polynomial $\Phi_m(x) = \prod_i (F_i(x))^e$ when splitting over $\mathbb{Z}_q[x]$ (see Theorem **??**). For details, see Chapter 4 Stein (2012).

Example 0.1.26. *For $m = 5$, the 5th cyclotomic polynomial is*

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$

so $n = 4$ and $K = \mathbb{Q}(\zeta_5)$ the 4-dimensional cyclotomic field. Let $q = 19$, then we have $q' = 19^0 = 1$ to be the largest power of q that divides 5. So $e = \varphi(1) = 1$ and the multiplicative order of $19 \mod (4/1)$ is $f = 2$. Assuming we are given how the cyclotomic polynomial splits in $\mathbb{Z}_{19}[x]$, i.e.,

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = (x^2 + 5x + 1)(x^2 + 15x + 1),$$

then we can split the ideal into prime ideals in the ring of integers $R = \mathbb{Z}[\zeta_5]$ as

$$(q) = \mathfrak{q}_1\mathfrak{q}_2$$
$$\implies (19) = (19, (\zeta_5)^2 + 5\zeta_5 + 1)(19, (\zeta_5)^2 + 15\zeta_5 + 1).$$

If we further restrict $q \equiv 1 \mod m$, it follows that $f = 1$. In addition, it also entails that $q' = 1$ and $e = 1$. In addition, the cyclotomic polynomial $\Phi_m(x) = x^n + 1$ can be split into n linear factors $(x - \omega^i)$, where ω^i is a primitive mth root of unity in $\mathbb{Z}_q$. This satisfies the condition of Theorem **??** for q and m being coprime.[2] Hence, the ideal can be factored as

$$(q) = \prod_{\substack{i=1,\dots,m \\ \gcd(i,m)=1}} (q, \zeta_m - \omega^i)$$
$$= \prod_{i \in \mathbb{Z}_m^*} (q, \zeta_m - \omega^i).$$

Note the index i is not any integer between 1 and m, but those coprime with m. So for the above example, when $q = 11 \cong 1 \mod 5$, the polynomial splits in $\mathbb{Z}_{11}[x]$ as

$$\Phi_5(x) = (x - 3)(x - 9)(x - 5)(x - 4),$$

where each 3, 9, 5, 4 is a primitive 5th root of unity in $\mathbb{Z}_{11}$, generated by the 1st, 2nd, 3rd and 4th power of 3 in $\mod 11$. So the ideal splits as

$$(q) = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3\mathfrak{q}_4$$
$$\implies (11) = (11, \zeta_5 - 3)(11, \zeta_5 - 9)(11, \zeta_5 - 5)(11, \zeta_5 - 4).$$

[2] Note this also works if $q = p^k$ is a prime power coprime with m.

0.2 Number field embedding

Similar to LWE, the RLWE problem's hardness is also based on hard lattice problems, except these are special lattices called *ideal lattices*. In this subsection, we will study how algebraic objects such as ring of integers and its ideals are mapped to full-ranked lattices via embeddings. The embedding we will build is from a number field K to the n-dimensional Euclidean space $\mathbb{R}^n$ or a space H that is isomorphic to $\mathbb{R}^n$. As $\mathcal{O}_K$ and its ideals are additive groups, our embedding must preserves the additive group structure of these objects.

As a degree n polynomial can be uniquely identified by its coefficients, our naive choice of embedding is by sending a polynomial $f = a_0 + a_1 x + \cdots a_{n-1}x^{n-1}$ to a coefficient vector $(a_0, a_1, \cdots, a_{n-1}) \in \mathbb{R}^n$. This coefficient embedding is clearly an additive ring homomorphism and hence satisfies our basic requirements. Furthermore, it is related by a linear transformation to the canonical embedding that will be introduced next. However, the RLWE's proof and computations do not use the coefficient embedding. We list some reasons here and leave the details to Section **??**.

- Firstly, when working with cyclotomic fields, the canonical embedding makes both polynomial addition and multiplication efficient component-wise operations (under the point-value representation). These operations have simple geometric interpretations that lead to tight bounds.
- Secondly, in the coefficient embedding, specifying the error distribution in RLWE, which is an n-dimensional Gaussian, requires an n-by-n covariance matrix in general. With the canonical embedding, the error distribution in RLWE takes the simple form of a product of one-dimensional Gaussians. This dramatically decreases the number of parameters that need to be taken care of when working with RLWE.
- Finally, the canonical embedding makes the Galois automorphisms simply permutations of the embedded vector components. This is important for the reduction from decision to search RLWE, and is not possible with the coefficient embedding.

0.2.1 Canonical embedding

Let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/(f)$, where α is a primitive element of the field (by Theorem **??**) and f is its minimal polynomial of degree n. We now look at an alternative embedding of K into $\mathbb{C}^n$. Since f is monic and irreducible in $\mathbb{Q}[x]$, and $\mathbb{Q}$ has characteristic 0, f is separable by Theorem **??** so it has n distinct roots $\{\alpha_1, \ldots, \alpha_n\}$. For each root α_i, we define a map σ_i from K to $\mathbb{C}$ sending α to α_i by

$$\begin{aligned}&\sigma_i : K \to \mathbb{Q}(\alpha_i) \subseteq \mathbb{C}\\ &\sigma_i(a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1}) = a_0 + a_1\alpha_i + a_2\alpha_i^2 + \cdots + a_{n-1}\alpha_i^{n-1},\end{aligned}$$

where $a_i \in \mathbb{Q}$. Note that σ_i fixes $\mathbb{Q}$ in that $\sigma_i(x) = x$ for all $x \in \mathbb{Q}$ and $f(\sigma_i(\alpha)) = 0$ so σ_i is an automorphism (of the field extension). One can show that $\{\sigma_i\}_{i=1}^n$ are the only embeddings of K into $\mathbb{C}$, which implies the embeddings are independent of the choice of the primitive element α.

Since the roots of f consist of real and complex numbers, we can distinguish these embeddings as real and complex embeddings. If $\sigma_i(\alpha) \in \mathbb{R}$, then it is a **real embedding**, otherwise it is a **complex embedding**. By the Complex Conjugate Root Theorem, which states that the complex roots of real coefficient polynomials are in conjugate pairs, we know the images of the complex embeddings are in conjugate pairs. Let s_1 be the number of real embeddings and s_2 be the number of conjugate pairs of complex embeddings, then the total number of embeddings is $n = s_1 + 2s_2$. Let $\{\sigma_i\}_{i=1}^{s_1}$ be the real and $\{\sigma_j\}_{j=s_l+1}^{n}$ be the complex embeddings, where $\sigma_{s_1+j} = \overline{\sigma_{s_1+s_2+j}}$ are in the same conjugate pair for each $j \in [1, \ldots, s_2]$, then we have the following definition of a canonical embedding.

Canonical embedding

Definition 0.2.1. *A **canonical embedding** σ of an n-dimensional number field K is defined as*

$$\begin{aligned}&\sigma : K \to \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} \subseteq \mathbb{C}^{s_1} \times \mathbb{C}^{2s_2} \cong \mathbb{C}^n\\ &\sigma(r) \mapsto (\sigma_1(r), \ldots, \sigma_{s_1}(r), \sigma_{s_1+1}(r), \ldots, \sigma_{s_1+2s_2}(r)).\end{aligned} \tag{4}$$

Canonical space

By its definition, the canonical embedding maps a number field to an n-dimensional space, named **canonical space**, which is expressed as

$$H = \left\{(x_1, \ldots, x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} \mid x_{s_1+j} = \overline{x_{s_1+s_2+j}}, \text{ for all } j \in [s_2]\right\}.$$

The canonical space H can be shown to be isomorphic to $\mathbb{R}^n$ by establishing a one-to-one correspondence between the standard basis of $\mathbb{R}^n$ and a basis of H as the row vectors in the following matrix

$$B = \begin{pmatrix} I_{s_1 \times s_1} & 0 & 0 \\ 0 & I_{s_2 \times s_2} & iI_{s_2 \times s_2} \\ 0 & I_{s_2 \times s_2} & -iI_{s_2 \times s_2} \end{pmatrix}.$$

The matrix $I_{s_1 \times s_1}$ is the s_1 by s_1 identity matrix.[3] The image $\sigma(r) \in H$ can then be written in terms of this basis as a real vector

$$\begin{aligned} \tau(r) = (&\sigma_1(r), \ldots, \sigma_{s_1}(r), \\ &Re(\sigma_{s_1+1}(r)), \ldots, Re(\sigma_{s_1+s_2}(r)), Im(\sigma_{s_1+1}(r)), \ldots, Im(\sigma_{s_1+s_2}(r))) \end{aligned} \tag{5}$$

by taking the real and complex parts from two conjugate complex embeddings respectively. Taking the dot product of each row vector in B with $\tau(r)$, we get back to $\sigma(r)$ in Equation 4, that is,

$$\sigma(r) = B \cdot (\tau(r))^T.$$

Here are some examples to illustrate canonical embedding, canonical space and its basis.

Example 0.2.2. *When $K = \mathbb{Q}(\sqrt{2})$ is a quadratic field. The minimal polynomial of $\sqrt{2}$ is $x^2 - 2$, which has two roots $\pm\sqrt{2}$. The canonical embedding consists two real embeddings only and is defined as*

$$\sigma(\sqrt{2}) = (\sqrt{2}, -\sqrt{2}).$$

The basis of the canonical space H is

$$B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Given the integral basis $\{1, \sqrt{2}\}$ of K, the basis vectors are mapped to the canonical space H and can be written in terms of the basis of H as real vectors

$$\begin{aligned} \tau(1) &= (1, 1) \\ \tau(\sqrt{2}) &= (\sqrt{2}, -\sqrt{2}), \end{aligned}$$

which form a $\mathbb{Z}$-basis of the image $\sigma(\mathcal{O}_K)$, that is, $\sigma(\mathcal{O}_K) = \{a(1,1) + b(\sqrt{2}, -\sqrt{2}) \mid a, b \in Z\}$.

Example 0.2.3. *When $K = \mathbb{Q}(\zeta_8)$ is the 8th cyclotomic field. The 8th primitive root of unity $\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$ and its minimal polynomial is the 8th cyclotomic polynomial $\Phi_8(x) = x^4 + 1$. The roots of $\Phi_8(x)$ are*

$$\begin{aligned} \zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},\ \zeta_8^3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \\ \zeta_8^5 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2},\ \zeta_8^7 = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}. \end{aligned}$$

The canonical embedding consists of exactly four complex embeddings, i.e., $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$,

$$\begin{aligned} \sigma_1\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},\ \sigma_2\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \\ \sigma_3\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2},\ \sigma_4\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right) = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \end{aligned}$$

where $\sigma_1 = \overline{\sigma_3}$ and $\sigma_2 = \overline{\sigma_4}$ are in conjugate pairs. The basis of the canonical space H is

$$B = \begin{pmatrix} 1 & 0 & i & 0 \\ 0 & 1 & 0 & i \\ 1 & 0 & -i & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

[3] Note in Lyubashevsky et al. (2010), the row vectors are multiplied by $\frac{1}{\sqrt{2}}$ to make them an orthonormal basis, i.e., B is a unitary matrix (i.e., $BB^* = I$, where B^* is B's conjugate transpose).

By Equation 5, the canonical embedding of the primitive element ζ_8 can be written in terms of this basis as the real vector

$$\tau\left(\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}\right)=(Re(\sigma_1),Re(\sigma_2),Im(\sigma_1),Im(\sigma_2))=\left(\frac{\sqrt{2}}{2},-\frac{\sqrt{2}}{2},\frac{\sqrt{2}}{2},\frac{\sqrt{2}}{2}\right).$$

By multiplying each row of B with this expression, we get back to the canonical embedding $\sigma = (\sigma_1,\sigma_2,\sigma_3,\sigma_4)$.

L_p*-norm*

Given the canonical embedding, it allows us to talk about the geometric norm of an algebraic element $x \in K$. More precisely, we can define the L_p**-norm** of x by looking at the L_p-norm of its image $\sigma(x)$ that is embedded into the real space $\mathbb{R}^n$

$$||x||_p = ||\sigma(x)||_p = \begin{cases} \left(\sum_{i\in[n]} |\sigma_i(x)|^p\right)^{1/p} & \text{if } p<\infty, \\ \max_{i\in[n]} |\sigma_i(x)| & \text{if } p=\infty. \end{cases} \tag{6}$$

In the next example, we illustrate the L_p-norm of a root of unity in a cyclotomic field.

Example 0.2.4. *Let $K=\mathbb{Q}(\zeta_n)$ be the nth cyclotomic field and $\sigma: K \to H$ be its canonical embedding. The cyclotomic polynomial $\Phi_n(x)$ is the minimal polynomial of ζ_n and it has only complex roots for $n \geq 3$, as the two real roots are non-primitive. Since the Galois group $Gal(K/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$ is isomorphic to the multiplicative group (Theorem* **??***), the complex embeddings are given by $\sigma_i(\zeta_n)=\zeta_n^i$ for $i \in (\mathbb{Z}/n\mathbb{Z})^*$ and $n=2s_2=|(\mathbb{Z}/n\mathbb{Z})^*|$. Since the primitive roots of unity are closed under σ_i, the magnitude $|\sigma_i(\zeta_n^j)|=1$. So the L_P-norm of an nth root of unity is $||\zeta_n^j||_p = n^{1/p}$ for $p<\infty$ or $||\zeta_m^j||_\infty = 1$.*

We have shown that the canonical embedding σ sends a number field to a space isomorphic to $\mathbb{R}^n$. When restricted to the ring of integers $\mathcal{O}_K$ that is closed under addition, we would like to see what σ does to preserve the discreteness and the additive group structure of $\mathcal{O}_K$. The following theorem states that the canonical embedding maps $\mathcal{O}_K$ to a full-rank lattice.

$\tau(\mathcal{O}_K)$ *is lattice*

Theorem 0.2.5. *Let K be an n-dimensional number field, then $\sigma(\mathcal{O}_K)$ is a full-rank lattice in $\mathbb{R}^n$.*

Proof. Let $\{e_1,\ldots,e_n\}$ be an integral basis of $\mathcal{O}_K$, then every element $x \in \mathcal{O}_K$ can be written as $x=\sum_{i=1}^n z_i e_i$, where $z_i \in Z$. The embedding of x can then be written as $\sigma(x)=\sum_{i=1}^n z_i\sigma(e_i)$, where the coefficients are fixed because σ fixes $\mathbb{Q}$. Hence, $\sigma(\mathcal{O}_K)$ is also a $\mathbb{Z}$-module generated by $\{\sigma(e_1),\ldots,\sigma(e_n)\}$.

By definition, a lattice is a free $\mathbb{Z}$-module. If we can show $\{\sigma(e_1),\ldots,\sigma(e_n)\}$ is a basis of $\sigma(\mathcal{O}_K)$, then $\sigma(\mathcal{O}_K)$ is a free $\mathbb{Z}$-module. To do so, write each $\sigma(e_i)$ in terms of the canonical space basis according to Equation 5 as a real vector, so we have the following basis matrix for $\sigma(\mathcal{O}_K)$

$$N^T = \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_{s_1}(e_1) & Re(\sigma_{s_1+1}(e_1)) & \cdots & Re(\sigma_{s_1+s_2}(e_1)) & Im(\sigma_{s_1+1}(e_1)) & \ldots & Im(\sigma_{s_1+s_2}(e_1)) \\ \vdots & & \vdots & \vdots & & & \vdots & & \\ \sigma_1(e_n) & \cdots & \sigma_{s_1}(e_n) & Re(\sigma_{s_1+1}(e_n)) & \cdots & Re(\sigma_{s_1+s_2}(e_n)) & Im(\sigma_{s_1+1}(e_n)) & \ldots & Im(\sigma_{s_1+s_2}(e_n)) \end{pmatrix}.$$

Then show that the matrix has a non-zero determinant, and consequently the rows are independent. By Equation 4 of canonical embedding, we can write the images of the integral basis $\{e_1,\ldots,e_n\}$ under the canonical embedding as the matrix

$$M^T = \begin{pmatrix} \sigma_1(e_1) & \cdots & \sigma_{s_1}(e_1) & \sigma_{s_1+1}(e_1) & \overline{\sigma_{s_1+1}}(e_1) & \cdots & \sigma_{s_1+s_2}(e_1) & \overline{\sigma_{s_1+s_2}}(e_1) \\ \vdots & & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \sigma_1(e_n) & \cdots & \sigma_{s_1}(e_n) & \sigma_{s_1+1}(e_n) & \overline{\sigma_{s_1+1}}(e_n) & \cdots & \sigma_{s_1+s_2}(e_n) & \overline{\sigma_{s_1+s_2}}(e_n) \end{pmatrix}.$$

The two matrices are of the same dimension and their determinants are related by

$$\det N = \frac{1}{2^{s_2}} \det M, \tag{7}$$

so it remains to show $\det M \neq 0$. If a rational matrix A changes a basis of K to another basis by

$$e'_j = \sum_k A_{kj} e_k,$$

then the above matrix M is also changed to a new matrix $M' = MA$. We know K always has a power basis $\{1, r, \ldots, r^{n-1}\}$ (Theorem **??**) and the matrix M^T in terms of the power basis is a *Vandermonde matrix* with a non-zero determinant as the powers of r are all distinct. Then we can conclude that the above matrix M has non-zero determinant and so does the matrix N. □

An important corollary of Theorem 0.2.5 is that every fractional ideal of K is also mapped to a full-rank ideal.

Corollary 0.2.6. *If I is a fractional ideal in an n-dimensional number field K, then $\sigma(I)$ is a full-rank lattice in $\mathbb{R}^n$.*

Proof. Given I is a fractional ideal in K, for a non-zero integer $m \in K$ we have $m\mathcal{O}_K \subseteq I \subseteq \frac{1}{m}\mathcal{O}_K$, and both the subset and superset of I are full-rank lattices in $\mathbb{R}^n$, so is I. See Lemma 7.1.8 in Stein (2012) for more detail. □

As mentioned earlier, the canonical embedding allows polynomial addition and multiplication to be done component-wise efficiently, which is a convenient feature for both the deduction from search to decision RLWE and polynomial computations. We explain next why such a nice feature comes with the canonical embedding. We know a polynomial can be uniquely represented by both the coefficient and point-value representations, and the latter allows us to multiply two polynomials component-wise Cormen et al. (2001). To allow efficient transformation $O(n \log n)$ between the two representations, we should evaluate a degree n polynomial at the n-th roots of unity, which is essentially what *fast Fourier transform* (FFT) does. We know both the n-th cyclotomic field K and its ring of integers $\mathcal{O}_K$ have a power basis $B = \{1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}\}$, which consists of the n-th roots of unity just as we need. We can use the power basis to build a Vandermonde matrix M^T. Since K can also be interpreted as a polynomial ring quotient by the ideal (f), an element $a \in K$ can be viewed as $a(x) = \sum_{i=0}^{n-1} a_i x^i$ and its image under the embedding is $\sigma_i(a(x)) = a(\sigma_i(x))$. Hence, each embedding $\sigma_i(a(x))$ is equivalent to evaluate $a(x)$ at $\sigma_i(x)$. Therefore, we have

$$M^T \cdot (a_0, \ldots, a_{n-1})^T = \sigma(a) = B \cdot (\tau(a))^T.$$

Therefore, for a polynomial $a \in \mathcal{O}_K$, its image $\sigma(a)$ (or $\tau(a)$ in terms of the basis B) is precisely its point-value representation evaluated at the n-th roots of unity.

In short, when using the canonical embedding, the image of K is a lattice with a power basis consisting of the primitive roots of unity. Since each element in K is also a polynomial, when converting to the point-value representation, the primitive roots of unity are the precise points that are needed. So adding or multiplying two polynomials in the point-value representation is equivalent to adding or multiplying two elements $\sigma(K)$ w.r.t. the power basis.

0.2.2 Geometric quantities of ideal lattice

We know from the previous subsection that a fractional ideal I in a number field is mapped by a canonical embedding σ to a lattice in the Euclidean space, called *ideal lattice*. In this subsection, we will go through some geometric quantities of I (i.e., its ideal lattice $\sigma(I)$) including its determinant and minimum distance. The results in this subsection are directly related to the gap (or approximation) factors of hard ideal lattice problems.

To begin with, we first state the main result that is directly relevant to the RLWE's hardness proof. Recall that the minimum distance $\lambda_1(L)$ of a lattice L is the length of the shortest non-zero vector in L, where the length is measured by L_p-norm as defined in Equation 6.

Lemma 0.2.7. *Let I be a fractional ideal in an n-dimensional number field K, then its minimum distance measured by L_p-norm satisfies*

$$n^{1/p} \cdot N(I)^{1/n} \leq \lambda_1(I) \leq n^{1/p} \cdot N(I)^{1/n} \cdot \sqrt{\Delta_K^{1/n}}. \tag{8}$$

Here, $N(I)$ is the norm of the fractional ideal and Δ_K is the discriminant of the number field K. We will introduce these concepts next, which not only helps to understand the lemma, but give insights about the algebraic structures of $\mathcal{O}_K$ and its ideals under the canonical embedding.

Given a subgroup H of G, the Lagrange's Theorem says that the order of G satisfies $|G| = |G : H||H|$, where $|G : H|$ is the index of H that measures the number of cosets of H in G. If H is a normal subgroup, then the index is equivalent to the order of the quotient group G/H. Since an ideal I of $\mathcal{O}_K$ is an additive normal subgroup and it has a geometric interpretation due to the canonical embedding, we relate its index to the norm as next.

Ideal norm

Definition 0.2.8. *Let I be a non-zero ideal of $\mathcal{O}_K$. The **norm** of I, denoted by $N(I)$, is the index of I as a subgroup of $\mathcal{O}_K$, i.e., $N(I) = |\mathcal{O}_K/I|$.*

As for the norm of number field elements (Appendix **??**), the norm of ideals is also multiplicative. That is, $N(IJ) = N(I)N(J)$. If $I = J/d$ is a fractional ideal in K with the integral ideal J, then its norm is

$$N(I) = N(dI)/|N(d)| \tag{9}$$

Example 0.2.9. *When $\mathcal{O}_K = \mathbb{Z}$, the integral ideal $J = 5\mathbb{Z}$ and the fractional ideal $I = J/4 = \frac{5}{4}\mathbb{Z}$, the norm $N(I) = N(J)/|N(4)| = 5/4$.*

For the fractional ideal I and integral ideal dI with $d \in \mathcal{O}_K$, we have $dx \in dI$ for any non-zero $x \in I$. Hence, when viewed as subgroups, their indices satisfies $[\mathcal{O}_K : (dx)] \geq [\mathcal{O}_K : dI]$ and it follows $N(dx) \geq N(dI)$. By Equation 9 and the multiplicity of norm, we have $N(x) \geq N(I)$ for any non-zero $x \in I$. Combine this with Equation 6 of L_p-norm, we can prove the lower bound of $\lambda_1(I)$. The upper bound is proved by the discriminant of K and Minkowski's First Theorem (Theorem **??**; see also Lemma 6.1 Peikert and Rosen (2007) for the proof of the upper bound).

The discriminant of a number field loosely speaking measures the size of the ring of integers $\mathcal{O}_K$. Without loss of generality, for the basis elements $e_1, \ldots, e_n$ of K, define the n by n matrix

$$M = \begin{pmatrix} \sigma_1(e_1) & \sigma_1(e_2) & \cdots & \sigma_1(e_n) \\ \sigma_2(e_1) & \sigma_2(e_2) & \cdots & \sigma_2(e_n) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_n(e_1) & \sigma_n(e_2) & \cdots & \sigma_n(e_n) \end{pmatrix},$$

where $\sigma = (\sigma_1, \ldots, \sigma_n)$ is the canonical embedding of K. By the same argument in the proof of Theorem 0.2.5, we know the determinant of M is non-zero. We know this matrix is related to the basis matrix N of the ideal lattice and their determinants satisfy Equation 7. This matrix looks just like the basis matrix for a lattice that was introduced in Section **??**. Now we are ready to define the discriminant of K.

Δ_K

Definition 0.2.10. *Let K be an n-dimensional number field with an integral basis $\{e_1, \ldots, e_n\}$. The **discriminant** of K is*

$$\Delta_K = disc_{K/\mathbb{Q}}(e_1, \ldots, e_n) = \det(M)^2.$$

An important property of number field discriminant is that it is invariant under the choice of an integral basis. This can be seen from the following lemma and corollary.

Lemma 0.2.11. *Suppose $x_1, \ldots, x_n, y_1, \ldots, y_n \in K$ are elements in the number field and they are related by a transformation matrix A, then*

$$disc_{K/\mathbb{Q}}(x_1, \ldots, x_n) = det(A)^2 disc_{K/\mathbb{Q}}(y_1, \ldots, y_n).$$

Since the change of integral basis matrix A is an unimodular matrix, i.e., $\det A = \pm 1$, we conclude that discriminant is an invariant quantity.

Invariant $\Delta(K)$

Corollary 0.2.12. *Suppose $\{e_1, \ldots, e_n\}$ and $\{e'_1, \ldots, e'_n\}$ are both integral bases of the number field K, then*

$$disc_{K/\mathbb{Q}}(e_1, \ldots, e_n) = disc_{K/\mathbb{Q}}(e'_1, \ldots, e'_n).$$

We finish this subsection by making some observations about Δ_K. First, the determinant of the basis matrix M is equivalent to the fundamental domain of $\sigma(\mathcal{O}_K)$. This entails that the absolute[4]

[4] Although it is defined as the square of a matrix determinant, discriminant can be negative as the matrix entries can be complex numbers.

discriminant of K measures the geometric sparsity of $\mathcal{O}_K$. Larger $|\Delta_K|$ implies larger $\det M$, so the more sparse the ideal lattice is.

Second, equation 7 says $|\det N| = \frac{1}{2^{s_2}}|\det M|$. Since N is the basis matrix of the ideal lattice $\sigma(\mathcal{O}_K)$, by definition of field discriminant, this equation implies

$$\det(\sigma(\mathcal{O}_K)) = \frac{1}{2^{s_2}}\sqrt{|\Delta_K|}. \tag{10}$$

Ideal lattice determinant

Finally, an integral lattice I is an additive subgroup of $\mathcal{O}_K$ so Lagrange's Theorem entails $|\mathcal{O}_K| = |\mathcal{O}_K : I||I|$. The canonical embedding σ is an isomorphism between $\mathcal{O}_K$ and I to the corresponding ideal lattices. Moreover, I being a subgroup is sparser than $\mathcal{O}_K$ when mapped by σ, so has larger determinant. Hence, we have

$$\begin{aligned}\det(\sigma(I)) &= [\sigma(\mathcal{O}_K) : \sigma(I)]\det(\sigma(\mathcal{O}_K)) \\ &= N(I)\det(\sigma(\mathcal{O}_K)) \\ &= \frac{1}{2^{s_2}}N(I)\sqrt{|\Delta_K|}\end{aligned} \tag{11}$$

Equation 11 also holds for a fractional ideal $J = I/d$. Substitute the integral ideal $I = dJ$ into the equation will incur a factor d on both sides, because $\det(\sigma(dJ)) = d\det(\sigma(J))$ and $N(dJ) = N(d)N(J) = dN(J)$.

0.3 Dual lattice in number field

In the previous subsection, we have built a connection between a number field K and its image $H = \sigma(K)$ under the canonical embedding σ and shown that $H \cong \mathbb{R}^n$. In this subsection, we discuss how dual lattices in K are defined. The motivation is to understand the structure of dual lattices of an ideal lattice $\sigma(I)$. The notion of dual appears in crucial parts of the development of lattice-based cryptography, including the definition of smoothing parameters of a lattice (Definition **??**) and the general definition of RLWE distribution (Definition **??**).

Lattice in K

Definition 0.3.1. *A **lattice** in an n-dimensional number field K is the $\mathbb{Z}$-span of a $\mathbb{Q}$-basis of K.*

For lattices in $\mathbb{R}^n$, dot product is an obvious metric between two geometric vectors. For lattices in a number field, we need a more general inner product that can be obtained through the trace operator.

Definition 0.3.2. *Given a canonical embedding of a number field K*

$$\begin{aligned}\sigma : K &\to \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} \\ \sigma(\alpha) &\mapsto (\sigma_1(\alpha), \ldots, \sigma_n(\alpha)),\end{aligned}$$

Trace operator

*the **trace** of an element $\alpha \in K$ is defined as*

$$\begin{aligned}Tr_{K\setminus\mathbb{Q}} &: K \to \mathbb{Q} \\ Tr_{K/\mathbb{Q}}(\alpha) &= \sum_{i=1}^{n}\sigma_i(\alpha).\end{aligned}$$

From that, we obtain the trace inner product as follows:

$$Tr_{K/\mathbb{Q}}(xy) = \sum \sigma_i(xy) = \sum \sigma_i(x)\sigma_i(y) = \langle \sigma(x), \overline{\sigma(y)} \rangle. \tag{12}$$

Dual lattice

Definition 0.3.3. *Let L be a lattice in a number field K. Its **dual lattice** is*

$$L^\vee = \{x \in K \mid Tr_{K/Q}(xL) \subseteq \mathbb{Z}\}.$$

Example 0.3.4. *The lattice $L = \mathbb{Z}[i]$ in the number field $K = \mathbb{Q}(i)$ has a basis $B = \{1, i\}$. The dual lattice $L^\vee = \frac{1}{2}\mathbb{Z}[i]$ with a basis $B^\vee = \{\frac{1}{2}, \frac{i}{2}\}$.*

The dual of a number field lattice is also a lattice. Here are some properties of the dual in $\mathbb{R}^n$ that also hold true for dual in number fields.

Corollary 0.3.5. *For lattices in a number field K, the following hold:*

1. $L^{\vee\vee} = L$,
2. $L_1 \subseteq L_2 \iff L_2^\vee \subseteq L_1^\vee$,
3. $(\alpha L)^\vee \iff \frac{1}{\alpha} L^\vee$, *for an invertible element* $\alpha \in K$.

The following theorem relates the dual lattice to differentiation and provides an easier way of computing the dual basis and dual lattice from a given lattice.

Dual basis

Theorem 0.3.6. *Let $K = \mathbb{Q}(\alpha)$ be an n-dimensional number field with a power basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$ and $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of the element α, which can be expressed as*

$$f(x) = (x - \alpha)(c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}).$$

Then the dual basis to the power basis relative to the trace product is $\left\{ \frac{c_0}{f'(\alpha)}, \ldots, \frac{c_{n-1}}{f'(\alpha)} \right\}$. In particular, if $K = \mathbb{Q}(\alpha)$ and the primitive element $\alpha \in \mathcal{O}_K$ is an algebraic integer, then the lattice $L = \mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{n-1}$ and its dual are related by the first derivative of the minimal polynomial, that is,

$$L^\vee = \frac{1}{f'(\alpha)} L.$$

Example 0.3.7. *An important application of this theorem in RLWE is when $K = \mathbb{Q}[\zeta_m]$ is the m-th cyclotomic number field, where $m = 2n = 2^k > 1$ is a power of 2. Let the lattice $L = \mathcal{O}_K = \mathbb{Z}[\zeta_m]$. The minimal polynomial of ζ_m is $f(x) = x^n + 1$, whose derivative is $f'(x) = nx^{n-1}$. By Theorem 0.3.6,*

$$L^\vee = (\mathbb{Z}[\zeta_m])^\vee = \frac{1}{f'(\zeta_m)} \mathbb{Z}[\zeta_m] = \frac{1}{n\zeta_m^{n-1}} \mathbb{Z}[\zeta_m] = \frac{1}{n} \zeta_m^{n+1} \mathbb{Z}[\zeta_m] = \frac{1}{n} L.$$

The second last equality is because the roots of unity form a cyclic group so $\zeta_m^{-(n-1)} = \zeta_m^{n+1}$.

This example shows an essential property of cyclotomic number fields when choosing appropriate parameter settings. It says the ideal lattice $\sigma(\mathcal{O}_K)$ and its dual are related by only a scaling factor, so there is no difference working in either domain when defining the RLWE problem. We will see more detail in the next section.

We further study the ideal lattice $\mathcal{O}_K$ in a general number field. By definition, the dual of $\mathcal{O}_K$ is

$$\mathcal{O}_K^\vee = \{x \in K \mid Tr_{K/\mathbb{Q}}(x\mathcal{O}_K) \subseteq \mathbb{Z}\}.$$

Since each element in $\mathcal{O}_K$ is an algebraic integer, in that has an integer trace.[5] So on the one hand, $\mathcal{O}_K \subseteq \mathcal{O}_K^\vee$. On the other hand, not all elements with integer traces are in $\mathcal{O}_K^\vee$. The next theorem shows that these elements need to form a fractional ideal.

$\mathcal{O}_K^\vee$ is frac ideal

Theorem 0.3.8. *The dual lattice $\mathcal{O}_K^\vee$ is the largest fractional ideal in K whose elements have integer traces.*

Theorem 0.3.9. *For a fractional ideal I in K, its dual lattice is a fractional ideal satisfying the equation $I^\vee = I^{-1}\mathcal{O}_K^\vee$.*

We have seen the inverse of a fractional ideal in Equation 3, it is tempting to see if the inverse of the dual $\mathcal{O}_K^\vee$ (which is also a fractional ideal) is any special. By definition of fractional ideal inverse (Equation 3), we have

$$(\mathcal{O}_K)^{-1} = \{x \in K \mid x\mathcal{O}_K \subseteq \mathcal{O}_K\} = \mathcal{O}_K$$
$$(\mathcal{O}_K^\vee)^{-1} = \{x \in K \mid x\mathcal{O}_K^\vee \subseteq \mathcal{O}_K\}.$$

Since $\mathcal{O}_K \subseteq \mathcal{O}_K^\vee$, their inverses satisfy $(\mathcal{O}_K^\vee)^{-1} \subseteq \mathcal{O}_K$. Unlike the dual which is a fractional ideal and not necessarily within $\mathcal{O}_K$, this inclusion makes $(\mathcal{O}_K^\vee)^{-1}$ an integral ideal, which is also called the **different ideal**. For example, let $K = \mathbb{Q}(i)$ and $\mathcal{O}_K = \mathbb{Z}[i]$. The dual ideal is $\mathcal{O}_K^\vee = \mathbb{Z}[i]^\vee = \frac{1}{2}\mathbb{Z}[i]$, so the different ideal is $\mathcal{D}_K = (\frac{1}{2}\mathbb{Z}[i])^{-1} = 2\mathbb{Z}[i]$.

Different ideal

[5] This can be verified by taking the power basis $\{1, r, \ldots, r^{n-1}\}$ of K which is also a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Each $x \in \mathcal{O}_K$ can be written as $x = c_0 + c_1 r + \cdots + c_{n-1} r^{n-1}$. By definition, only $Tr(c_0) \in \mathbb{Z}$ and the rest are 0.

In the special case when $\mathcal{O}_K$ has a power basis, Theorem 0.3.6 can also be expressed in terms of different ideal because

$$\begin{aligned} \mathcal{O}_K^\vee &= \frac{1}{f'}\mathcal{O}_K \\ \implies f'\mathcal{O}_K^{-1} &= (\mathcal{O}_K^\vee)^{-1} \\ \implies (f') &= \mathcal{D}_K \end{aligned}$$

When $f = x^n + 1$, the last equality implies $\mathcal{D}_K = n\mathcal{O}_K$.See Theorem **??** in Appendix **??** for formal statements of these results.

$\mathcal{D}_K = n\mathcal{O}_K$ **Lemma 0.3.10.** *For $m = 2n = 2^k \geq 2$ a power of 2, let $K = \mathbb{Q}(\zeta_m)$ be an mth cyclotomic number field and $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ be its ring of integers. The different ideal satisfies $\mathcal{D}_K = n\mathcal{O}_K$.*

This lemma plays an important role in RLWE in the special case where the number field is an m-th cyclotomic field. It implies that the ring of integers $n^{-1}\mathcal{O}_K = \mathcal{O}_K^\vee$ and its dual are equivalent by a scaling factor. Hence, the secret polynomial $\mathbf{s}$ and the random polynomial $\mathbf{a}$ can both be sampled from the same domain R_q, unlike in the general context where the preference is to leave $\mathbf{s} \in R_q^\vee$ in the dual.

References

T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction to Algorithms*. The MIT Press, 2nd edition, 2001.

V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 1–23. Springer, 2010.

C. Peikert and A. Rosen. Lattices that admit logarithmic worst-case to average-case connection factors. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 478–487, 2007.

W. Stein. Algebraic number theory, a computational approach. *Harvard, Massachusetts*, 2012.