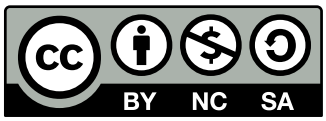
Aalto University
School of Electrical
Engineering

Bachelor's Programme in Electrical Engineering

Real cyclo-multiquadratic number fields in lattice-based cryptography

Konsta Koistinen

Bachelor's Thesis
2025



Aalto University
School of Electrical
Engineering

Author Konsta Koistinen

Title Real cyclo-multiquadratic number fields in lattice-based cryptography

Degree programme Electrical Engineering

Major Electronics and Electrical Engineering

Teacher in charge Dr. Markus Turunen

Advisors Rahinatou Yuh Njah Epouse Nchiwo (M.Sc.), Prof. Camilla Hollanti

Date 26.8.2025 **Number of pages** 38+5 **Language** English

Abstract

Advances in quantum computing threaten the cryptographic protocols protecting private messaging and other sensitive data. Post-quantum cryptography (PQC) aims to address this threat by researching and developing new cryptographic protocols, which are secure even against quantum algorithms. Lattice-based cryptography (LBC) is one of the leading approaches to PQC. LBC studies and develops cryptographic algorithms relying on lattice problems which are believed to be hard even for quantum computers. Two of the most prominent paradigms used in LBC are ring learning with errors (RLWE) and polynomial learning with errors (PLWE), which utilize the structure of rings of integers of algebraic number fields and polynomial rings to build secure and efficient cryptoschemes.

This thesis describes the RLWE and PLWE problems and the conditions under which they are equivalent, and reviews known RLWE/PLWE equivalence results. The main result of this thesis is an RLWE/PLWE equivalence proof for a subset of a family of fields we call real cyclo-multiquadratic, defined as the compositum of the maximal real subfield of a cyclotomic field and a multiquadratic field. Equivalence is shown in the case where the conductor of the maximal real subfield of a cyclotomic field is p^s or $2^r p^s$ for an odd prime p. This is done in order to broaden the family of suitable number fields for potential applications of LBC. Additionally, an improved upper bound for the condition number of the RLWE to PLWE transformation matrix for real quadratic fields is presented. Computational efficiency of real cyclo-multiquadratic fields will be studied in subsequent work. Research into the distribution of weak instances of real cyclo-multiquadratic fields is suggested.

Keywords number theory, cryptography, lattices, ring learning with errors, polynomial learning with errors, condition number

Aalto-yliopisto
Sähkötekniikan
korkeakoulu

Tekijä Konsta Koistinen

Työn nimi Reaaliset syklo-multikvadraattiset lukukunnat hilakryptografiassa

Koulutusohjelma Sähkötekniikan kandidaattiohjelma

Pääaine Elektroniikka ja sähkötekniikka

Vastuuopettaja TkT Markus Turunen

Työn ohjaajat Rahinatou Yuh Njah Epouse Nchiwo (M.Sc.), Prof. Camilla Hollanti

Päivämäärä 26.8.2025 **Sivumäärä** 38+5 **Kieli** englanti

Tiivistelmä

Kvanttilaskennan kehitys uhkaa kryptografisia protokollia, jotka suojaavat arkaluontoista dataa ja yksityistä viestintää. Kvanttiturvallinen kryptografia (Post-Quantum Cryptography, PQC) pyrkii vastaamaan tähän uhkaan tutkimalla ja kehittämällä uusia kryptografisia protokollia, jotka ovat turvallisia myös kvanttialgoritmeja hyödyntäviä hyökkääjiä vastaan. Yksi johtavista lähestymistavoista kvanttiturvallisen kryptografian kehityksessä on hilakryptografia (Lattice-Based Cryptography, LBC). Hilakryptografia tutkii ja kehittää vaikeisiin hilaongelmiin perustuvia kryptografisia algoritmeja, joiden uskotaan olevan vaikeita murtaa myös kvanttitietokoneilla. Kaksi merkittävimmistä hilakryptografiassa käytetyistä ongelmista ovat kohinainen oppiminen renkaassa (Ring Learning With Errors, RLWE) ja kohinainen oppiminen polynomirenkaassa (Polynomial Learning With Errors, PLWE), jotka hyödyntävät algebrallisten kokonaislukurenkaiden ja polynomirenkaiden rakenteita turvallisten ja suorituskykyisten kryptojärjestelmien rakentamisessa.

Tämä opinnäytetyö kuvailee RLWE- ja PLWE-ongelmia ja ehtoja, joiden täyttyessä ne ovat ekvivalentteja, sekä käy läpi tunnettuja RLWE/PLWE-ekvivalenssituloksia. Työn päätulos on todistus RLWE/PLWE-ekvivalenssista osajoukolle niin kutsuttuja reaalisia syklo-multikvadraattisia kuntia, jotka on määritelty syklotomisen kunnan maksimaalisen reaalisen alikunnan ja multikvadraattisen kunnan komposiittikuntana. Ekvivalenssi osoitetaan tapauksessa, jossa syklotomisen kunnan maksimaalisen reaalisen alikunnan johtaja (engl. conductor) on p^s tai $2^r p^s$, missä p on pariton alkuluku. Saatu tulos laajentaa mahdollisissa hilakryptografisissa sovelluksissa käytettävissä olevien lukukuntien joukkoa. Opinnäytetyö esittää lisäksi parannetun ylärajan reaalisten kvadraattisten kuntien RLWE-PWLE muunnosmatriisin häiriöalttiudelle. Reaalisten syklo-multikvadraattisten kuntien laskennallista tehokkuutta tutkitaan tulevissa töissä. Lisäksi lisätutkimusta näiden lukukuntien heikkojen instanssien jakaumasta toivotaan.

Avainsanat lukuteoria, kryptografia, hilat, kohinainen oppiminen renkaassa, kohinainen oppiminen polynomirenkaassa, häiriöalttius

Contents

1 Introduction

Advances in quantum computing threaten the cryptographic protocols protecting sensitive data and private communication. As quantum computers rapidly become more powerful and practical, quantum algorithms have the potential to break current cryptographic systems. Harvesting attacks, which involve storing encrypted data to be decrypted once a sufficiently powerful quantum computer becomes available, are another reason why the subject is important now. Additionally, the standardization process and migration to new cryptosystems is slow. Research into quantum resistant cryptographic protocols is therefore of vital importance.

Post-quantum cryptography (PQC) refers to cryptosystems that run on classical computers and are secure even against quantum attacks. One of the most promising branches of PQC is lattice-based cryptography (LBC), which consists of cryptographic schemes relying on hard lattice problems. Cryptosystems based on these problems are considered promising candidates for quantum-resistant cryptography schemes because of their conceptual simplicity, ease of implementation, and existing strong hardness proofs for the underlying lattice problems. As an indication of this, two of the first three post-quantum encryption algorithms standardized by National Institute of Standards and Technology (NIST), ML-DSA and ML-KEM, are based on lattice problems [Nat25]. Furthermore, at the time of writing, there are no known quantum or traditional algorithms for solving the relevant lattice problems efficiently.

An early practical LBC scheme was introduced by Regev in 2005, as well as the learning with errors (LWE) problem it is based on [Reg05]. Crucially, Regev showed that the LWE problem is hard on average, which makes it suitable for cryptographic use. This is versus being hard only in the worst case, meaning that an average instance is, with high probability, as hard as the worst instance. LWE presented an improvement in efficiency over the previous lattice-based cryptosystems via a significant reduction of public key and ciphertext sizes. Regev's system had public key sizes of $\tilde{O}(n^2)$ and a plaintext size increase of $\tilde{O}(n)$ in encryption, while the previous systems required $\tilde{O}(n^4)$ and $\tilde{O}(n^2)$, respectively. This variant of the learning with errors problem is sometimes called unstructured, since it employs no additional algebraic structure. Though secure, it also had practical limitations due to the quadratic overhead.

To address the practical limitations of LWE, structured LWE problems were introduced by Stehlé, Steinfeld, Tanaka and Xagawa in 2009 [Ste+09] and Lyubashevsky, Peikert and Regev in 2010 [LPR10]. Lyubashevsky et al. developed ring learning with errors (RLWE), an LWE variant utilizing the algebraic structure of rings of integers of algebraic number fields. Exploiting this added structure, the authors were able to further improve the efficiency of encryption. Stehlé et al. introduced what is now referred to as polynomial learning with errors (PLWE), which was first called PLWE in [BV11]. PLWE brings further efficiency improvements for practical applications over RLWE.

However, the practical efficiency improvements gained by exploiting additional algebraic structure can make cryptoschemes based on PLWE problems vulnerable to attacks [EHL14]. Additionally, worst-case to average-case reduction for PLWE exists only for the case of power-of-two cyclotomic polynomials at the writing of this

thesis [Ste+09]. Current research investigates when and for which classes of fields the RLWE and PLWE problems are equivalent so that we may enjoy the strong security guarantees of RLWE while benefiting from the additional efficiency of PLWE [DSS24; Bla+25; Aho+25].

RLWE and PLWE are currently known to be equivalent for some families of cyclotomic fields, maximal real subfields of cyclotomic fields, and certain composite fields. This thesis studies the equivalence of RLWE and PLWE over what we call real cyclo-multiquadratic fields. We do this in order to extend the class of suitable fields for potential applications of lattice-based cryptography.

Section 2 of this thesis presents an extensive review of preliminaries from algebra and algebraic number theory, as well as introduces lattices and necessary notions from cryptography. Section 3 discusses ring learning with errors and polynomial learning with errors. We define the equivalence of RLWE and PLWE and present some established RLWE/PLWE equivalence results for specific classes of fields. Our main result is presented in Section 4, where we prove RLWE/PLWE equivalence for a subset of a family of fields we call real cyclo-multiquadratic using methods from algebra and algebraic number theory.

2 Preliminaries

In this section, we introduce the central definitions and results used in this thesis. We start with essential algebraic structures and notions. With the basics established, we proceed to introduce some fundamental notions of algebraic number theory. We then continue to define lattices and establish a connection to them from the structures of algebraic number theory. Finally, we define some fundamental cryptographic notions necessary for our research.

2.1 Algebraic number theory

The efficiency improvements of structured LWE schemes, as well as their vulnerabilities, both stem from the algebraic structure they employ. In this section, we introduce the necessary concepts and results from algebraic number theory to understand structured LWE. We start by recalling some basic algebraic structures and their properties in order to keep this thesis self-contained.

Definition 2.1. A *binary operation* $\star$ on a non-empty set G is a function

$$\star : G \times G \rightarrow G.$$

Definition 2.2. A *group* $(G, \cdot)$ is a non-empty set G equipped with a binary operation $\cdot$ satisfying the following:

1. The operation $\cdot$ is associative, that is,
   $\forall a, b, c \in G : \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

2. There exists a unique identity element e for $\cdot$, that is,
   $\exists! e \in G, \ \forall x \in G : \quad e \cdot x = x \cdot e = x$

3. Every element in G has an *inverse* with respect to $\cdot$, that is,
   $\forall g \in G, \ \exists h \in G : \quad g \cdot h = e = h \cdot g$.

For brevity, we usually refer to the group $(G, \cdot)$ simply as G. Likewise, we often omit the group operation symbol when it is clear from context, and write ab for $a \cdot b$. For abstract groups, we generally use multiplicative notation.

A group $(G, \cdot)$ where $a \cdot b = b \cdot a \ \ \forall a, b \in G$ is called *abelian*. For abelian groups, the group operation is often denoted by $+$.

Example 2.3.

- Integers modulo n, denoted by $\mathbb{Z}_n$, form an additive group.

- The invertible residues modulo n form a group under multiplication, denoted by $\mathbb{Z}_n^*$ and called the group of units modulo n.

- Invertible $n \times n$ matrices with real entries form a non-abelian group under multiplication, denoted by $\mathrm{GL}_n(\mathbb{R})$.

- Rotations of a square by an integer multiple of 90 degrees form a group with function composition.

An abelian group G whose elements can be expressed uniquely as a finite $\mathbb{Z}$-linear combination of elements of a subset of G is called a *free abelian group*. That is, a free abelian group is an abelian group with a basis. The number of elements in a basis of a free abelian group is called its *rank* and it does not depend on the choice of basis [ST25, Theorem 1.27]. Moreover, every change of basis matrix of a free abelian group has integer entries and determinant ± 1. That is, the change of basis matrix is *unimodular* [ST25, Lemma 1.28].

Definition 2.4. A *subgroup* of a group $(G, \cdot)$ is a subset H of G that forms a group under the operation of G. We say H is *closed* under the operation inherited from G. A subgroup N of G is called *normal*, if for all $g \in G$ and $n \in N$, $gng^{-1} \in N$.

The group of all rotations of a square mentioned in Example 2.3 is a normal subgroup of the group of all symmetries of a square. This group is called the dihedral group of order 8, denoted D_8.

Definition 2.5. Let H be a subgroup of G. For $g \in G$, the *right coset* of H generated by g is

$$Hg = \{hg \mid g \in G\}.$$

Similarly, the *left coset* of H generated by g is

$$gH = \{gh \mid g \in G\}.$$

Cosets partition G into equivalence classes. Clearly, for normal subgroups the left and right cosets are equal. In fact, we may form new groups using normal subgroups.

Definition 2.6. Let H be a normal subgroup of G. Then the cosets together with the coset product $(aH)(bH) = (ab)H$ form the *quotient group*, denoted G/H.

Definition 2.7. Let $(G, \cdot_G)$ and $(G', \cdot_{G'})$ be groups. A *group homomorphism* is a function $\phi : G \to G'$ such that

$$\forall a, b \in G : \quad \phi(a \cdot_G b) = \phi(a) \cdot_{G'} \phi(b).$$

An injective homomorphism is called a *monomorphism*. A surjective homomorphism is called an *epimorphism*. If a homomorphism is both injective and surjective, it is an *isomorphism*. If there exists an isomorphism between two groups G and G', they are called *isomorphic*, denoted $G \cong G'$. An isomorphism from a group to itself is an *automorphism*. Automorphisms play a central role in Galois theory and are used to construct lattices from structures introduced later in this section.

Definition 2.8. Let $\phi : G \to G'$ be a group homomorphism. The *kernel* of ϕ is the subset of G which maps to the identity of G', i.e.,

$$\ker \phi = \{g \in G \mid \phi(g) = e_{G'}\} = \phi^{-1}(e_{G'}).$$

The *image* of ϕ is the set of images of ϕ, i.e.,

$$\operatorname{im} \phi = \{g' \in G' \mid g' = \phi(g),\ g \in G\} = \phi(G).$$

The kernel of a homomorphism $G \to G'$ is a normal subgroup of G, and the image is a subgroup of G'.

Definition 2.9. A *ring* $(R, +, \cdot)$ is an abelian group $(R, +)$ endowed with a second binary operation $\cdot$, which is also associative, distributive, and has a two-sided identity, i.e.,

1. $\forall r, s, t \in R: \quad (r \cdot s) \cdot t = r \cdot (s \cdot t)$
2. $\exists 1 \in R \; \forall r \in R: \quad 1 \cdot r = r \cdot 1 = r$
   and further interacting with + via the following *distributive* properties:
3. $\forall r, s, t \in R: \quad (r + s) \cdot t = r \cdot t + s \cdot t$ and $t \cdot (r + s) = t \cdot r + t \cdot s$.

For rings, the additive identity element is usually denoted 0. Just as with groups, we often omit the operation $\cdot$ and refer to the ring by the name of the underlying set. A ring whose multiplicative subgroup $(R, \cdot)$ is abelian is called a commutative ring.

Remark. In this thesis, we require that rings have a multiplicative identity denoted by 1. Furthermore, as we will be working mainly with rings of integers and polynomial rings, we generally assume that rings are also commutative.

Example 2.10.

- The integers form a ring with the usual addition and multiplication, denoted by $\mathbb{Z}$.
- $\mathbb{Z}[x]$, the set of all polynomials in the indeterminate x with integer coefficients, forms a ring under the usual polynomial addition and multiplication.

Definition 2.11. Let R be a ring. A subgroup I of $(R, +)$ is a *left ideal* of R if $rI \subseteq I$ for all $r \in R$; that is,

$$\forall r \in R \; \forall a \in I: \quad ra \in I;$$

it is a *right ideal* if $Ir \subseteq I$ for all $r \in R$; that is,

$$\forall r \in R \; \forall a \in I: \quad ar \in I$$

A *two-sided ideal* is a subgroup I of R, which is both a left and right ideal.

We will refer to two-sided ideals simply as ideals in this thesis, as the rings we consider are commutative.

Example 2.12. All multiples of a polynomial $f \in \mathbb{Z}[x]$ form an ideal in $\mathbb{Z}[x]$, denoted (f). As it has only one generator, it is called the *principal ideal* generated by f.

Definition 2.13. Let I be a proper ideal of a ring R. The *quotient ring* R/I consists of the cosets $r + I$ for $r \in R$, with the multiplication operation given by

$$(r + I)(s + I) = rs + I \quad \forall r, s \in R.$$

The central objects of study in PLWE are the quotient of the ring of integer coefficient polynomials by a principal ideal, usually generated by a monic irreducible polynomial.

Definition 2.14. Let R, S be rings. A function $\phi : R \to S$ is a *ring homomorphism* if

$$\forall a, b \in R: \quad \phi(a+b) = \phi(a) + \phi(b),$$

$$\forall a, b \in R: \quad \phi(a \cdot b) = \phi(a) \cdot \phi(b),$$

$$\phi(1_R) = 1_S.$$

That is, a ring homomorphism is a group homomorphism of the underlying abelian groups which preserves both ring operations and the multiplicative identity.

Image and kernel of ring homomorphism are defined the same as for group homomorphisms. Now $\operatorname{im}\phi$ is a subring of S and $\ker\phi$ is an ideal of R. In fact, every ideal is a kernel of some ring homomorphism, see [Alu09, Example 3.3].

Definition 2.15. An *integral domain* is a non-zero commutative ring R (with 1) such that

$$\forall a, b \in R: \quad ab = 0 \implies a = 0 \text{ or } b = 0.$$

Definition 2.16. Let R be a ring. An *R-module* is an abelian group M, together with a function $\alpha : R \times M \to M$, with $\alpha(r, m) = rm$ for $r \in R,\ m \in M$, where the following hold for all $r, s \in R,\ m, n \in M$:

1. $r(m+n) = rm + rn$ (Left-distributivity)
2. $(r+s)m = rm + rs$ (Right-distributivity)
3. $r(sm) = (rs)m$ (Associativity)
4. $1m = m$.

Notice that an ideal I of a ring R is in fact an R-module. Additionally, abelian groups written additively correspond to $\mathbb{Z}$-modules.

Definition 2.17. A *field* is an integral domain in which every nonzero element has a multiplicative inverse, i.e., is a *unit*.

Some familiar examples of fields include the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$. A *subfield* of a field L is a subset $K \subseteq L$ such that K forms a field under the operations inherited from L. A *finite field* is a field whose underlying set is of finite cardinality. It can be proven that actually, this cardinality is p^k for a prime p and integer $k \geq 1$. $\mathbb{Z}_p$, the integers modulo a prime, are a simple example of a finite field of *order* p. In cryptography, finite fields give us the ability to define and use uniform distributions.

Example 2.18. Let $f(x) \in \mathbb{Q}[x]$ be a monic irreducible polynomial. Then $\mathbb{Q}[x]/(f(x))$, the quotient ring of polynomials with rational coefficients modulo the principal ideal generated by f, is a field.

Modular arithmetic in polynomial rings is done analogously to modular arithmetic of integers. Informally, quotienting by a polynomial sets the polynomial equal to zero in the quotient ring. Reducing a polynomial g modulo the polynomial f consists of finding a representation $g = hf + r$, where the degree of r is strictly less than the degree of f. This representation can be found using the usual polynomial division algorithm. Then we see that $g \equiv r \pmod{f}$.

Definition 2.19. A *vector space* is a module over a field.

Definition 2.20. If a field K is a subfield of a field L, we say that L is a *field extension* of K, denoted L/K, which can also be viewed as a vector space over K.

Definition 2.21. The *degree* of the extension L/K, or the *degree of L over K*, is the dimension of L considered as a vector space over K, denoted

$$[L : K] = \dim_K(L).$$

Number fields are finite dimensional vector spaces over $\mathbb{Q}$, giving us the ability to use powerful tools from linear algebra in the study of these fields.

Definition 2.22. An *algebraic number* θ is a root of a polynomial with rational coefficients. An *algebraic integer* θ is a root of a monic polynomial with integer coefficients.

Definition 2.23. A *number field* K is a finite extension of the field of rationals by algebraic elements, that is, $K = \mathbb{Q}(\theta_1, \ldots, \theta_n)$, where each θ_i is algebraic.

Definition 2.24. Let K be a number field and $\theta \in K$ be algebraic over K. The *minimal polynomial* of θ over $\mathbb{Q}$ is the unique monic polynomial f of lowest degree such that $f(\theta) = 0$.

Theorem 2.25. *Let $K = \mathbb{Q}(\theta)$ be a number field and $f(x)$ be the minimal polynomial of θ over $\mathbb{Q}$. Then $\mathbb{Q}(\theta)$ is isomorphic to $\mathbb{Q}[x]/(f(x))$.*

Proof. Define the evaluation map,

$$\phi : \mathbb{Q}[x] \to \mathbb{Q}(\theta),\ p(x) \mapsto p(\theta).$$

Let $p(x) \in \mathbb{Q}[x]$ be a nonzero polynomial. Since $\mathbb{Q}[x]$ is a Euclidean domain, we can always factor $p(x)$ uniquely as $p(x) = f(x)g(x) + r(x)$ for $g(x), r(x) \in \mathbb{Q}[x]$ with $\deg r(x) < \deg f(x)$. It is easy to see that ϕ is a surjective ring homomorphism fixing the base field $\mathbb{Q}$. Moreover, if $p(x) \in \ker \phi$, that is, $\phi(p(x)) = p(\theta) = 0$, we must have $f(x) \mid p(x)$ by minimality of $f(x)$. Therefore, $\ker \phi = (f(x))$ and we have the desired isomorphism $\mathbb{Q}(\theta) \cong \mathbb{Q}[x]/(f(x))$ by the First Isomorphism Theorem. □

Theorem 2.26. *Let $K = \mathbb{Q}(\theta)$ be a number field with $n = [K : \mathbb{Q}]$. Then there are exactly n distinct monomorphisms $\sigma_i : K \to \mathbb{C}$ mapping θ to the distinct zeros in $\mathbb{C}$ of the minimal polynomial of θ.*

Proof. See [ST25, p. 45]. □

These monomorphisms are often called *embeddings*, since they can be seen as embedding a number field into the complex numbers.

Theorem 2.27 (Tower Law)**.** *If $K \subseteq M \subseteq L$ are number fields, then*

$$[L : K] = [L : M][M : K].$$

Proof. See [Ste15, p. 80–81]. □

Theorem 2.28 (Primitive Element Theorem)**.** *Let L be a finite extension of a number field K. Then $L = K(\theta)$ for some $\theta \in L$.*

Proof. See [ST25, p. 43]. □

It follows that all number fields are generated over $\mathbb{Q}$ by adjunction of a single element. Such extensions are called *simple*. Furthermore, the powers $\{\theta^k\}_{k=0}^{n-1}$ of the primitive element θ form a *power basis* for $K = \mathbb{Q}(\theta)$ over $\mathbb{Q}$, where $n = [K : \mathbb{Q}]$.

Definition 2.29. An nth *root of unity* is a solution of $x^n = 1$. A root of unity is called *primitive*, if it is not an mth root of unity for any $m < n$.

The nth roots of unity split the unit circle into n arcs of equal lengths. Moreover, nth roots of unity form a cyclic group under multiplication: the multiplicative inverse of an nth root of unity as well as any product of nth roots of unity is again an nth root of unity. The primitive nth roots of unity generate this group. Figure 1 illustrates the 5th roots of unity.

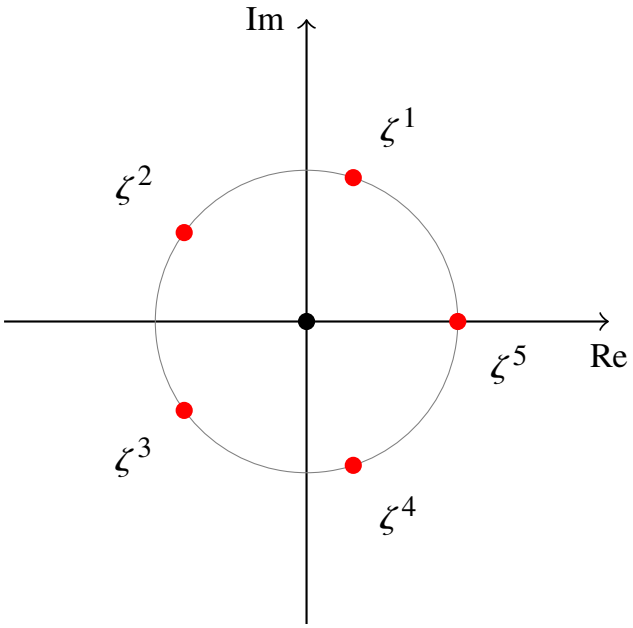


Figure 1: 5th roots of unity.

Definition 2.30. The nth *cyclotomic field* $K = \mathbb{Q}(\zeta_n)$ is an extension of the rational numbers by a primitive nth root of unity.

Cyclotomic fields are important for structured LWE because they are well-studied and relatively simple to characterize. Their cyclic structure enables the use of transforms like the Fast Fourier Transform (FFT) and efficient representations, speeding up arithmetic for cryptoschemes based on them.

The degree of the nth cyclotomic field over $\mathbb{Q}$ is $\varphi(n)$, where φ is *Euler's totient function*. $\varphi(n)$ is the number of integers $k \in [1, n]$ such that $\gcd(k, n) = 1$. These are the invertible residues modulo n.

In this thesis, we are particularly interested in the *maximal totally real subfield of a cyclotomic field* $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. The primitive element of this extension is $\zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$.

Definition 2.31. The nth *cyclotomic polynomial* is the minimal polynomial of a primitive nth root of unity, denoted Φ_n, with

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(n,k)=1}} (x - \zeta_n^k).$$

Definition 2.32. Let E and F be subfields of K. Then the *compositum* of E and F is the smallest subfield of K containing both E and F. The *composite field* is denoted EF.

The objects of study in the main result of this thesis are given as a compositum of certain number fields.

Definition 2.33 (Galois group)**.** Let K be an algebraic number field. Then the set of automorphisms of K fixing $\mathbb{Q}$, $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(x) = x,\ \forall x \in \mathbb{Q}\}$, forms the *Galois group* of the extension $K/\mathbb{Q}$ together with function composition.

The Galois group acts on the number field $K = \mathbb{Q}(\theta)$ by permuting the roots of the defining polynomial of K, i.e., the minimal polynomial $f(x) \in \mathbb{Q}[x]$ of θ over $\mathbb{Q}$. This follows from the fact that every automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ fixes $\mathbb{Q}$. We have

$$\sigma(0) = \sigma(f(\theta)) = \sigma\left(\sum_{k=0}^{n-1} a_k \theta^k\right) = \sum_{k=0}^{n-1} \sigma(a_k \theta^k) = \sum_{k=0}^{n-1} a_k \sigma(\theta^k) = \sum_{k=0}^{n-1} a_k \sigma(\theta)^k,$$

where we use the properties of ring homomorphisms and the fact that the automorphisms fix $\mathbb{Q}$. This shows that, for any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, $\sigma(\theta)$ is also a root of $f(x)$. The elements $\sigma_i(\theta)$, $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$, are called the *Galois conjugates* of θ. See Figure 2 for an example of a Galois automorphism acting on roots of unity.

A field extension is called abelian (resp. cyclic) if its Galois group is abelian (resp. cyclic). Both cyclotomic fields and their maximal real subfields are cyclic extensions over $\mathbb{Q}$.

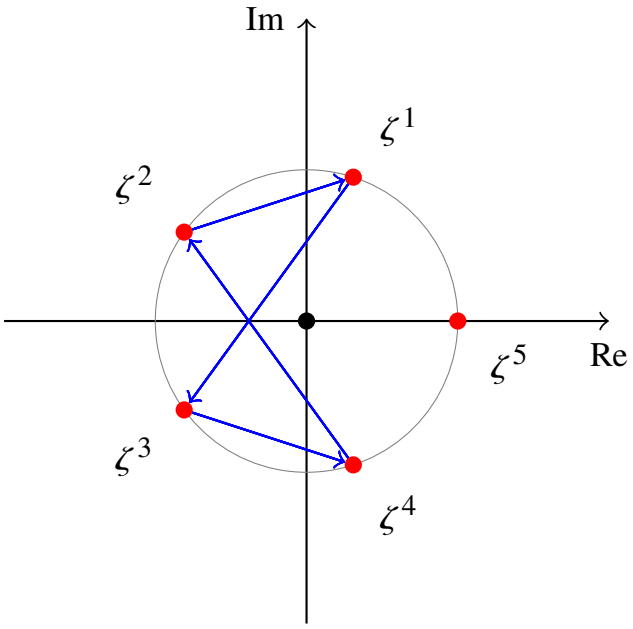


Figure 2: Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ acting on 5th roots of unity. The automorphism presented is $\sigma_3 : \zeta \mapsto \zeta^3$.

Definition 2.34 (Definition 2.21 [ST25])**.** Let K be a number field. The set of all algebraic integers in K forms a ring with the usual addition and multiplication called the *ring of integers of* K, denoted O_K.

Definition 2.35. An *integral basis* of K, or of O_K, is a $\mathbb{Z}$-basis for $(O_K, +)$.

Definition 2.36. An algebraic number field K is called *monogenic* if there exists an $\theta \in K$ such that $O_K = \mathbb{Z}[\theta]$.

For monogenic fields, the powers of θ form a power integral basis for the ring of integers. Importantly, all quadratic fields and cyclotomic fields, as well as their maximal real subfields, are monogenic. For proofs of these facts, we refer the reader to [Was12, Theorem 2.6, Proposition 2.16] and [ST25, Theorem 3.3].

Definition 2.37. Let K be a number field of degree n with a $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$. The *discriminant* of this basis is

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\det[\sigma_i(\alpha_j)])^2.$$

Definition 2.38. The *discriminant of a number field* K is the discriminant of its integral basis, denoted either Δ_K or $\Delta(K)$.

Remark. The discriminant of K does not depend on the choice of basis. This is because the additive groups of rings of integers are free abelian [ST25, Theorem 2.28] and bases of free abelian groups are related by a unimodular matrix [ST25, Lemma 1.28].

Definition 2.39. An ideal $\mathfrak{p} \neq R$ of a ring R is called *prime*, if for all ideals $\mathfrak{a}, \mathfrak{b}$ of R

$$\mathfrak{ab} \subseteq \mathfrak{p} \implies \mathfrak{b} \subseteq \mathfrak{p} \text{ or } \mathfrak{a} \subseteq \mathfrak{p}.$$

The concept of ideals was first introduced in the 19th century in order to restore a sense of unique factorization into irreducibles in rings of integers. For example, in $\mathbb{Z}[\sqrt{-5}]$, we have $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, where all elements in both factorizations are irreducible in $\mathbb{Z}[\sqrt{-5}]$. This shows that the fundamental theorem of arithmetic can fail in this setting. However, ideals in rings of integers do admit unique factorization into prime ideals, up to multiplication by a unit and reordering.

Definition 2.40. Let $K = \mathbb{Q}(\theta)$ be a number field of degree n and $\{\sigma_1, \dots, \sigma_n\}$ the set of all embeddings of K into $\mathbb{C}$. If $\sigma_k(K) \subseteq \mathbb{R}$, or equivalently $\sigma_k(\theta) \in \mathbb{R}$, we say that σ_k is *real*. Otherwise, σ_k is called *complex*.

From the fact that complex conjugation is an automorphism of $\mathbb{C}$, it follows that complex embeddings of a number field come in complex conjugate pairs. Hence, $n = r + 2s$, where r denotes the number of real embeddings and $2s$ all complex embeddings of K.

In order to later define geometric quantities for elements of O_K, we first define the metric space

$$\mathcal{M}_n = \{(x_1, x_2, \dots, x_n) \in \mathbb{R}^r \times \mathbb{C}^{2s} \mid x_{r+i} = \bar{x}_{r+s+i},\ 1 \leq i \leq s\}$$

with the usual inner product in $\mathbb{C}^n$. The metric on $\mathcal{M}_n$ is the usual Euclidean metric induced by the norm with respect to the inner product.

Definition 2.41. Let K be a number field of degree n and denote by σ_i its n field automorphisms. The *Minkowski embedding*, or canonical embedding, is the map $\sigma : K \to \mathcal{M}_n$ defined as

$$\sigma(x) = (\sigma_1(x),\ \sigma_2(x),\ \dots,\ \sigma_n(x)).$$

Theorem 2.42 (Kronecker–Weber)**.** *Let K be a finite abelian extension of $\mathbb{Q}$. Then K is contained in some cyclotomic extension of $\mathbb{Q}$.*

Proof. See [Nar04, p. 280]. □

The Kronecker–Weber theorem allows us to define the *conductor* of a number field K, which is the smallest $n \in \mathbb{N}$ such that $K \subseteq \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity. The conductor of $K_n = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, the maximal real subfield of the nth cyclotomic field $\mathbb{Q}(\zeta_n)$, is trivially n. The conductor plays a significant role in our result, as we will see in the sections below.

2.1.1 Ramification

The concept of ramification is central to a part of the proof of our main result in Section 4, hence we find it convenient to give a brief overview of it here. For the following, let p be a rational prime, K a number field, and $\mathcal{O}_K$ its rings of integers.

The ideal $(p) = p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, because clearly $(p) \neq \mathbb{Z}$ and $(a)(b) \subseteq (p)$ implies $(a) \subseteq (p)$ or $(b) \subseteq (p)$. Since (p) is prime in $\mathbb{Z}$, $p\mathcal{O}_K$ is also an ideal of $\mathcal{O}_K$, though it need not be prime in $\mathcal{O}_K$. However, because rings of integers have unique factorization into prime ideals, we have

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g} \quad (e_i \geq 1),$$

where $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$. Notice that, for each $\mathfrak{p}_i$, we have that $\mathfrak{p}_i \cap \mathbb{Z} = p\mathbb{Z}$. We say that the ideals $\mathfrak{p}_i$ *lie above* p. e_i is called the *ramification index* of $\mathfrak{p}_i$ over p. p is said to *ramify* in $\mathcal{O}_K$, if $e_i > 1$ for any i. Otherwise, p is *unramified* in $\mathcal{O}_K$. The rational primes which ramify in a number field K are precisely the primes which divide its discriminant Δ_K. Figure 3 presents an example of splitting of a rational prime in ring extensions.

Example 2.43. Consider the number field $\mathbb{Q}(i)$. Its ring of integers is $\mathbb{Z}[i]$, often called the *Gaussian integers*. The discriminant of $\mathbb{Q}(i)$ is $-4 = -2^2$, which implies that only 2 ramifies in $\mathbb{Z}[i]$. We find that the principal ideal generated by 2 factors in $\mathbb{Z}[i]$ as $(2) = (1+i)^2$. The ramification index of $(1+i)$ over 2 in $\mathbb{Z}[i]$ is therefore 2.

$\mathcal{O}_K/\mathfrak{p}_i$ is a field for each i, since prime ideals of rings of integers are also maximal [ST25, Theorem 6.4(d)]. In fact, since $\mathbb{Z}/(p) = \mathbb{Z}_p$ embeds into $\mathcal{O}_K/\mathfrak{p}_i$ for each i via $\mathbb{Z} \hookrightarrow \mathcal{O}_K \to \mathcal{O}_K/\mathfrak{p}_i$, we see that $\mathcal{O}_K/\mathfrak{p}_i$ are finite extensions of the finite field of order p. Define the *inertia degree* of $\mathfrak{p}_i$ over p as

$$f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}_p].$$

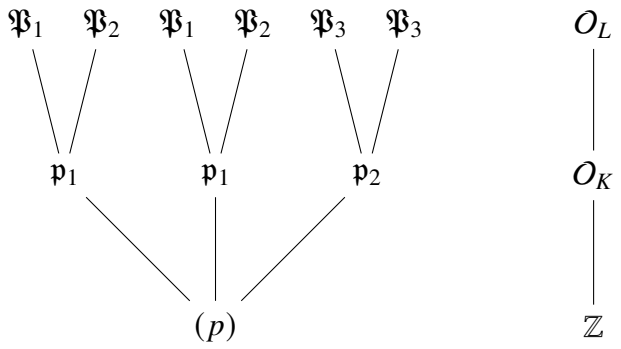


Figure 3: Possible ramification and splitting behavior of a rational prime p in rings of integers of number fields $K \subset L$. The ramification index of $\mathfrak{p}_1$ above p is 2. Similarly, the ramification index of $\mathfrak{P}_3$ above $\mathfrak{p}_2$ is also 2.

If K is Galois, that is, if any irreducible polynomial over $\mathbb{Q}$ with at least one root in K splits entirely into linear factors over K, then the Galois group $\mathrm{Gal}(K/\mathbb{Q})$

acts transitively on the set of all prime ideals above a rational prime p [Neu99, Proposition 9.1]. That is, for any two prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ above p, there exists a Galois automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\mathfrak{p}_1 = \sigma(\mathfrak{p}_2)$. In other words, the Galois conjugate of any prime ideal above p is also a prime ideal above p. It follows that, for each $\mathfrak{p}_i$ above p, the ramification index e_i and inertia degree f_i are independent of the index i. Thus,

$$p\mathcal{O}_K = (\mathfrak{p}_1 \dots \mathfrak{p}_g)^e$$

Additionally, the degree of K over $\mathbb{Q}$ has the form $[K : \mathbb{Q}] = efg$ [Lan13, p. 26].

2.2 Lattices

We will now introduce the concept of lattices and some of their important invariants. We define lattice problems central to lattice-based cryptography and describe a connection between lattices and rings of integers of number fields and their ideals, which is used heavily in structured LWE.

Definition 2.44. Let $\{b_1, \dots, b_m\}$ be a set of m linearly independent vectors in $\mathbb{R}^n$ $(m \leq n)$. The *lattice* $\mathcal{L}$ generated by $B = [b_1, \dots, b_m]$ is the set of $\mathbb{Z}$-linear combinations of $b_1, \dots, b_n$, i.e.,

$$\mathcal{L} = \mathcal{L}(B) = \{a_1 b_1 + \dots + a_m b_m \mid a_1, \dots, a_m \in \mathbb{Z}\} = B\mathbb{Z}.$$

Alternatively, an n-dimensional lattice $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{R}^n$. With the above notation, the set of b_i is called a *basis* of $\mathcal{L}$. It can be helpful to consider a general n-dimensional lattice to be a linear transformation of $\mathbb{Z}^n$ by a basis change matrix B. The integer n is called the *dimension* of $\mathcal{L}$, and m is called the *rank* of $\mathcal{L}$. If $m = n$, the lattice $\mathcal{L}$ is called *full-rank*. In this thesis, we generally assume lattices to be full rank.

Proposition 2.45. *Suppose that G is a finitely generated additive subgroup of a number field K with $\mathbb{Z}$-basis $\{\theta_1, \dots, \theta_n\}$. Then the image of G in $\mathcal{M}_n$ under the Minkowski embedding is a lattice with basis $\{\sigma(\theta_1), \dots, \sigma(\theta_n)\}$.*

Proof. See [ST25, p. 184]. □

This means that we can embed rings of integers and their ideals as lattices into Euclidean space and consider these algebraic structures geometrically. It allows us to translate between lattice problems and problems of algebraic number theory, and gives us a notion of distance between elements of a number ring via the usual metric on $\mathbb{C}^n$. This type of study is referred to as *geometry of numbers* [Cas96]. Figure 4 demonstrates how the ring $\mathbb{Z}[x]/(\Phi_3(x)) \cong \mathbb{Z}[\zeta_3]$ embeds as a hexagonal lattice.

Definition 2.46. Let $\mathcal{L}$ be an n-dimensional lattice with basis $\{b_1, \dots, b_n\}$. The *fundamental domain* of $\mathcal{L}$ is the set

$$T = \left\{ \sum_{i=1}^{n} a_i b_i \mid a_i \in \mathbb{R},\ a_i \in [0, 1) \right\}.$$

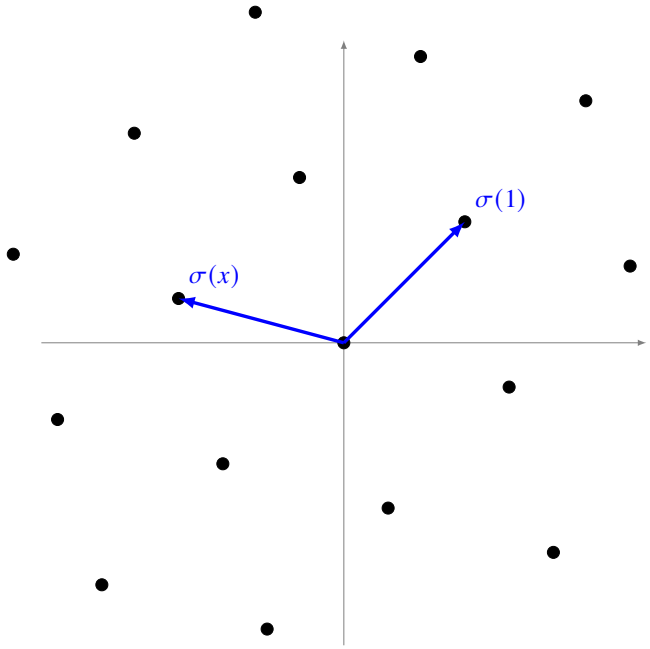


Figure 4: Minkowski embedding of $\mathbb{Z}[x]/(\Phi_3) \cong \mathbb{Z}[\zeta_3]$ is a hexagonal 2-dimensional lattice.

Notice that $\bigcup_{v\in\mathcal{L}}(v+T) = \mathbb{R}^n$, that is, the translates of the fundamental domain by lattice vectors tile the whole space with no overlap.

The volume of the fundamental domain of a lattice $\mathcal{L}$ is called the *determinant* of $\mathcal{L}$, denoted $\det(\mathcal{L})$ or $\mathrm{vol}(\mathcal{L})$. It is obtained as the absolute determinant of the basis matrix $B = [b_1, \ldots, b_n]$. Crucially, while the fundamental domain depends on the choice of basis, the volume of the fundamental domain does not. This follows from the fact that lattices are free abelian groups, and any change of basis matrix of a free abelian group is unimodular. In particular, the matrix has determinant ± 1. Figure 5 illustrates the invariance of the volume of fundamental domain.

Proposition 2.47. *The volume of the fundamental domain of the ring of integers $\mathcal{O}_K$ embedded in $\mathcal{M}_n$ can be given in terms of the field discriminant as $\sqrt{|\Delta_K|}$.*

Proof. Follows directly from the definition of the discriminant of a number field by using the fact that the determinant of a matrix gives the signed volume of the parallelepiped spanned by its columns. □

Definition 2.48. The ith *successive minima* of a given lattice $\mathcal{L}$ is defined as

$$\lambda_i(\mathcal{L}) = \min\{r \mid \dim(\mathrm{span}(\mathcal{L} \cap \bar{B}(0,r))) \geq i\}.$$

That is, λ_i is the minimum distance r such that the closed ball of radius r centered at the origin contains at least i linearly independent lattice vectors. As a special case for $i = 1$ we get the *minimum distance* λ_1 of the lattice $\mathcal{L}$, which is the shortest distance between any two points of $\mathcal{L}$.

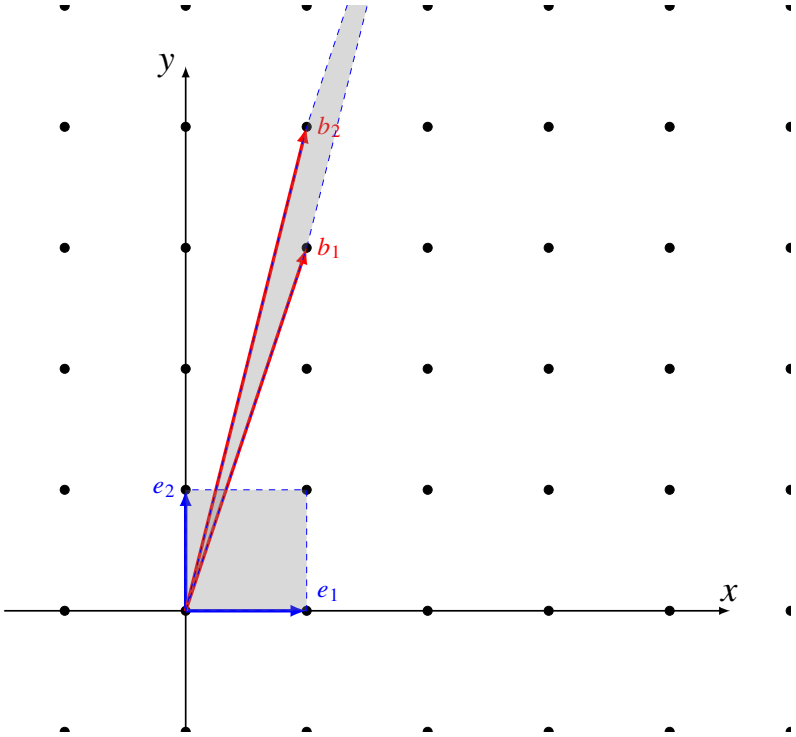


Figure 5: The additive subgroup $\mathbb{Z}^2$ in $\mathbb{R}^2$ is a lattice. The area shaded in gray is the fundamental domain of $\mathbb{Z}^2$. $[e_1, e_2]$ and $[b_1, b_2]$ are alternative bases for the same lattice.

We now define some optimization problems on lattices, which are fundamental to lattice-based cryptography.

Definition 2.49 (Shortest Vector Problem (SVP))**.** Given a lattice basis B, find a shortest non-zero vector in the lattice $\mathcal{L}(B)$. That is, a vector $\mathbf{v} \in \mathcal{L}(B)$ with $\|\mathbf{v}\| = \lambda_1(\mathcal{L}(B))$.

Notice that the shortest vector in a lattice is not unique: if $\|\mathbf{v}\| = \lambda_1$ we also have $-\mathbf{v} \in \mathcal{L}$ with $\|-\mathbf{v}\| = \lambda_1$ by the fact that lattices are additive groups. The number of shortest vectors of a lattice is called the *kissing number*.

Definition 2.50 (Closest Vector Problem (CVP))**.** Given a lattice basis B and a non-lattice target point $\mathbf{t}$, find the vector $\mathbf{v}$ in the $\mathbb{Z}$-span of B that is closest to $\mathbf{t}$. That is, find $\mathbf{v} \in \mathcal{L}(B)$ such that $\|\mathbf{v} - \mathbf{t}\| \leq \|\mathbf{u} - \mathbf{t}\|\ \forall \mathbf{u} \in \mathcal{L}(B)$.

Definition 2.51 (Bounded-Distance Decoding Problem (BDD))**.** Given a basis B of an n-dimensional lattice $\mathcal{L}(B)$, $\gamma \in \mathbb{R}$ with $\gamma < \lambda_1/2$ and a target point $\mathbf{t} \in \mathbb{R}^n$ satisfying $\text{dist}(\mathbf{t}, \mathcal{L}(B)) \leq \gamma$, find the unique closest lattice point $\mathbf{v} \in \mathcal{L}(B)$ to $\mathbf{t}$.

Definition 2.52 (Shortest Independent Vectors Problem (SIVP))**.** Given an n-dimensional lattice $\mathcal{L}$, find n linearly independent lattice vectors of length at most $\lambda_n(\mathcal{L})$. That is, find linearly independent $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathcal{L}$ such that $\max_i \|\mathbf{v}_i\| \leq \lambda_n$.

In practice, cryptosystems are rarely based on these exact search problems. Instead, they generally utilize either the following approximate versions, or decision variants formulated as gap problems. For the following, $\gamma = \gamma(n)$ is an approximation factor depending on the rank of the lattice.

Definition 2.53 (Approximate Shortest Vector Problem (SVP_γ))**.** Given a lattice basis B and $\gamma \geq 1$, find a short non-zero vector $\mathbf{v}$ in the lattice $\mathcal{L}(B)$ such that $\|\mathbf{v}\| \leq \gamma\lambda_1(\mathcal{L}(B))$.

Definition 2.54 (Approximate Shortest Independent Vectors Problem (SIVP_γ))**.** Given an n-dimensional lattice $\mathcal{L}$, find n linearly independent lattice vectors of length at most $\gamma\lambda_n(\mathcal{L})$. That is, find linearly independent $\mathbf{v}_1, ..., \mathbf{v}_n \in \mathcal{L}$ such that $\max_i \|\mathbf{v}_i\| \leq \gamma\lambda_n$.

Definition 2.55 (GapSVP_γ)**.** Given a basis B of an n-dimensional lattice $\mathcal{L}$, $\gamma \geq 1$ and $d \in \mathbb{Q}$, decide whether $\lambda_1(\mathcal{L}) \leq d$ or $\lambda_1(\mathcal{L}) > \gamma d$. Either answer is admissible if $\lambda_1(\mathcal{L})$ lies in the gap $(d, \gamma d]$.

Figure 6 illustrates SVP, SVP_γ and BDD.

It is important to note that these lattice problems are easy in two dimensions. However, as the dimension of the lattice increases, the problems quickly become intractable.

2.3 Cryptography

This section describes the notions from cryptography important to this thesis. We also give a brief description of the Learning with Errors problem and how it relates to lattices.

In this thesis, we consider a problem hard if there is no algorithm capable of solving it in polynomial time in the security parameter n when n is large enough. The security parameter is a quantity that measures the size of the input; in our context, it usually corresponds to the degree of the number field under consideration or, equivalently, the lattice dimension. A *worst-case hard* problem is a problem whose worst-case instances are hard to solve. Lattice problems such as SVP and SIVP, as well as their approximate variants SVP_γ and SIVP_γ introduced in Section 2.2, are considered worst-case hard in high dimensions.

For cryptographic applications, being hard in the worst case is generally not enough. Security requires the underlying problem to be hard for a randomly chosen instance, namely *average-case hardness*.

Hardness of a problem in cryptography is commonly proven by showing that the ability to solve the problem would allow one to solve a different problem which is known or believed to be hard. This is called *reduction*, and we say P *reduces* to Q, if the ability to solve Q allows you to solve P. For example, Ajtai's pioneering work in 1996 [Ajt96] introduced a central technique in lattice-based cryptography for guaranteeing the hardness of a cryptosystem called *worst-case to average-case reduction*, where one constructs an average-case hard problem whose average instances correspond to the hard instances of a worst-case hard problem. Such a cryptographic protocol

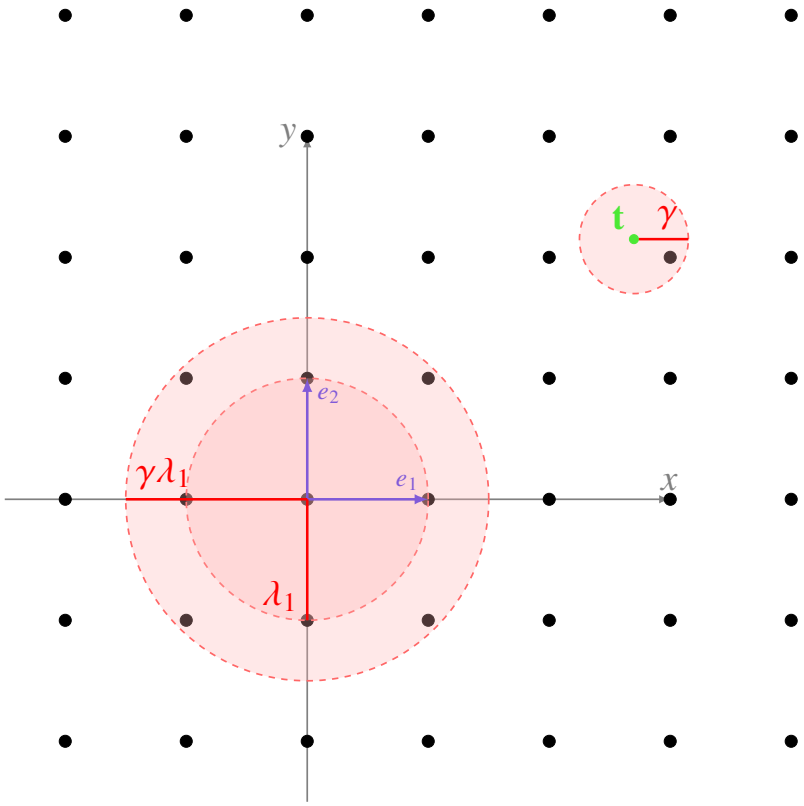


Figure 6: Bounded Distance Decoding, Shortest Vector Problem and its approximate version in two dimensions.

enjoys a strong security guarantee, as a random instance of the problem is, with high probability, a hard problem.

In Regev's paper introducing the LWE problem, its hardness was shown via a quantum reduction from worst-case lattice problems, such as SVP_γ and SIVP_γ [Reg05; Reg09]. Since then, much of modern lattice-based cryptography has been built from variants of LWE, including RLWE and PLWE. In the remainder of this section, we introduce LWE.

Sample a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$ and random vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$, and return pairs $(\mathbf{a}_i, \langle \mathbf{s}, \mathbf{a}_i \rangle + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where e_i is a small error sampled from a discrete error distribution over the integers modulo q. The search version of the problem, called the search LWE problem, consists of finding the secret $\mathbf{s}$ given arbitrarily many such pairs. Decision version consists of determining whether the samples are generated by the process described above, or chosen uniformly at random.

The search LWE problem is a problem of solving a noisy linear system. As we know, solving a linear system is easy using, for instance, Gaussian elimination. Thus, the error added to the inner products is of central importance, and the choice of parameters for the noise distribution the errors are drawn from is key in construction cryptosystems relying on LWE. Intuitively, the noise needs to be large enough so that

the linear system cannot be correctly inverted, ensuring that the encryption is secure. At the same time, the noise must not be too large, or the messages can no longer be correctly decrypted.

We can translate the search LWE problem into a lattice problem as follows. Suppose we are given m LWE samples $(\mathbf{a}_i, b_i = \langle \mathbf{s}, \mathbf{a}_i \rangle + e_i)$ and we stack the vectors $\mathbf{a}_i$ into a matrix $A \in \mathbb{Z}_q^{n \times m}$. Then the set

$$\mathcal{L}(A) = \{\mathbf{z} \in \mathbb{Z}^m \mid \mathbf{z}' = A^T \mathbf{s} \text{ for some } \mathbf{s} \in \mathbb{Z}_q^n,\ \mathbf{z} \equiv \mathbf{z}' \pmod{q}\}$$

forms a lattice [Chi+15, Section 2.1.2]. From this we notice that the search LWE problem corresponds to a BDD problem on a lattice.

LWE pairs can be utilized in public key encryption to form keys, which requires n multiplications in the form of the inner product [Chi+15, Section 2.2.1]. Moreover, the public key contains the matrix A, and therefore requires $O(n^2)$ space. The structured LWE variants RLWE and PLWE which we discuss in the next section were introduced to address these practical inefficiencies.

3 Overview of RLWE and PLWE

This section discusses ring learning with errors and polynomial learning with errors. We define RLWE and PLWE distributions and problems as well as equivalence of RLWE and PLWE. Finally, we highlight some known RLWE/PLWE equivalence results.

3.1 RLWE and PLWE problems

The LWE problem introduced in [Reg05] plays a central role in lattice-based cryptography owing to its simplicity and strong security guarantees. However, it is not very efficient for practical application due to its quadratic overhead. In order to address these limitations, Luybashevsky et al. introduced a structured version of the LWE problem called Ring Learning With Errors (RLWE) [LPR10]. It improves efficiency to linear in the security parameter while maintaining strong security guarantees, which can be seen from its reduction from a well-known worst-case hard problem. Despite the many advantages of RLWE, the related ring structure may not always be practical for implementation. More practical rings are used in Polynomial Learning With Errors (PLWE) problem, which was introduced in [Ste+09] as ideal-LWE. We begin by formally defining RLWE and PLWE distributions and problems below.

Definition 3.1. Let K be an algebraic number field with ring of integers $\mathcal{O}_K$ and q a rational prime. Let χ be a discrete random distribution over $\mathcal{O}_K/q\mathcal{O}_K$. For $s \in \mathcal{O}_K/q\mathcal{O}_K$, the (primal) *RLWE distribution* $\mathcal{A}_{s,\chi}$ is the distribution over $\mathcal{O}_K/q\mathcal{O}_K \times \mathcal{O}_K/q\mathcal{O}_K$ obtained by sampling an element a uniformly from $\mathcal{O}_K/q\mathcal{O}_K$, e drawn from χ, and returning the pair $(a, as + e)$.

Lyubashevsky et al. showed that the RLWE distribution is pseudorandom [LPR10, Section 4]. This was done via a quantum reduction from worst-case SVP_γ on ideal lattices. That is, if SVP_γ is hard in the worst case on ideal lattices for quantum algorithms, then RLWE samples look pseudorandom to any polynomial-time attacker.

Rings of integers used in RLWE are convenient for security proofs, but in general they may be difficult objects to work with. For this reason, we have the following related lattice problem using the more concrete polynomial rings, which may be more practical for cryptographic applications.

Definition 3.2. Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial, $\mathcal{O}_f$ the quotient ring $\mathbb{Z}[x]/(f(x))$ and q a rational prime. Let χ be a discrete random distribution over $\mathcal{O}_f/q\mathcal{O}_f$. For $s \in \mathcal{O}_f/q\mathcal{O}_f$, the *PLWE distribution* $\mathcal{B}_{s,\chi}$ is the distribution over $\mathcal{O}_f/q\mathcal{O}_f \times \mathcal{O}_f/q\mathcal{O}_f$ obtained by sampling an element a uniformly from $\mathcal{O}_f/q\mathcal{O}_f$, e drawn from χ, and returning the pair $(a, as + e)$.

With the notation established above, we define the RLWE/PLWE search and decision problems:

Definition 3.3 (RLWE/PLWE decision problems)**.** Given access to arbitrarily many independent samples, decide with non-negligible advantage whether the sampled distribution is uniform or an RLWE/PLWE distribution.

Definition 3.4 (RLWE/PLWE search problems)**.** Given access to arbitrarily many independent samples from $\mathcal{A}_{s,\chi}$ ($\mathcal{B}_{s,\chi}$ for PLWE) for an arbitrary secret s, find s with non-negligible advantage, i.e., significantly better than by random guessing.

Notice that, in contrast to the inner product in the unstructured LWE setting, the product of two elements of the rings O_K/qO_K and O_f/qO_f is again an element of the same ring, thus encoding n bits of information, when $[K : \mathbb{Q}] = n$ or $\deg f(x) = n$. Furthermore, this structure also lowers the storage requirement of public keys to $\tilde{O}(n)$.

Originally, RLWE was formulated using $O_K^\vee$, the dual of the ring of integers of K [LPR10]. However, [RSW18] showed that there exist reductions between the primal and dual versions. Hence, unless otherwise stated, we only consider the primal versions of the RLWE and PLWE problems in this thesis.

3.2 Equivalence of RLWE and PLWE

Despite the strong security guarantee enjoyed by RLWE, PLWE is generally the problem employed in practice. The preference for PLWE is due to polynomial rings being simpler to characterize, and further improvements to arithmetic efficiency achieved by optimizations such as Toom–Cook and Karatsuba algorithms [Aho+25, Section 1.1]. Moreover, additional efficiency improvements up to quasilinear time are possible using Number Theoretic Transform (NTT) [AB75; LS19].

To simultaneously enjoy both the practical benefits of PLWE as well as the security of RLWE, we must establish an equivalence between RLWE and PLWE. We study this equivalence for a specific class of fields in Section 4. The suitable sense of equivalence is captured by the following definition.

Definition 3.5. Let K be the splitting field of a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$. Then the RLWE and PLWE problems are called *equivalent* if there exists an algorithm taking any RLWE sample into a PLWE sample and vice versa in probabilistic polynomial time in the degree of K over $\mathbb{Q}$ while incurring a noise increase, which is at most polynomial in the degree of K.

The transformation of PLWE samples from the polynomial ring into RLWE samples in the Minkowski space $\mathcal{M}_n$ is achieved by left-multiplying the coefficient vector by a matrix as follows:

$$V_f : \mathbb{Z}[x]/(f(x)) \to \sigma_1(O_K) \times \cdots \times \sigma_n(O_K)$$

$$a(x) = \sum_{i=0}^{n-1} a_i x^i \mapsto V_f \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & \theta_1 & \dots & \theta_1^{n-1} \\ 1 & \theta_2 & \dots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \dots & \theta_n^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix} = \begin{bmatrix} a(\theta_1) \\ a(\theta_2) \\ \vdots \\ a(\theta_n) \end{bmatrix}. \quad (1)$$

This takes reduced sampled polynomials to their evaluations at the Galois conjugates θ_i of the generating element θ of the ring of integers. The transformation is easily done in polynomial time, hence the constraining factor of RLWE/PLWE equivalence is the effect of the transformation on noise.

Similarly to [RSW18], the noise increase of this transformation is measured by a quantity called the condition number. To introduce condition number, we must first define a matrix norm.

Definition 3.6. The *Frobenius norm* $\|\cdot\|$ of a matrix $A \in \mathrm{GL}_n(\mathbb{C})$ is

$$\|A\| = \sqrt{\mathrm{Tr}(AA^*)} = \sqrt{\sum_{i,j} |a_{ij}|^2},$$

where Tr is the usual matrix trace and A^* denotes the conjugate transpose of A.

Definition 3.7. The *condition number* $\kappa(A)$ of a matrix A, with respect to the Frobenius norm, is defined as

$$\kappa(A) = \|A\|\|A^{-1}\|.$$

In general, the condition number measures how sensitive a linear system is to errors. As a rule of thumb, if the condition number of a matrix A is 10^k, one can expect to lose k digits of precision when solving a linear system involving A [CK07, p. 321].

Below, we briefly review some known equivalence results.

3.3 Brief review of known equivalence results

As shown in [DD12], and more concisely in [Bla22a, Theorem 3.1], the sample transformation between RLWE and PLWE for power-of-two cyclotomic polynomials is a scaled isometry. In other words, the embedding is a combination of a rigid rotation and a scaling. Due in part to this simplicity, power-of-two cyclotomics have become the main fields used in practical implementations of RLWE. However, this class of fields lacks granularity for tuning the desired security level and thus is not optimal for all applications. Furthermore, even though power-of-two cyclotomics seem to not be affected by the known attacks on PLWE, it is beneficial to have other practical options available in case a vulnerability in 2-power cyclotomics is found. To this end, the equivalence of RLWE and PLWE has gained much attention.

Despite the general nice properties enjoyed by cyclotomic fields and the popularity of power-of-two cyclotomics in cryptography, we know by [DSS24] that RLWE and PLWE are not equivalent for general cyclotomic fields. [Bla22a] showed that as long as the number of prime divisors of n is kept constant, we have RLWE/PLWE equivalence for $\mathbb{Q}(\zeta_n)$. However, the general condition number bound obtained is a high-degree polynomial in n.

By focusing on the case where the conductor is either $n = p^s$ or $n = 2^r p^s$ for an odd prime p, [DSS21] were able to improve the bound for the case of prime power conductor from [Bla22a]. [Bla+25] brought further improvements for the upper bound for nth cyclotomic fields when n is divisible by up to six distinct primes. In addition, the authors derived an exact formula for the condition number under a modified basis, which also leads to equivalence in this basis as long as the number of distinct prime divisors of n is $O(\log(n))$.

An important question that arises is whether other practical classes of fields enjoy RLWE/PLWE equivalence. This question was answered in the affirmative in [Bla22b], where the author proves RLWE/PLWE equivalence for the maximal real subfield of the $4p$th cyclotomic field, with p being a rational prime. These maximal real subfields of cyclotomic fields have received further attention, as they inherit some nice properties from cyclotomic fields. Namely, they are monogenic, and, as subfields of cyclic fields, they are also cyclic. Additionally, maximal real subfields of cyclotomic fields enjoy quasilinear-time arithmetic via Discrete Cosine Transform (DCT) [Aho+25, Section 4]. RLWE/PLWE equivalence has since been shown for maximal real subfields of cyclotomic fields of conductor $n = 2^r pq$, with $p \neq q$ odd primes in [BL21], $n = 3^s$ or $n = 2^r 3^s$ in [Aho+25], and generalized to $n = p^s$ or $n = 2^r p^s$ for an odd prime p in [BHS25].

Other fields which have been considered are cyclo-multiquadratic fields, introduced in [Bla+25]. A cyclo-multiquadratic field is the compositum of a cyclotomic and a multiquadratic field $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_r})$, where d_i are suitably chosen squarefree positive integers. This family of fields is proposed as a way to improve the efficiency of converting ring elements between different representations, which is frequently needed in current state-of-the-art implementations of homomorphic encryption [Bla+25, Section 2]. The authors show that, with appropriate choice of parameters, RLWE and PLWE are equivalent for cyclo-multiquadratic fields.

In Section 4, we study the equivalence for another class of fields, which we call *real cyclo-multiquadratic*, defined as the compositum of the maximal real subfield of a cyclotomic field and a multiquadratic field.

4 RLWE/PLWE equivalence over real cyclo-multiquadratic fields

In this section, we present our main result. We begin by gathering some further notions and tools necessary for our proof. Section 4.3 contains our proof of RLWE/PLWE equivalence for real cyclo-multiquadratic number fields, when the conductor of the maximal real subfield of a cyclotomic field is p^s or $2^r p^s$, $s \geq 1, r \geq 2$, for an odd prime p.

4.1 Kronecker product

To describe the RLWE/PLWE sample transformation matrix for real cyclo-multiquadratic fields, we introduce a special case of a tensor product for matrices called a Kronecker product.

Definition 4.1. Let $A = (a_{ij}) \in \mathrm{M}_{m\times n}(\mathbb{C})$ and $B = (b_{ij}) \in \mathrm{M}_{p\times q}(\mathbb{C})$ be matrices. Then the *Kronecker product* of A and B is

$$A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{bmatrix}.$$

The embedding change matrix for real cyclo-multiquadratic fields is not a simple Vandermonde matrix like in Eq. (1). Instead, it is a Kronecker product of individual Vandermonde and quasi-Vandermonde matrices.

The Kronecker product behaves nicely with the Frobenius norm. Namely, the Frobenius norm of a Kronecker product of two matrices is the product of the individual Frobenius norms [Bla+25, Lemma 3.8]:

$$\|A \otimes B\| = \|A\|\|B\|.$$

Furthermore, $A \otimes B$ is invertible if and only if both A and B are invertible [Bla+25, Lemma 3.7]. When this is the case,

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

It then follows that the condition number with respect to the Frobenius norm satisfies the following useful property with the Kronecker product.

Lemma 4.2. *For $A \in GL_n(\mathbb{C})$ and $B \in GL_m(\mathbb{C})$, we have*

$$\kappa(A \otimes B) = \kappa(A)\kappa(B).$$

Proof. See [Bla+25, Corollary 3.9]. □

This property of the Kronecker product with the condition number is central in the proof of the main result of this thesis, Theorem 4.12 and Theorem 4.13.

4.2 Modified Chebyshev polynomials

For the maximal real subfields of cyclotomic fields, it is convenient to use a different basis than the usual power basis in the PLWE setting of $\mathbb{Z}[x]/(\Psi_n(x))$, where $\Psi_n(x)$ is the minimal polynomial of $\psi_n = \zeta_n + \zeta_n^{-1}$ over $\mathbb{Q}$. This basis is constructed from the Chebyshev polynomials of the first kind [CK07, Chapter 12.2], modified to retain the nice properties of the original polynomials with respect to cosines with ψ_n, where we have additional factors of 2.

Definition 4.3. The family $P_i(x)$ of *modified Chebyshev polynomials* is defined recursively by

$$P_n(x) = xP_{n-1}(x) - P_{n-2}(x) \quad n \geq 3,$$

with the initializing sequence $P_0(x) = 1,\ P_1(x) = x,\ P_2(x) = x^2 - 2$.

Since the elements of the set $\{P_i(x)\}_{i=0}^{N-1}$, where $N = \varphi(n)/2$, are polynomials of pairwise distinct degrees, they are clearly linearly independent over $\mathbb{Z}$. Furthermore, as all $P_i(x)$ are monic and have integer coefficients, they form a basis for $\mathbb{Z}[x]/(\Psi_n(x))$. Additionally, notice that defining the modified Chebyshev polynomials this way gives

$$P_n(2\cos(\theta)) = 2\cos(n\theta) \quad \forall\theta,\ \forall n \geq 1.$$

Remark. The condition number results in [Aho+25] and [BHS25] are obtained under the modified Chebyshev basis. However, the equivalence result holds for the power basis as well. This is because, as shown in [Aho+25, Section 5], the change of basis between modified Chebyshev and power bases can be performed in quasilinear time, which keeps the sample transformation still in polynomial time. Furthermore, the error is not affected: we may sample polynomials a, s, e in the power basis, perform a basis change for a and s to multiply them efficiently using DCT in the modified Chebyshev basis, and finally perform another basis change back to the power basis and add the error.

We may express the minimal polynomials of $2\cos(2\pi/n)$ in the cases of interest to us using the modified Chebyshev polynomials as follows.

Proposition 4.4 (Corollary 3.1 [BHS25])**.** *Let p be an odd prime, $s \geq 1$, $n = p^s$ and $k = (p-1)/2$. Then the minimal polynomial of ψ_n is*

$$\Psi_n(x) = \sum_{i=0}^{k} P_{ip^{s-1}}(x).$$

Proposition 4.5 (Corollary 3.2 [BHS25])**.** *Let p be an odd prime, $n = 2^r p^s$, $k = (p-1)/2$ and $N = \varphi(n)/2 = (p-1)2^{r-2}p^{s-1} = [\mathbb{Q}(\psi_n) : \mathbb{Q}]$. Then the minimal polynomial of ψ_n is*

$$\Psi_n(x) = \sum_{i=0}^{k} (-1)^{k-i} P_{i2^{r-1}p^{s-1}}(x).$$

4.3 RLWE/PLWE equivalence for a family of real cyclo-multiquadratic fields

This section presents our main result. We start by fixing some notation for this section. Denote by $\psi_n = \zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$ and $\Psi_n(x)$ its minimal polynomial over $\mathbb{Q}$. Let $K_n = \mathbb{Q}(\psi_n)$ be the maximal real subfield of the nth cyclotomic field, $O_{K_n} = \mathbb{Z}[\psi_n]$ its ring of integers and $N = \varphi(n)/2$ its degree over $\mathbb{Q}$. Further, let K denote the compositum of K_n and $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})$, where p_i are distinct primes, which we call a *real cyclo-multiquadratic* field. For a number field K, let Δ_K denote its discriminant. Finally, recall that number fields K and L are called *linearly disjoint*, if $K \cap L = \mathbb{Q}$.

Lemma 4.6. *Let $K_n = \mathbb{Q}(\psi_n)$ be a number field. Choose primes $p_1, \ldots, p_r$ such that $p_i \nmid n$ for all i. Then $K_n \cap \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r}) = \mathbb{Q}$.*

Proof. First consider the subextension $\mathbb{Q}(\sqrt{p_1})$. Suppose for a contradiction that $K_n \cap \mathbb{Q}(\sqrt{p_1}) = \mathbb{Q}(\sqrt{p_1})$, and thus $\mathbb{Q}(\sqrt{p_1}) \subseteq K_n$. But we know from Theorem B.1 that the discriminant of K_n can only contain as prime divisors the primes dividing the discriminant of the nth cyclotomic field, namely the factors of n. Hence, if $\mathbb{Q}(\sqrt{p_1}) \subseteq K_n$, p_1 would ramify in $\mathbb{Q}(\zeta_n)$. But we know that the primes which ramify in $\mathbb{Q}(\zeta_n)$ are precisely the prime divisors of n. Therefore, we have a contradiction to our choice $p_i \nmid n$. The claim then follows for arbitrary r inductively by applying the same argument to $K_n(\sqrt{p_1}) \cap \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$. □

In addition, we know from Proposition B.3 that, for linearly disjoint Galois fields, the Galois group of their composite field is isomorphic to the direct product of their individual Galois groups. Since square roots of primes are clearly linearly independent over $\mathbb{Q}$, the following result follows immediately.

Proposition 4.7. *Let $K_n = \mathbb{Q}(\psi_n)$ be a number field and $p_1, \ldots, p_r$ rational primes such that $p_i \nmid n$ for all i. Then the Galois group of the composite $K = K_n\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})$ is isomorphic to the direct product*

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(K_n/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\sqrt{p_r})/\mathbb{Q}).$$

Proof. Combine Lemma 4.6 and Proposition B.3. □

We know from Theorem B.2 that for number fields with coprime discriminants, the ring of integers of the composite field is a $\mathbb{Z}$-module tensor product of the individual rings of integers. This extends to arbitrary r number of finite extensions with pairwise coprime discriminants by a simple induction argument, as shown in [Nar04, p. 160]. By the ramification argument from Lemma 4.6, we see that our real cyclo-multiquadratic fields with $p_i \nmid n$, with the additional requirement that $p_i \equiv 1 \pmod 4$ so that $\Delta_{\mathbb{Q}(\sqrt{p_i})} = p_i$, fulfill these criteria and therefore we have

$$O_K \cong O_{K_n} \otimes_{\mathbb{Z}} O_{\sqrt{p_1}} \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} O_{\sqrt{p_r}}. \tag{2}$$

Denote

$$\mathcal{O} = \mathbb{Z}[x]/(\Psi_n) \otimes_{\mathbb{Z}} \mathbb{Z}[x]/(m_1) \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[x]/(m_r), \tag{3}$$

where

$$m_i(x) = \begin{cases} x^2 - p_i, & p_i \equiv 2,3 \pmod 4 \\ x^2 - x + \frac{1-p_i}{4}, & p_i \equiv 1 \pmod 4 \end{cases}$$

are the minimal polynomials of p_i over $\mathbb{Q}$ and Ψ_n is the minimal polynomial of $2\cos(2\pi/n)$ over $\mathbb{Q}$.

Lemma 4.8. *Let $\mathcal{O}$ be the tensor product given in Eq. (3). Then we have*

$$\mathcal{O} \cong \mathcal{O}_K.$$

Proof. It is well known that the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{d})$ for a squarefree integer d is $\mathbb{Z}[\epsilon_d]$, where

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

With that, denote

$$\epsilon_i = \begin{cases} \sqrt{p_i}, & p_i \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{p_i}}{2}, & p_i \equiv 1 \pmod 4. \end{cases}$$

Since quadratic fields and maximal real subfields of cyclotomic fields are both monogenic, meaning their rings of integers are $\mathbb{Z}[\epsilon]$ and $\mathbb{Z}[\psi_n]$ respectively with simple power bases, successive evaluation at $\psi_n, \epsilon_1, \ldots, \epsilon_r$ yields the desired isomorphism

$$\mathcal{O} = \mathbb{Z}[x]/(\Psi_n) \otimes_Z \mathbb{Z}[x]/(m_1) \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathbb{Z}[x]/(m_r) \cong \mathcal{O}_{K_n} \otimes_{\mathbb{Z}} \mathcal{O}_{\sqrt{p_1}} \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} \mathcal{O}_{\sqrt{p_r}}.$$

□

As shown in [Bla+25], the embedding change matrices V_{p_i} for quadratic fields are given by

$$V_{p_i} = \begin{cases} \begin{bmatrix} 1 & \sqrt{p} \\ 1 & -\sqrt{p} \end{bmatrix}, & p_i \equiv 2,3 \pmod 4 \\ \begin{bmatrix} 1 & \frac{1+\sqrt{p}}{2} \\ 1 & \frac{1-\sqrt{p}}{2} \end{bmatrix}, & p_i \equiv 1 \pmod 4 \end{cases}$$

and the associated condition numbers with respect to the Frobenius norm are

$$\kappa(V_{p_i}) = \begin{cases} \sqrt{p_i} + \frac{1}{\sqrt{p_i}}, & p_i \equiv 2,3 \pmod 4 \\ \frac{5}{2\sqrt{p_i}} + \frac{\sqrt{p_i}}{2}, & p_i \equiv 1 \pmod 4. \end{cases} \tag{4}$$

Explicit computation of the condition numbers is left to Appendix A for expositional clarity.

Corollary 4.9. *For each prime $p \geq 2$,*

$$\kappa(V_p) \leq 1 + \sqrt{p}.$$

Proof. Consider

$$1 + \sqrt{p_i} - \kappa(V_{p_i}) = \begin{cases} \frac{\sqrt{p_i}-1}{\sqrt{p_i}}, & p_i \equiv 2,3 \pmod 4 \\ \frac{p_i+2\sqrt{p_i}-5}{2\sqrt{p_i}}, & p_i \equiv 1 \pmod 4. \end{cases}$$

One easily verifies that for $p_i \equiv 2,3 \pmod 4$, the difference is nonnegative whenever $p_i \geq 1$ and for $p_i \equiv 1 \pmod 4$ we find the cutoff to be $7 - 2\sqrt{6} \approx 2.1$. □

In the modified Chebyshev basis $\{P_0(x), \ldots, P_{N-1}(x)\}$, the Minkowski embedding $\mathbb{Z}[x]/(\Psi_n) \to \mathcal{M}_N$ is given by

$$\sum_{i=0}^{N-1} a_i P_i(x) \mapsto V_{K_n} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N-1} \end{bmatrix},$$

where

$$V_{K_n} = \begin{bmatrix} 1 & 2\cos(2\pi/n) & 2\cos(2\pi 2/n) & \ldots & 2\cos(2\pi(N-1)/n) \\ \vdots & \vdots & \vdots & \vdots & \\ 1 & 2\cos(2\pi\eta_1/n) & 2\cos(2\pi\eta_1 2/n) & \ldots & 2\cos(2\pi\eta_1(N-1)/n) \\ \vdots & \vdots & \vdots & \vdots & \\ 1 & 2\cos(2\pi\eta_{N-1}/n) & 2\cos(2\pi\eta_{N-1}2/n) & \ldots & 2\cos(2\pi\eta_{N-1}(N-1)/n) \end{bmatrix},$$

with $\eta_i \in \{1, \ldots, n/2\}$ and $\gcd(\eta, n) = 1$, as shown in [BHS25, p. 17].

The full embedding change is then given by

$$V_K : \mathcal{O} \to \sigma_1(\mathcal{O}_K) \times \cdots \times \sigma_{N2^r}(\mathcal{O}_K)$$

$$\sum_{i=0}^{N2^r-1} a_i \bar{x}^i \mapsto V_K \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{N2^r-1} \end{bmatrix},$$

where $V_K = V_{K_n} \otimes V_{\sqrt{p_1}} \otimes \cdots \otimes V_{\sqrt{p_r}}$.

Remark. The form of the transformation matrix V_K can be seen to result from the structure of the Galois group of the full composite field K. By Proposition 4.7, the Galois automorphisms of K are of the form

$$\sigma_{k_0,k_1,\ldots,k_r} := \sigma_{k_0}^{(0)} \circ \sigma_{k_1}^{(1)} \circ \cdots \circ \sigma_{k_r}^{(r)},$$

where $\sigma_{k_0}^{(0)} \in \mathrm{Gal}(K_n/\mathbb{Q})$, $\sigma_{k_i}^{(i)} \in \mathrm{Gal}(\mathbb{Q}(\sqrt{p_i})/\mathbb{Q})$ for $i \in \{1, \ldots, r\}$, and $k_0 \in \{1, 2, \ldots, N\}$ and $k_1, \ldots, k_r \in \{1, 2\}$. The block matrix form of a Kronecker product follows from permuting the indices k_i. Alternatively, the Kronecker product form simply follows from the tensor product structure of $\mathcal{O}_K$.

Lemma 4.10 (Theorem 4.1 [BHS25]). *For $n = p^s$ with $p \geq 3$ prime, $s \geq 1$, $k = (p^s - 1)/2$,*

$$\kappa(V_{K_n})^2 < 3k\kappa(C_{k+1})^2 < 3k(\sqrt{2}(k+1))^2 = \frac{3}{4}(n^3 + n^2 - n - 1),$$

where V_{K_n} is the embedding change matrix for $\mathbb{Q}(\psi_n)$, the maximal real subfield of the nth cyclotomic field.

Lemma 4.11 (Theorem 4.2 [BHS25]). *For $n = 2^r p^s$ with $p \geq 3$ prime, $r \geq 2$, $s \geq 1$, $k = 2^{r-2}p^s - 1$,*

$$\kappa(V_{K_n})^2 < 3k\kappa(C_{k+1})^2 < \frac{3}{32}n^3 - \frac{3}{8}n^2$$

where V_{K_n} is the embedding change matrix for $\mathbb{Q}(\psi_n)$, the maximal real subfield of the nth cyclotomic field.

Theorem 4.12. *Let $n = p^s$, with $p \geq 3$ prime and $s \geq 1$. Let K be the real cyclo-multiquadratic number field obtained as the compositum of $K_n = \mathbb{Q}(\psi_n)$ and $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})$. Then the condition number of the linear transformation taking PLWE samples into RLWE samples is*

$$\kappa(V_K) < \sqrt{3}n^{3/2} \prod_{i=1}^{r} (1 + \sqrt{p_i}).$$

Proof. Combine Lemma 4.10, Corollary 4.9 and Lemma 4.2. Explicit bound approximations can be found in Appendix C. □

Theorem 4.13. *Let $n = 2^r p^s$, with $p \geq 3$ prime and $r \geq 2$, $s \geq 1$. Let K be the real cyclo-multiquadratic number field obtained as the compositum of $K_n = \mathbb{Q}(\psi_n)$ and $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_r})$. Then the condition number of the linear transformation taking PLWE samples into RLWE samples is*

$$\kappa(V_K) < \frac{\sqrt{6}}{8}n^{3/2} \prod_{i=1}^{r} (1 + \sqrt{p_i}).$$

Proof. As above, use Lemma 4.11, Corollary 4.9 and Lemma 4.2. Explicit bound approximations can be found in Appendix C. □

Because of the condition $p_i \equiv 1 \pmod 4$, the minimal polynomials defining the quadratic fields are $m_i(x) = x^2 - x + \frac{1-p_i}{2}$. Due to this, we need to apply a map from $O_K \to \mathbb{Z}[x_0, x_1, \ldots, x_r]/(\Psi_n(x_0), x_1^2 - p_1, \ldots, x_r^2 - p_r)$, which consists of a substitution $x_i \to \frac{x_i+1}{2}$ for the PLWE sample elements (a_i, b_i), and then multiplication of the PLWE elements by 2 [Ped+21, p. 15–16]. In the end, this results in an increase in the upper bound for $\kappa(V_{p_i})$ from $1 + \sqrt{p_i}$ to $1 + 3\sqrt{p_i}/2$ [Bla+25, p. 21–22]. We have elected to omit this consideration in the exposition of our proof, as the effect of this transformation is negligible.

5 Summary

In this thesis, we described Ring Learning With Errors (RLWE) and Polynomial Learning With Errors (PLWE) and defined the equivalence of the RLWE and PLWE problems. This study was motivated by the dire need to find more candidate fields potentially suitable to be used in lattice-based cryptography, withstanding the quantum threat. We considered a family of fields which we call real cyclo-multiquadratic. As our main contribution, we proved that RLWE and PLWE are equivalent for real cyclo-multiquadratic fields when the conductor of the maximal real subfield of a cyclotomic field in the compositum is either p^s or $2^r p^s$ for an odd prime p, $s \geq 1$, $r \geq 2$. Additionally, as a part of our proof, we obtained an improved upper bound for the embedding change matrix of a real quadratic field.

Our equivalence result shows that real cyclo-multiquadratic fields benefit from the security guarantees from RLWE when the conductor of the maximal real subfield of a cyclotomic field in the compositum is p^s or $2^r p^s$, $s \geq 1$, $r \geq 2$ and p an odd prime. To make lattice-based protocols more efficient for this class of fields, further research into arithmetic over these fields is required. We also suggest that a heuristic search for weak instances of our fields against known root-based attacks be performed.

References

[AB75] Ramesh C Agarwal and C Sidney Burrus. "Number theoretic transforms to implement fast digital convolution". In: *Proceedings of the IEEE* 63.4 (1975), pp. 550–560.

[Aho+25] Joonas Ahola, Iván Blanco-Chacón, Wilmar Bolaños, Antti Haavikko, Camilla Hollanti, and Rodrigo M. Sánchez-Ledesma. "Fast multiplication and the PLWE–RLWE equivalence for an infinite family of maximal real subfields of cyclotomic fields". In: *Designs, Codes and Cryptography* (2025). DOI: 10.1007/s10623-025-01601-3.

[Ajt96] Miklós Ajtai. "Generating hard instances of lattice problems (extended abstract)". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 99–108. DOI: 10.1145/237814.237838.

[Alu09] Paolo Aluffi. *Algebra: Chapter 0*. Reprinted with corrections. USA: American Mathematical Society, 2009. 713 pp. ISBN: 978-0-8218-4781-7.

[Bla22a] Iván Blanco-Chacón. "On the RLWE/PLWE equivalence for cyclotomic number fields". In: *Applicable Algebra in Engineering, Communication and Computing* 33.1 (2022), pp. 53–71. DOI: 10.1007/s00200-020-00433-z.

[Bla22b] Iván Blanco-Chacón. "RLWE/PLWE equivalence for totally real cyclotomic subextensions via quasi-Vandermonde matrices". In: *Journal of Algebra and Its Applications* 21.11 (2022), p. 2250218. DOI: 10.1142/S0219498822502188.

[BL21] Iván Blanco-Chacón and Lorena López-Hernanz. *RLWE/PLWE equivalence for the maximal totally real subextension of the $2^r pq$-th cyclotomic field*. 2021. arXiv: 2111.13484 [cs.CR]. URL: https://arxiv.org/abs/2111.13484.

[Bla+25] Iván Blanco-Chacón, Alberto Pedrouzo-Ulloa, Rahinatou Y. Njah Nchiwo, and Beatriz Barbero-Lucas. "Fast polynomial arithmetic in homomorphic encryption with cyclo-multiquadratic fields". In: *Cryptography and Communications* (2025). DOI: 10.1007/s12095-024-00771-6.

[BHS25] Wilmar Bolaños, Antti Haavikko, and Rodrigo M. Sánchez-Ledesma. *A Fast Multiplication Algorithm and RLWE-PLWE Equivalence for the Maximal Real Subfield of the $2^r p^s$-th Cyclotomic Field*. Cryptology ePrint Archive, Paper 2025/994. 2025. URL: https://eprint.iacr.org/2025/994.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. "Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages". In: *Advances in Cryptology – CRYPTO 2011*. Ed. by Phillip Rogaway. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 505–524. DOI: 10.1007/978-3-642-22792-9_29.

[Cas96] John William Scott Cassels. *An introduction to the geometry of numbers*. Springer Berlin, Heidelberg, 1996. 345 pp. ISBN: 978-3-540-61788-4. DOI: 10.1007/978-3-642-62035-5.

[CK07] E. Ward Cheney and David R. Kincaid. *Numerical Mathematics and Computing*. 6th. USA: Brooks/Cole Publishing Co., 2007. ISBN: 0495114758.

[Chi+15] Dong Pyo Chi, Jeong Woon Choi, Jeong San Kim, and Taewan Kim. *Lattice Based Cryptography for Beginners*. Cryptology ePrint Archive, Paper 2015/938. 2015. URL: https://eprint.iacr.org/2015/938.

[DSS21] Antonio J. Di Scala, Carlo Sanna, and Edoardo Signorini. "On the condition number of the Vandermonde matrix of the nth cyclotomic polynomial". In: *Journal of Mathematical Cryptology* 15.1 (2021), pp. 174–178. DOI: 10.1515/jmc-2020-0009.

[DSS24] Antonio J. Di Scala, Carlo Sanna, and Edoardo Signorini. "RLWE and PLWE over cyclotomic fields are not equivalent". In: *Applicable Algebra in Engineering, Communication and Computing* 35.3 (2024), pp. 351–358. DOI: 10.1007/s00200-022-00552-9.

[DD12] Léo Ducas and Alain Durmus. "Ring-LWE in Polynomial Rings". In: *Public Key Cryptography – PKC 2012*. Ed. by Marc Fischlin, Johannes Buchmann, and Mark Manulis. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 34–51. DOI: 10.1007/978-3-642-30057-8_3.

[EHL14] Kirsten Eisenträger, Sean Hallgren, and Kristin Lauter. "Weak Instances of PLWE". In: *Selected Areas in Cryptography – SAC 2014*. Ed. by Antoine Joux and Amr Youssef. Cham: Springer International Publishing, 2014, pp. 183–194. DOI: 10.1007/978-3-319-13051-4_11.

[Lan02] Serge Lang. *Algebra*. Revised 3rd ed. Springer New York, NY, 2002. 914 pp. ISBN: 978-0-387-95385-4. DOI: 10.1007/978-1-4613-0041-0.

[Lan13] Serge Lang. *Algebraic Number Theory*. 2nd ed. Springer New York, NY, 2013. 357 pp. ISBN: 978-1-4612-6922-9. DOI: 10.1007/978-1-4612-0853-2.

[Lia76] Joseph J. Liang. "On the integral basis of the maximal real subfield of a cyclotomic field." In: *Journal für die reine und angewandte Mathematik* 0286_0287 (1976), pp. 223–226.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. “On Ideal Lattices and Learning with Errors over Rings”. In: *Advances in Cryptology – EUROCRYPT 2010*. Ed. by Henri Gilbert. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 1–23. DOI: 10.1007/978-3-642-13190-5_1.

[LS19] Vadim Lyubashevsky and Gregor Seiler. *NTTRU: Truly Fast NTRU Using NTT*. Cryptology ePrint Archive, Paper 2019/040. 2019. URL: https://eprint.iacr.org/2019/040.

[Nar04] Władysław Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. 3rd ed. Springer Berlin, Heidelberg, 2004. 712 pp. ISBN: 978-3-642-06010-6. DOI: 10.1007/978-3-662-07001-7.

[Nat25] National Institute of Standards and Technology. *NIST Releases First 3 Finalized Post-Quantum Encryption Standards*. 2025. URL: https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards (visited on 08/18/2025).

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Trans. by Norbert Schappacher. 1st ed. Germany: Springer Berlin, Heidelberg, 1999. 571 pp. ISBN: 978-3-540-65399-8. DOI: 10.1201/9781003462002.

[Ped+21] Alberto Pedrouzo-Ulloa, Juan Ramón Troncoso-Pastoriza, Nicolas Gama, Mariya Georgieva, and Fernando Pérez-González. “Revisiting Multivariate Ring Learning with Errors and Its Applications on Lattice-Based Cryptography”. In: *Mathematics* 9.8 (2021). ISSN: 2227-7390. DOI: 10.3390/math9080858.

[Reg05] Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*. STOC ’05. Baltimore, MD, USA: Association for Computing Machinery, 2005, pp. 84–93. DOI: 10.1145/1060590.1060603.

[Reg09] Oded Regev. “On lattices, learning with errors, random linear codes, and cryptography”. In: *Journal of the ACM* 56.34 (6 2009), pp. 1–40. DOI: 10.1145/1568318.1568324.

[RSW18] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. “On the Ring-LWE and Polynomial-LWE Problems”. In: *Advances in Cryptology – EUROCRYPT 2018*. Ed. by Jesper Buus Nielsen and Vincent Rijmen. Cham: Springer International Publishing, 2018, pp. 146–173. DOI: 10.1007/978-3-319-78381-9_6.

[Ste+09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. “Efficient Public Key Encryption Based on Ideal Lattices”. In: *Advances in Cryptology – ASIACRYPT 2009*. Ed. by Mitsuru Matsui. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 617–635. DOI: 10.1007/978-3-642-10366-7_36.

[Ste15] Ian Stewart. *Galois Theory*. 4th ed. New York, USA: Chapman and Hall/CRC, 2015. 344 pp. ISBN: 9780429172250. DOI: 10.1201/b18187.

[ST25] Ian Stewart and David Tall. *Algebraic Number Theory and Fermat's Last Theorem*. 5th ed. Chapman and Hall/CRC, 2025. 504 pp. ISBN: 9781003462002. DOI: 10.1201/9781003462002.

[Was12] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. 2nd ed. Springer New York, NY, 2012. 490 pp. ISBN: 978-1-4612-7346-2. DOI: 10.1007/978-1-4612-1934-7.

A Condition number of embedding change for quadratic fields

We wish to prove the condition numbers for the embedding change matrices for quadratic fields given in Eq. (4), namely that we have

$$\kappa(V_{p_i}) = \begin{cases} \sqrt{p_i} + \frac{1}{\sqrt{p_i}}, & p_i \equiv 2,3 \pmod 4 \\ \frac{5}{2\sqrt{p_i}} + \frac{\sqrt{p_i}}{2}, & p_i \equiv 1 \pmod 4, \end{cases}$$

where

$$V_{p_i} = \begin{cases} \begin{bmatrix} 1 & \sqrt{p} \\ 1 & -\sqrt{p} \end{bmatrix}, & p_i \equiv 2,3 \pmod 4 \\ \begin{bmatrix} 1 & \frac{1+\sqrt{p}}{2} \\ 1 & \frac{1-\sqrt{p}}{2} \end{bmatrix}, & p_i \equiv 1 \pmod 4. \end{cases}$$

A.1 Case $p_i \equiv 2,3 \pmod 4$

For this equivalence class, we have

$$V_{p_i} = \begin{bmatrix} 1 & \sqrt{p} \\ 1 & -\sqrt{p} \end{bmatrix}, \quad V_{p_i}^{-1} = \frac{1}{2\sqrt{p}} \begin{bmatrix} \sqrt{p} & \sqrt{p} \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2\sqrt{p}} \\ \frac{1}{2} & -\frac{1}{2\sqrt{p}} \end{bmatrix}.$$

Additionally, $V_{p_i}^* = V_{p_i}^T$, as p is a positive prime.

$$V_{p_i} V_{p_i}^* = V_{p_i} V_{p_i}^T = \begin{bmatrix} 1 & \sqrt{p} \\ 1 & -\sqrt{p} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \sqrt{p} & -\sqrt{p} \end{bmatrix} = \begin{bmatrix} 1+p & 1-p \\ 1-p & 1+p \end{bmatrix}$$
$$\implies \|V_{p_i}\| = \sqrt{\mathrm{Tr}(V_{p_i} V_{p_i}^*)} = \sqrt{2(1+p)}.$$

$$V_{p_i}^{-1}(V_{p_i}^{-1})^* = V_{p_i}^{-1}(V_{p_i}^{-1})^T = \frac{1}{4p} \begin{bmatrix} \sqrt{p} & \sqrt{p} \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \sqrt{p} & 1 \\ \sqrt{p} & -1 \end{bmatrix} = \frac{1}{4p} \begin{bmatrix} 2p & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2p} \end{bmatrix}$$
$$\implies \|V_{p_i}^{-1}\| = \sqrt{\frac{p+1}{2p}}$$
$$\implies \kappa(V_{p_i}) = \|V_{p_i}\| \|V_{p_i}^{-1}\| = \sqrt{2(1+p)} \sqrt{\frac{p+1}{2p}} = \frac{p+1}{\sqrt{p}} = \sqrt{p} + \frac{1}{\sqrt{p}}.$$

A.2 Case $p_i \equiv 1 \pmod 4$

For this equivalence class, we have

$$V_{p_i} = \begin{bmatrix} 1 & \frac{1+\sqrt{p}}{2} \\ 1 & \frac{1-\sqrt{p}}{2} \end{bmatrix}, \quad V_{p_i}^{-1} = \frac{1}{\sqrt{p}} \begin{bmatrix} \frac{\sqrt{p}-1}{2} & \frac{1+\sqrt{p}}{2} \\ 1 & -1 \end{bmatrix}.$$

Additionally, $V_{p_i}^* = V_{p_i}^T$, as p is a positive prime.

$$\begin{aligned} V_{p_i}V_{p_i}^* = V_{p_i}V_{p_i}^T &= \begin{bmatrix} 1 & \frac{1+\sqrt{p}}{2} \\ 1 & \frac{1-\sqrt{p}}{2} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{p}}{2} & \frac{1-\sqrt{p}}{2} \end{bmatrix} = \begin{bmatrix} \frac{4+(1+\sqrt{p})^2}{4} & \frac{4+1+p}{4} \\ \frac{4+1+p}{4} & \frac{4+(1-\sqrt{p})^2}{4} \end{bmatrix} \\ &= \frac{1}{4}\begin{bmatrix} 5+2\sqrt{p}+p & 5+p \\ 5+p & 5-2\sqrt{p}+p \end{bmatrix} \\ &\implies \|V_{p_i}\| = \sqrt{\mathrm{Tr}(V_{p_i}V_{p_i}^*)} = \sqrt{\frac{5+p}{2}}. \end{aligned}$$

$$\begin{aligned} V_{p_i}^{-1}(V_{p_i}^{-1})^* &= \frac{1}{p}\begin{bmatrix} \frac{\sqrt{p}-1}{2} & \frac{1+\sqrt{p}}{2} \\ 1 & -1 \end{bmatrix} \begin{bmatrix} \frac{\sqrt{p}-1}{2} & 1 \\ \frac{1+\sqrt{p}}{2} & -1 \end{bmatrix} \\ &= \frac{1}{p}\begin{bmatrix} \frac{(1-\sqrt{p})^2+(1+\sqrt{p})^2}{4} & \frac{(\sqrt{p}-1)+(\sqrt{p}+1)}{2} \\ \frac{(\sqrt{p}-1)+(\sqrt{p}+1)}{2} & 2 \end{bmatrix} \\ &= \frac{1}{p}\begin{bmatrix} \frac{p+1}{2} & -1 \\ -1 & 2 \end{bmatrix} \\ &\implies \|V_{p_i}^{-1}\| = \sqrt{\mathrm{Tr}(V_{p_i}^{-1}(V_{p_i}^{-1})^*)} = \sqrt{\frac{p+5}{2p}} \\ &\implies \kappa(V_{p_i}) = \|V_{p_i}\|\|V_{p_i}^{-1}\| = \sqrt{\frac{5+p}{2}}\sqrt{\frac{p+5}{2p}} = \frac{5}{2\sqrt{p}} + \frac{\sqrt{p}}{2}. \end{aligned}$$

B Referenced results

Theorem B.1 (Theorem 1 [Lia76]). *The discriminant of $K_n = \mathbb{Q}(\psi_n)$ is*

$$\Delta_{K_n} = \begin{cases} 2^{(m-1)2^{m-2}-1}, & \text{if } n = 2^m,\ m > 2 \\ p^{\frac{mp^m-(m+1)p^{m-1}-1}{2}}, & \text{if } n = p^m \text{ or } n = 2p^m,\ p > 2 \text{ prime} \\ n^{\varphi(n)/2}\prod_{i=1}^{t} p_i^{-\varphi(n)/2(p_i-1)}, & \text{if } n = \prod_{i=1}^{t} p_i^{m_i},\ t > 1,\ n \neq 2p^m \end{cases}$$

In particular, only primes which ramify in $\mathbb{Q}(\zeta_n)$ can ramify in $K_n = \mathbb{Q}(\psi_n)$. We use this to show linear disjointness of the multiquadratic field and the maximal real subfield of a cyclotomic field in Lemma 4.6.

Theorem B.2 (Theorem 4.26 [Nar04]). *Let for $i = 1, 2$ $K_i/\mathbb{Q}$ $(i = 1, 2)$ be finite extensions of degrees n_i and discriminants $\Delta(K_i)$, and assume $\gcd(\Delta(K_1), \Delta(K_2)) = 1$. Then the degree of the composite $L = K_1K_2$ equals n_1n_2, one has*

$$\Delta(L) = \Delta(K_1)^{n_2}\Delta(K_2)^{n_1},$$

and if $\omega_1, \ldots, \omega_{n_1}$ is an integral basis of K_1 and $\Omega_1, \ldots, \Omega_{n_2}$ is an integral basis of K_2, then the set $\{\omega_i\Omega_j\}$ is an integral basis of L.

In other words, under these assumptions, the ring of integers of a composite field is a $\mathbb{Z}$-module tensor product $O_{K_1} \otimes_{\mathbb{Z}} O_{K_2}$ of the individual rings of integers. We utilize this theorem to describe the rings of integers of real cyclo-multiquadratic fields in Eq. (2).

Proposition B.3 (p. 268 [Lan02]). *Let $K_1, \ldots, K_n$ be Galois extensions of k with Galois groups $G_1, \ldots, G_n$. Assume that $K_{i+1} \cap (K_1 \ldots K_i) = k$ for each $i = 1, \ldots, n-1$. Then the Galois group of $K_1, \ldots, K_n$ is isomorphic to the product $G_1 \times \cdots \times G_n$ in the natural way.*

Proof. See [Lan02, p. 268, Corollary 1.15]. □

That is, for linearly disjoint Galois fields, the Galois group of their composite field is isomorphic to the direct product of their individual Galois groups. This fact is used to describe the Galois groups of real cyclo-multiquadratic fields in Proposition 4.7.

C Condition number bound approximations

We gather here the details of the approximations used in the condition number bounds for real cyclo-multiquadratic fields.

C.1 Theorem 4.12

Let $n = p^s$, $s \geq 1$, p odd prime. Then

$$\begin{aligned}
\kappa(V_K) &= \kappa(V_{K_n} \otimes V_{p_1} \otimes \cdots \otimes V_{p_r}) \\
&= \kappa(V_{K_n})\kappa(V_{p_1}) \ldots \kappa(V_{p_r}) \\
&< \frac{\sqrt{3}}{2}\sqrt{n^3 + n^2 - n - 1} \prod_{i=1}^{r} (1 + \sqrt{p_i}) \\
&= \frac{\sqrt{3}}{2}(n+1)\sqrt{n-1} \prod_{i=1}^{r} (1 + \sqrt{p_i}) \\
&< \frac{\sqrt{3}}{2}(2n)\sqrt{n} \prod_{i=1}^{r} (1 + \sqrt{p_i}) \\
&= \sqrt{3} n^{3/2} \prod_{i=1}^{r} (1 + \sqrt{p_i}).
\end{aligned}$$

The first inequality follows from combining the condition number bounds for quadratic fields from Corollary 4.9 and maximal real subfields of a cyclotomic field from Lemma 4.10 using the property of the Kronecker product with the condition number from Lemma 4.2.

C.2 Theorem 4.13

Let $n = 2^r p^s, r \geq 2, s \geq 1$, p odd prime. Then

$$\begin{aligned}
\kappa(V_K) &= \kappa(V_{K_n} \otimes V_{p_1} \otimes \cdots \otimes V_{p_r}) \\
&= \kappa(V_{K_n})\kappa(V_{p_1}) \ldots \kappa(V_{p_r}) \\
&< \sqrt{\frac{3}{32}n^3 - \frac{3}{8}n^2} \prod_{i=1}^{r}(1 + \sqrt{p_i}) \\
&= \frac{\sqrt{3}}{2\sqrt{2}} n \sqrt{\frac{1}{4}n - 1} \prod_{i=1}^{r}(1 + \sqrt{p_i}) \\
&= \frac{\sqrt{6}}{4} n \sqrt{\frac{1}{4}n - 1} \prod_{i=1}^{r}(1 + \sqrt{p_i}) \\
&< \frac{\sqrt{6}}{4} n \sqrt{\frac{1}{4}n} \prod_{i=1}^{r}(1 + \sqrt{p_i}) \\
&= \frac{\sqrt{6}}{8} n^{3/2} \prod_{i=1}^{r}(1 + \sqrt{p_i}).
\end{aligned}$$

The first inequality follows from combining the condition number bounds for quadratic fields from Corollary 4.9 and maximal real subfields of a cyclotomic field from Lemma 4.11 using the property of the Kronecker product with the condition number from Lemma 4.2.