6-1-2016

Cyclotomic Polynomials in Ring-LWE Homomorphic Encryption Schemes

Tamalika Mukherjee
txm1809@rit.edu

Rochester Institute of Technology
College of Science
School of Mathematical Sciences

Cyclotomic Polynomials in Ring-LWE Homomorphic Encryption Schemes

by
Tamalika Mukherjee

Thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science
in
Applied and Computational Mathematics

June 1, 2016

Committee Signatures

Dr. Anurag Agarwal
School of Mathematical Sciences

Dr. Stanisław Radziszowski
Department of Computer Science

Prof. David Barth-Hart
School of Mathematical Sciences

Dr. Elizabeth Cherry
School of Mathematical Sciences

Abstract

Homomorphic Encryption has been considered the 'Holy Grail of Cryptography' since the discovery of secure public key cryptography in the 1970s. In 2009, a long-standing question about whether fully homomorphic encryption is theoretically plausible was affirmatively answered by Craig Gentry and his bootstrapping construction. Gentry's breakthrough has initiated a surge of new research in this area, one of the most promising ideas being the Learning With Errors (LWE) problem posed by Oded Regev's. Although this problem has proved to be versatile as a basis for homomorphic encryption schemes, the large key sizes result in a quadratic overhead making this inefficient for practical purposes. In order to address this efficiency issue, Oded Regev, Chris Peikert and Vadim Lyubashevsky ported the LWE problem to a ring setting, thus calling it the Ring Learning with Errors (Ring-LWE) problem.

The underlying ring structure of the Ring-LWE problem is $\mathbb{Z}[x]/\Phi_m(x)$ where $\Phi_m(x)$ is the mth cyclotomic polynomial. The hardness of this problem is based on special properties of cyclotomic number fields. In this thesis, we explore the properties of lattices and algebraic number fields, in particular, cyclotomic number fields which make them a good choice to be used in the Ring-LWE problem setting.

The biggest crutch in homomorphic encryption schemes till date is performing homomorphic multiplication. As the noise term in the resulting ciphertext grows multiplicatively, it is very hard to recover the original ciphertext after a certain number of multiplications without compromising on efficiency. We investigate the efficiency of an implemented cryptosystem based on the Ring-LWE hardness and measure the performance of homomorphic multiplication by varying different parameters such as the cipherspace cyclotomic index and the underlying ring $\mathbb{Z}_p$.

Acknowledgements

There have been many influential people throughout my academic career at Rochester Institute of Technology who have guided me, placed opportunities in front of me and showed me the doors that might be useful to open. I would like to thank each and everyone of them.

I would especially like to thank my thesis advisers Dr. Anurag Agarwal and Dr. Stanisław Radziszowski for always keeping their office doors open and allowing this thesis to be my own work, but consistently steering me in the right direction whenever they thought I needed it.

I would also like to acknowledge Professor David Barth-Hart for graciously being a part of my thesis committee, and I am gratefully indebted to him for his very valuable comments on this thesis. The cryptography group at RIT has also been extremely supportive, especially Dr. Peizhao Hu. I am extremely grateful to Eric Crockett and Dr. Chris Peikert for helping me set up my experiments and explaining things in great detail whenever I needed some clarification regarding their work.

Finally, I must express my very profound gratitude to my parents and to my sister Tanuka Mukherjee for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

Dedication

To my parents Ashok Mukherjee and Nandita Mukherjee, for trusting me to pursue my college education far away from home and always believing in me.

Contents

Chapter 1

Overview

The Ring Learning With Errors problem is based on the Learning With Errors problem which was introduced by Oded Regev [28]. An informal overview is given here. Let $\Phi_m(x)$ be the mth cyclotomic polynomial, $R = \mathbb{Z}[x]/\langle\Phi_m(x)\rangle$ be the ring of integers modulo $\Phi_m(x)$ and q be a prime such that $q \equiv 1 \pmod{m}$ be a large prime. Fix an error distribution over R, say χ. For $i \in \mathbb{N}$, let $e_i \in \chi$, let $a_i, s_i \in R_q$ be uniformly random ring elements. Define $b_i = a_i s + e_i$. The goal is to distinguish a polynomial number of independent 'random noisy ring equations' from truly uniform pairs. In other words

$$\{a_i, b_i\}_{i=1}^{\text{poly(n)}} \approx \{a_i, u_i\}_{i=1}^{\text{poly(n)}}$$

where u_i's are uniformly sampled from R_q.

Homomorphic encryption is a form of encryption that allows us to perform computations on ciphertexts. In the past few years, many homomorphic encryption schemes have been proposed, that have been based on the Ring Learning With Errors problem. Unfortunately these encryption schemes are yet to be used in industry mostly because of the amount of time it takes to perform operations in such schemes. The biggest crutch is homomorphic

multiplication. Since a message is encrypted with a small amount of noise, every time a multiplication is performed, this noise grows multiplicatively. Thus after a certain number of multiplications, the original encrypted plaintext is lost because of the large error. Fortunately, there have been many methods introduced such as key-switching to deal with this problem. This work investigates the performance of homomorphic multiplication in the encryption scheme implemented by Chris Peikert and Eric Crockett in their Lattice Cryptography library called $\Lambda \circ \lambda$ [8].

The first four chapters develop the mathematical background required to understand the Ring Learning With Errors problem and the efficient algorithms implemented in [20]. Chapters 5 and 6 describe the Ring Learning With Errors problem as well as the experiments performed on the homomorphic encryption scheme, we conclude with a summary of our results and plans for future work.

Chapter 2

Lattice Theory and Hard Problems

2.1 Lattices

Lattices are regular arrangements of points in n-dimensional Euclidean space.

Definition 2.1.1. *Let $B = \{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_k}\}$ be a set of linearly independent vectors in $\mathbb{R}^n$. The lattice L generated by B is*

$$L(B) = \{a_1\mathbf{b_1} + a_2\mathbf{b_2} + \ldots + a_k\mathbf{b_k} |\ a_1, a_2, \ldots, a_k \in \mathbb{Z}\}$$

The set B is called the basis of the lattice $L(\mathcal{B})$. The integers n and k are called the dimension and rank of the lattice. When $n = k$, $L(B)$ is called a full-rank lattice [24].

Definition 2.1.2. *The span of the lattice L generated by a basis $B = \{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_k}\}$*

is defined as

$$span(L(B)) = span(B) = \left\{ \sum_{i=1}^{k} a_i \mathbf{b_i} | a_i \in \mathbb{R} \right\}$$

We will focus on full-rank lattices for the rest of this discussion, but one could easily extend these concepts to more general dimensions as well. Observe that the definition of a lattice looks very similar to that of a vector space, except that a vector space would be defined by a linear combination of vectors with real coefficients. An important consequence of this definition is that lattices are discrete sets, that is, for every $\mathbf{x} \in L$, there exists a neighborhood $N(\mathbf{x}, \epsilon) = \{\mathbf{y} \in \mathbb{R}^n : \ ||\mathbf{x} - \mathbf{y}|| \leq \epsilon\}$ such that $N(x, \epsilon) \cap L = \{x\}$. In particular, lattices are discrete additive subgroups of $\mathbb{R}^n$ [15].

A simple example of a lattice is the integers, $\mathbb{Z} \subset \mathbb{R}$ which forms a 1-dimensional lattice, similarly $\mathbb{Z}^n \subset \mathbb{R}^n$ forms an n-dimensional lattice. The set of even integers $2\mathbb{Z}$ is a subgroup of $\mathbb{R}$ and thus forms a lattice. Figure 2.1 below illustrates the integer lattice of even numbers in two dimensions.. Although the set of odd integers is discrete, it does not form a lattice, since it is not a subgroup of the real numbers.

The basis of a lattice is not unique and in fact any two bases of a lattice are related by a matrix having integer coefficients and determinant is plus or minus one (See Figure 2.2).

Definition 2.1.3. *The fundamental domain of a lattice corresponding to the basis* $B = \{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_k}\}$ *is the parallelopiped given by:*

$$F(B) = \{t_1 \mathbf{b_1} + t_2 \mathbf{b_2} + \ldots + t_n \mathbf{b_n} : 0 \leq t_i < 1\}$$

The fundamental domain defined by vectors $\mathbf{b}_1$ and $\mathbf{b}_2$ is shown by the shaded region in Figure 2.2. We need this quantity to define the determinant of the lattice, which is the volume of $F(B)$. In other words $\det L = vol(F(B))$.

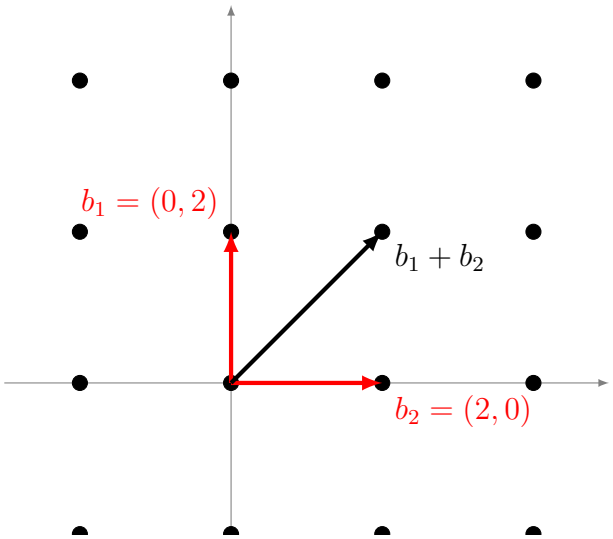

Figure 2.1: Lattice of even integers

Recall our previous remark about bases of the same lattice given by B and B' being related by a unimodular linear transformation U such that $B' = BU$. Observe that

$$\begin{aligned} vol(F(B')) &= |\det B'| \\ &= |\det BU| \\ &= |\det B||\det U| \\ &= |\det B| \\ &= vol(F(B)) \end{aligned}$$

Thus every basis of a lattice L has the same volume, which means that the determinant of the lattice is an invariant, independent of the fundamental domain used to calculate it [15].

One of the fundamental problems associated with lattice theory is finding the shortest vector in the lattice. An important quantity that we shall need to understand this is the minimum distance of a lattice.

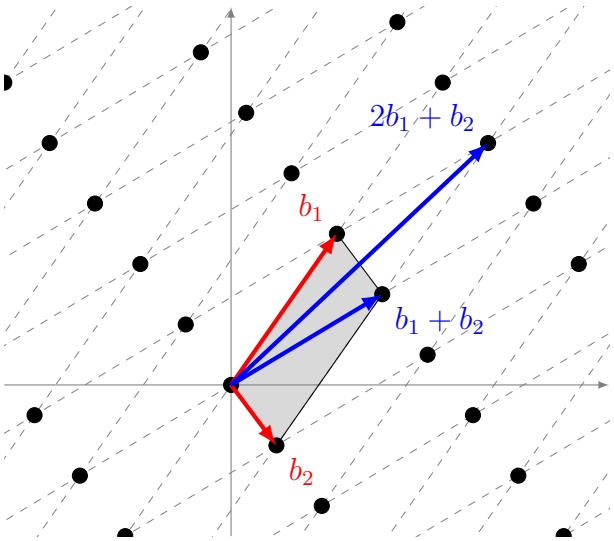

Figure 2.2: Different bases for the same lattice

Definition 2.1.4. *The smallest distance between any two distinct lattice points is given by* $\lambda_1(L) = \inf\{||\mathbf{x} - \mathbf{y}|| : \mathbf{x}, \mathbf{y} \in L, \mathbf{x} \neq \mathbf{y}\}$.

The following result is Minkowski's theorem is one of the most important theorems in lattice theory [24].

Theorem 2.1.5. *For any lattice* L *of rank* n *and any convex set* $S \subset span(L)$ *symmetric about the origin, if* $vol(S) > 2^n \det(L)$*, then* S *contains a non-zero lattice point* $\mathbf{v} \in S \cap L \setminus \{0\}$.

Minkowski's theorem (Theorem 2.1.5) relates the minimum distance of a lattice to its determinant. Take $S = N(\mathbf{0}, \sqrt{n}\det(L)^{1/n}) \cap span(L)$, which is the open ball centered at the origin with radius $\sqrt{n}\det(L)^{1/n}$. Since S contains an n-dimensional hypercube of length $2\det(L)^{1/n}$, we have that $vol(S) > 2^n \det(L)$. Thus by Minkowski's theorem, S contains a non-zero lattice point, in other words there exists a non-zero $\mathbf{v} \in L$ such that $||\mathbf{v}|| < \sqrt{n}\det(L)^{1/n}$. We can now state the following result:

Corollary 2.1.6. *For any lattice* L *of rank* n*, we have* $\lambda_1(L) < \sqrt{n}\det(L)^{1/n}$.

Corollary 2.1.6 gives us a weak upper bound on the shortest distance of a

vector in a lattice L [24]. Without loss of any generality, we will consider full rank integer lattices for the rest of this discussion.

2.2 Worst Case Lattice Problems

Worst case lattice problems are commonly used as a security assumption for cryptographic schemes since attacking lattice based systems would also entail solving the underlying lattice problem which has been proven to be NP-hard [23].

Shortest Vector Problem (SVP)

The shortest vector problem asks to find the shortest non-zero vector in a lattice L given by basis B. This problem has a rich history which can be traced back to Gauss and Hermite who studied an equivalent of the SVP problem in the context of quadratic forms. Gauss even gave an algorithm which solves this problem in two dimensions. Later Minkowski gave a tight upper bound for the length of the shortest vector, we have seen this bound in the previous section (Corollary 2.1.6).

Definition 2.2.1. ***Shortest Vector Problem (SVP)***
Given a lattice basis B, find a non-zero vector $\mathbf{v} \in L(B)$ such that $||\mathbf{v}|| = \lambda_1(L(B))$.

Figure 2.3 illustrates this problem in two dimensions. Here the basis $B = \{\mathbf{b}_1, \mathbf{b}_2\}$ and the shortest vector is $\mathbf{v}$. This problem is easy to solve in two dimensions using Gauss algorithm but it becomes increasingly more difficult in higher dimensions [24]. In cryptography, we are more interested in the approximation problem which can be defined with an approximation parameter $\gamma \geq 1$, which is usually a function of the rank of the lattice:

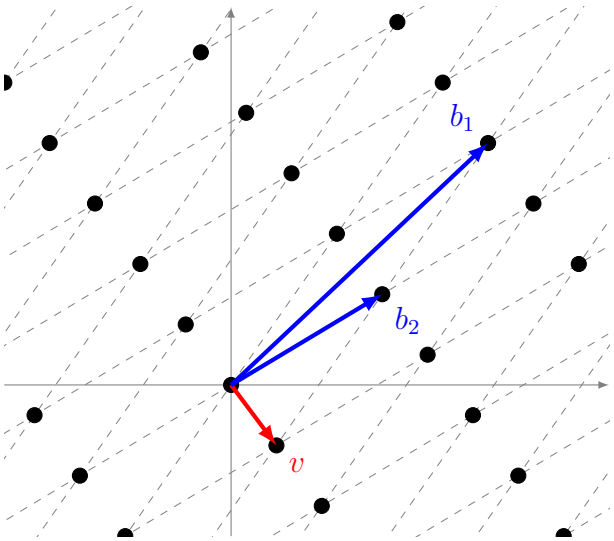

Figure 2.3: Shortest Vector Problem

Definition 2.2.2. ***Approximate Shortest Vector Problem*** *(SVP_γ)*
Given a lattice basis B, find a non-zero vector $\mathbf{v} \in L(B)$ such that $||\mathbf{v}|| \leq \gamma\lambda_1(L(B))$.

We want to base our security assumption of a cryptographic scheme on a problem that has been proven to be hard in the worst case. Till date, no such proof exists for this version of the problem. But there are proofs for the decision version of this problem [28].

Definition 2.2.3. ***Decisional Approximate Shortest Vector Problem*** *($GAPSVP_\gamma$)*
Given a lattice basis B and a positive integer d, distinguish between the cases $\lambda_1(L(B)) \leq d$ and $\lambda_1(L(B)) > \gamma \cdot d$.

The SVP problem was conjectured to be NP-hard by van Emde Boas in 1981 and later proved to be hard under randomized reductions by Ajtai in 1997 [1]. In 2001, Micciancio [23] gave the strongest NP-hardness result known till date, he showed that SVP is NP-hard to approximate within any factor less than $\sqrt{2}$.

Closest Vector Problem (CVP)

A related lattice problem whose decision version is known to be NP-complete is the Closest Vector Problem [24]. It is formally stated as follows:

Definition 2.2.4. ***Closest Vector Problem (CVP)***

Given a lattice basis B and a target vector $\mathbf{t}$*, find* $\mathbf{x} \in L(B)$ *such that for all* $\mathbf{y} \in L(B)$*,* $||\mathbf{x} - \mathbf{t}|| \leq ||\mathbf{y} - \mathbf{t}||$.

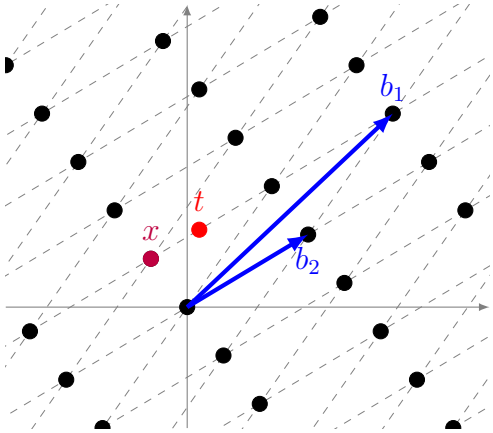

Figure 2.4: Closest Vector Problem

Figure 2.4 illustrates this problem in two dimensions where the basis $B = \{\mathbf{b}_1, \mathbf{b}_2\}$, the target vector $\mathbf{t}$ is marked in red and the closest vector $\mathbf{x}$ is marked in magenta.

The associated decisional approximation problem with the approximation parameter γ is stated below [28]:

Definition 2.2.5. ***Decisional Approximate Closest Vector Problem*** *($GAPCVP_\gamma$)*

Given a lattice basis B, a target vector $\mathbf{t}$ *and a parameter $d > 0$, a YES instance is when* $||\mathbf{x}-\mathbf{t}|| \leq d$*, whereas a NO instance is when* $||\mathbf{x}-\mathbf{t}|| > \gamma \cdot d$*.*

The NP-hardness of CVP was established by reducing it to the subset sum problem [24], thus solving CVP would imply that $P = NP$. It can be shown that SVP is no harder than CVP [14]. Note that the trivial reduction of

considering the target vector $\mathbf{t} = \mathbf{0}$ does not work since the CVP oracle would return the $\mathbf{0}$ vector as the closest vector to itself.

2.3 LLL Algorithm

The LLL-algorithm was developed by Hendrik Lenstra, Arjen Lenstra and László Lovász in 1982. This was the first attack against the SVP discussed in the previous section. Subsequent attacks are based on this one. The goal of the LLL-Algorithm is to obtain a nearly orthogonal lattice basis. It approximates the SVP in polynomial time within a factor of $(2/\sqrt{3})^n$. An upper bound for this problem is given by Hermite's Theorem which can be related to Corollary 2.1.6 and is stated as follows:

Theorem 2.3.1. *(Hermite's Theorem). Every lattice L of dimension n contains a non-zero vector $\mathbf{b} \in L$ satisfying:*

$$||\mathbf{b}|| \leq \sqrt{n}(\det L)^{\frac{1}{n}}$$

Intuitively it makes sense that the more orthogonal the vectors in the basis are the shorter the distances between the vectors will be. The Hadamard ratio of basis $B = \{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}\}$ is defined as

$$H(B) = \left(\frac{\det L}{||\mathbf{b_1}|| \ldots ||\mathbf{b_n}||}\right)^{\frac{1}{n}},$$

where $0 < H(B) \leq 1$. The closer $H(B)$ is to 1, the more orthogonal are the vectors in the basis [15]. We can obtain an orthogonalized set of vectors from a lattice basis $\tilde{B}$ using Gram-Schmidt Orthogonalization. The set $\tilde{B}$ need not be a basis for the lattice $L(B)$ because in Gram-Schmidt Orthogonalization, the vectors are obtained by adding and subtracting non-integer multiples of

the basis vectors, as such the group law may not be preserved. Recall Gram-Schmidt Orthogonalization as follows [3]:
For basis $B = \{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}\}$, define the Gram-Schmidt Orthogonalized basis as $\tilde{B} = \{\tilde{\mathbf{b}}_1, \tilde{\mathbf{b}}_2, \ldots, \tilde{\mathbf{b}}_n\}$:

$$\begin{aligned}
\tilde{\mathbf{b}}_1 &= \mathbf{b_1} \\
\tilde{\mathbf{b}}_2 &= \mathbf{b_2} - \mu_{1,2}\tilde{\mathbf{b}}_1 \\
&\ldots \\
\tilde{\mathbf{b}}_j &= \mathbf{b_j} - \sum_{i<j} \mu_{i,j}\tilde{\mathbf{b}}_i
\end{aligned}$$

where $\mu_{i,j} = \langle \mathbf{b}_j, \tilde{\mathbf{b}}_i \rangle / \langle \tilde{\mathbf{b}}_j, \tilde{\mathbf{b}}_j \rangle$.

Definition 2.3.2. *A basis $B = \{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}\}$ is said to be LLL-reduced if*

- *Size Condition: $|\mu_{i,j}| \leq \frac{1}{2}$, for all $1 \leq j < i \leq n$.*
- *Lovász Condition: $||\tilde{\mathbf{b_i}}||^2 \geq \left(\delta - \mu_{i,i-1}^2\right) ||\tilde{\mathbf{b}}_{i-1}||^2$ for all $1 < i \leq n$.*
- *We consider $\delta = \frac{3}{4}$, but the algorithm works in polynomial time for $\frac{1}{4} < \delta < 1$.*

The algorithm works as follows:
Input: basis $B = \{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}\}$ for lattice L.
Output: LLL-reduced basis B.

1. Set $k = 2$ and $\tilde{\mathbf{b_1}} = \mathbf{b_1}$.
2. While $k \leq n$, loop:
   (a) For $j = 1, 2, \ldots, k-1$:
   Set $\mathbf{b_k} = \mathbf{b_k} - \lfloor \mu_{k,j} \rceil \tilde{\mathbf{b_j}}$. [Size Reduction]
   (b) If $||\tilde{\mathbf{b_k}}||^2 \geq \left(\frac{3}{4} - \mu_{k,k-1}^2\right) ||\tilde{\mathbf{b_{k-1}}}||^2$: [Lovász Condition]
   Set $k = k + 1$

Else:
Swap $\mathbf{b_{k-1}}$ and $\mathbf{b_k}$
Set $k = \max(k-1, 2)$

3. End k loop
4. Return LLL-reduced basis B

The underlying idea behind the algorithm is to loop through the vectors in the lattice basis B and check for the two conditions that will make the basis LLL-reduced. Note that it is easy to form a basis that satisfies the *Size Condition*, since we can do this for every $\mathbf{b_k}$ by subtracting the appropriate linear combinations of $\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_{k-1}}$. But in the LLL-algorithm, this size reduction is done in stages, as the size reduction condition depends on the ordering of the vectors. The most important step is checking the *Lovász Condition*, which ensures that the length of the vectors do not decrease too quickly.

Theorem 2.3.3. *Given a basis $B = \{\mathbf{b_1}, \mathbf{b_2}, \ldots, \mathbf{b_n}\}$ for lattice L, and suppose*

$$M = \max\{\|\mathbf{b_i}\|^2 : i = 1, 2, \ldots, n\} \geq 2$$

then the LLL algorithm finds a reduced basis $L = L(B)$ using at most $O(n^5 \log(M))$ arithmetic operations.

The proof can be found in [16]. We will illustrate this algorithm using the following example: Take $\mathbf{b_1} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\mathbf{b_2} = \begin{pmatrix} 4 \\ 2 \\ 15 \end{pmatrix}$, $\mathbf{b_3} = \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}$ in $\mathbb{Z}^3$.
Note $\det L = |\det[\mathbf{b_1}\ \mathbf{b_2}\ \mathbf{b_3}]| = 6$.

1. Set $k = 2$.
2. Loop until $k \leq 3$
3. Loop $j = 1$ to $j - 1 = 2 - 1 = 1$:

(a)

$$\begin{aligned}\mathbf{b_2} &= \mathbf{b_2} - \lfloor \mu_{2,1} \rceil \tilde{\mathbf{b_1}} \\ &= \begin{pmatrix} 4 \\ 2 \\ 15 \end{pmatrix} - 4 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 2 \\ 15 \end{pmatrix}\end{aligned}$$

(b) Check $||\tilde{\mathbf{b}_2}||^2 \geq (\frac{3}{4} - \mu_{2,1}^2)||\tilde{\mathbf{b}_1}||^2 \rightarrow$ TRUE $\rightarrow$ set $k = 3$.

4. For $k = 3$.
   Loop $j = 1$ to $j - 1 = 3 - 1 = 2$:

   (a) j=1

$$\begin{aligned}\mathbf{b_3} &= \mathbf{b_3} - \lfloor \mu_{3,1} \rceil \tilde{\mathbf{b_1}} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} - 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}\end{aligned}$$

(a) j=2

$$\begin{aligned}\mathbf{b_3} &= \mathbf{b_3} - \lfloor \mu_{3,2} \rceil \tilde{\mathbf{b}_2} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} - \left\lfloor \frac{45}{229} \right\rceil \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}\end{aligned}$$

5. Check $||\tilde{\mathbf{b}_3}||^2 \geq (\frac{3}{4} - \mu_{3,2}^2)||\tilde{\mathbf{b}_2}||^2 \rightarrow$ FALSE $\rightarrow$ Swap $\tilde{\mathbf{b}_2}$ and $\tilde{\mathbf{b}_3}$, $k = 3 - 1 = 2$.

6. $k = 2$.

$$\mathbf{b_1} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{b_2} = \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}$$

7. Loop $j = 1$ to $j - 1 = 2 - 1 = 1$:

   (a)

$$\begin{aligned}\mathbf{b_2} &= \mathbf{b_2} - \lfloor \mu_{2,1} \rceil \tilde{\mathbf{b}_1} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} - 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}\end{aligned}$$

   (b) Check $||\tilde{\mathbf{b}_2}||^2 \geq (\frac{3}{4} - \mu_{2,1}^2)||\tilde{\mathbf{b}_1}||^2 \rightarrow$ TRUE $\rightarrow$ set $k = 2 + 1 = 3$.

8. $k = 3$

   Loop $j = 1$ to $j - 1 = 3 - 1 = 2$:

   (a) j=1

$$\begin{aligned}\mathbf{b_3} &= \mathbf{b_3} - \lfloor \mu_{3,1} \rceil \tilde{\mathbf{b_1}} \\ &= \begin{pmatrix} 0 \\ 2 \\ 15 \end{pmatrix} - 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 2 \\ 15 \end{pmatrix}\end{aligned}$$

   (a) j=2

$$\begin{aligned}\mathbf{b_3} &= \mathbf{b_3} - \lfloor \mu_{3,2} \rceil \tilde{\mathbf{b_2}} \\ &= \begin{pmatrix} 0 \\ 2 \\ 15 \end{pmatrix} - 5 \cdot \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}\end{aligned}$$

9. Check $||\tilde{\mathbf{b}_3}||^2 \geq (\frac{3}{4} - \mu_{3,2}^2)||\tilde{\mathbf{b}_2}||^2 \rightarrow$ FALSE $\rightarrow$ Swap $\tilde{\mathbf{b}_2}$ and $\tilde{\mathbf{b}_3}$, $k = 3 - 1 = 2$.

10. Set $k = 2$.

$$\mathbf{b_1} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{b_2} = \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}$$

11. Loop $j = 1$ to $j - 1 = 2 - 1 = 1$:

(a)

$$\begin{aligned}\mathbf{b_2} &= \mathbf{b_2} - \lfloor \mu_{2,1} \rceil \tilde{\mathbf{b_1}} \\ &= \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} - 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}\end{aligned}$$

(b) Check $||\tilde{\mathbf{b}_2}||^2 \geq (\frac{3}{4} - \mu_{2,1}^2)||\tilde{\mathbf{b}_1}||^2 \rightarrow$ TRUE $\rightarrow$ set $k = 2 + 1 = 3$.

12. For $k = 3$.
Loop $j = 1$ to $j - 1 = 3 - 1 = 2$:

(a) j=1

$$\begin{aligned}\mathbf{b_3} &= \mathbf{b_3} - \lfloor \mu_{3,1} \rceil \tilde{\mathbf{b_1}} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} - 0 \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}\end{aligned}$$

(a) j=2

$$\begin{aligned}\mathbf{b_3} &= \mathbf{b_3} - \lfloor \mu_{3,2} \rceil \tilde{\mathbf{b_2}} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix} - 0 \cdot \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}\end{aligned}$$

13. Check $||\tilde{\mathbf{b}_3}||^2 \geq (\frac{3}{4} - \mu_{3,2}^2)||\tilde{\mathbf{b}_2}||^2$ →TRUE → set $k = 3 + 1 = 4$. Stop loop.

We get our reduced basis as:

$$\mathbf{b_1} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \mathbf{b_2} = \begin{pmatrix} 0 \\ 2 \\ 0 \end{pmatrix}, \mathbf{b_3} = \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}$$

For a sanity check - $\det L = |\det[\mathbf{b_1}\ \mathbf{b_2}\ \mathbf{b_3}]| = 6$, we see that the determinant of the new basis is equal to that of the old basis. Now let us check whether the algorithm truly returns a more orthogonal basis than our original basis. To do this we use the Hadamard ratio as follows:

- $H(B_{original}) = \left(\frac{6}{\sqrt{255}}\right)^{\frac{1}{3}} = 0.7215$
- $H(B_{reduced}) = \left(\frac{6}{\sqrt{14}}\right)^{\frac{1}{3}} \approx 1$

Chapter 3

Algebraic Number Fields

3.1 Preliminaries

For the purposes of this thesis, we will assume that the reader is familiar with basic group, ring and field structures. Further reading about these topics can be found in [10].
One of the main goals of algebraic number theory is to extend the rational numbers to include complex solutions to certain polynomials in $\mathbb{Q}[x]$ which have no rational roots. More formally,

Definition 3.1.1. *A number $\alpha \in \mathbb{C}$ is algebraic if it satisfies a polynomial equation*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

where $a_i \in \mathbb{Q}$ for all $i \in \{0, 1, 2, \ldots n-1\}$.

From this definition we can intuitively think of the following concept,

Definition 3.1.2. *A number $\alpha \in \mathbb{C}$ is an algebraic integer if it satisfies a polynomial equation*

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$$

where $a_i \in \mathbb{Z}$ *for all* $i \in \{0, 1, 2, \ldots n-1\}$.

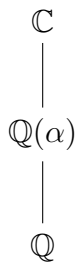

Figure 3.1: Hasse diagram depicting an algebraic extension of $\mathbb{Q}$

Let us consider an example of extending $\mathbb{Q}$. Consider $f(x) = x^2 - 2$, clearly $f(x) \in \mathbb{Q}[x]$. The equation $f(x) = 0$ has no roots in the rational numbers. So we want to extend $\mathbb{Q}$ to a field and look for a 'new' number α in this field such that it is a root of $f(x)$. Symbolically, we call $\alpha = \sqrt{2}$ and say that α is algebraic over $\mathbb{Q}$. We can define K as the smallest subfield of $\mathbb{C}$ containing both α and $\mathbb{Q}$. Then $K = \mathbb{Q}(\alpha)$ is a simple algebraic extension of $\mathbb{Q}$ depicted in Figure 3.1.

Definition 3.1.3. *If* K *is a subfield of* $\mathbb{C}$ *such that* $K = \mathbb{Q}(\omega)$ *for some root of unity* ω*, then* K *is called a cyclotomic field.*

For example the roots of $x^3 - 1 \in \mathbb{Q}[x]$ are $1, \omega, \omega^2$, where $\omega = \dfrac{-1 + \sqrt{-3}}{2}$. Thus $\mathbb{Q}(\sqrt{-3}) = \{a + b\sqrt{-3} | a, b \in \mathbb{Q}\}$ is a cyclotomic field, since $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\omega)$. We will be investigating cyclotomic fields in more detail in later chapters.

Let K be a subfield of $\mathbb{C}$ and $\alpha \in \mathbb{C}$ be algebraic over K. Some important definitions and properties of $K(\alpha)$ are described below [2] .

Definition 3.1.4. *The unique monic polynomial* $p(x) \in K[x]$ *such that*

$$I_K(\alpha) = \langle p(x) \rangle$$

where $I_K(\alpha) = \{f(x) \in K[x] | f(\alpha) = 0\}$*, is called the minimal polynomial of* α *over* K *and is denoted by* $irr_K(\alpha)$.

Definition 3.1.5. *The degree of α over K is defined by*

$$deg_K(\alpha) = deg(irr_K(\alpha))$$

Definition 3.1.6. *The degree of the extension $K(\alpha)$ over K is defined by*

$$[K(\alpha) : K] = n$$

where $n = deg(irr_K(\alpha))$.

Theorem 3.1.7. *The minimal polynomial $irr_K(\alpha)$ is irreducible in $K[x]$.*

Definition 3.1.8. *The conjugates of α over K are the roots in $\mathbb{C}$ of $irr_K(\alpha)$.*

Theorem 3.1.9. *The conjugates of α over K are distinct.*

It is easier to understand these properties with an example. Consider $\alpha = \frac{1+i}{\sqrt{2}} \in \mathbb{C}$. Then α is a root of $x^4 + 1 \in \mathbb{Q}[x]$. Since $x^4 + 1$ is irreducible in $\mathbb{Z}[x]$, by Gauss' lemma we can conclude that it is irreducible in $\mathbb{Q}[x]$ [10]. This means that

$$irr_{\mathbb{Q}}\left(\frac{1+i}{\sqrt{2}}\right) = x^4 + 1, deg\left(\frac{1+i}{\sqrt{2}}\right) = 4$$

We know that

$$x^4 + 1 = \left(x - \frac{1+i}{\sqrt{2}}\right)\left(x - \frac{1-i}{\sqrt{2}}\right)\left(x + \frac{1+i}{\sqrt{2}}\right)\left(x + \frac{1-i}{\sqrt{2}}\right)$$

Thus the conjugates of $\frac{1+i}{\sqrt{2}}$ over $\mathbb{Q}$ are

$$\frac{1+i}{\sqrt{2}}, \frac{1-i}{\sqrt{2}}, \frac{-1+i}{\sqrt{2}}, \frac{-1-i}{\sqrt{2}}$$

We want to study algebraic number fields, in particular the properties of cyclotomic fields to understand why they are used as the underlying ring structure of homomorphic encryption schemes. In order to define algebraic

number fields in a simple manner, we need the following theorem about multiple extensions.

Theorem 3.1.10. *Let K be a subfield of $\mathbb{C}$ and $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ be algebraic over K. Then there exists $\alpha \in \mathbb{C}$ that is algebraic over K such that*

$$K(\alpha_1, \ldots, \alpha_n) = K(\alpha)$$

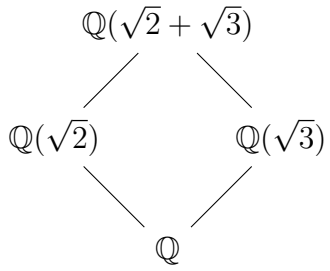

Figure 3.2: Algebraic extension of $\sqrt{2}, \sqrt{3}$ over $\mathbb{Q}$

As an example, consider $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, we want to express this as a simple extension. The conjugates of $\sqrt{2}$ over $\mathbb{Q}$ are $\sqrt{2}$ and $-\sqrt{2}$, similarly the conjugates of $\sqrt{3}$ over $\mathbb{Q}$ are $\sqrt{3}$ and $-\sqrt{3}$. The four combinations of these conjugates are distinct:

$$\sqrt{2}+\sqrt{3}, -\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}-\sqrt{3}$$

Thus we have $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ (see in Figure 3.2).
Set $\alpha = \sqrt{2}+\sqrt{3}$. We want to show that α is an algebraic number. So we

need to find a polynomial in $\mathbb{Q}[x]$ for which α is a root.

$$\begin{aligned}
\alpha^2 &= (\sqrt{2}+\sqrt{3})^2 \\
\alpha^2 &= 5+2\sqrt{6} \\
\alpha^2-5 &= 2\sqrt{6} \\
(\alpha^2-5)^2 &= (2\sqrt{6})^2 \\
\alpha^4-10\alpha^2+25 &= 24 \\
\alpha^4-10\alpha^2+1 &= 0
\end{aligned}$$

Thus α is a root of the monic quartic polynomial $f(x) = x^4-10x^2+1 \in \mathbb{Z}[x]$, which means that α is an algebraic number. In order for $f(x)$ to be a minimal polynomial over $\mathbb{Q}$, we need to prove that it is irreducible in $\mathbb{Z}[x]$ and therefore in $\mathbb{Q}[x]$.
Suppose that $f(x)$ is reducible in $\mathbb{Z}[x]$, this means that $f(x)$ is the product of two polynomials

- *Case 1:* $f(x) = (x^3+ax^2+bx+c)(x+d)$ or

  $$x^4-10x^2+1 = (x^3+ax^2+bx+c)(x+d)$$

  where $a,b,c,d \in \mathbb{Z}$. Notice that the only constant term on the right must be equal to the constant term on the left, in other words $cd = 1$. But since both $c,d \in \mathbb{Z}$, we have $c = 1, d = 1$ or $c = -1, d = -1$. This means that the only possible linear factors for $f(x)$ are $x-1$ or $x+1$. Now $f(-1) = f(1) = -8 \neq 0$, therefore $f(x)$ does not have any linear factors.

- *Case 2:* $f(x) = (x^2+ax+b)(x^2+cx+d)$. Then we have

  $$\begin{aligned}
  x^4-10x^2+1 &= (x^2+ax+b)(x^2+cx+d) \\
  &= x^4+(a+c)x^3+(b+ac+d)x^2+(bc+ad)x+bd
  \end{aligned}$$

where $a, b, c, d \in \mathbb{Z}$. Equating coefficients of like terms, we get

$$\begin{aligned} a + c &= 0 \\ b + ac + d &= -10 \\ bc + ad &= 0 \\ bd &= 1 \end{aligned}$$

Solving these equations, we get $b = d = \pm 1$, so that $b + d = \pm 2$, which implies that $a^2 = 8$ or 12, which is impossible. Thus $f(x)$ is irreducible.

We have

$$irr_{\mathbb{Q}}(\sqrt{2} + \sqrt{3}) = x^4 - 10x^2 + 1$$

and

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$$

Now we definine an algebraic number field as follows:

Definition 3.1.11. *An algebraic number field is a subfield of* $\mathbb{C}$ *in the form* $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ *where* $\alpha_1, \ldots, \alpha_n$ *are algebraic numbers.*

The following theorem simplifies our representation of an algebraic number field and is intuitive by combining the fact that any algebraic number is of the form a/b where b is a non-zero ordinary integer and a is an algebraic integer, with Theorem 3.1.10.

Theorem 3.1.12. *If* K *is an algebraic number field then there exists an algebraic integer* θ *such that* $K = \mathbb{Q}(\theta)$.

One of the main factors in studying these algebraic number fields is to explore whether the properties of integers in the rational numbers could be mimicked in these extensions. The most important property being unique factorization, recall that $\mathbb{Z}$ is a unique factorization domain (UFD). Keeping this in mind we define an analogy of the integers in general number fields as [22].

Definition 3.1.13. *The set of all algebraic integers that lie in the algebraic*

number field K is denoted by $\mathcal{O}_K$ and is called the ring of integers of K.

It is not surprising that the following statement is true

Theorem 3.1.14. *Let K be an algebraic number field, then $\mathcal{O}_K$ is an integral domain.*

Determining the ring of integers $\mathcal{O}_K$ for an algebraic number field K is generally a difficult problem. But it has been classified for the case of K being a quadratic field [2].

Theorem 3.1.15. *Let K be a quadratic field and m be a unique squarefree integer such that $K = \mathbb{Q}(\sqrt{m})$. Then the set $\mathcal{O}_K$ of algebraic integers in K is given by*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{m}, & m \not\equiv 1 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{m}}{2}\right), & m \equiv 1 \pmod 4 \end{cases}$$

Illustrating this theorem with an example, let us find $\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{-5})$ and $K = \mathbb{Q}(\sqrt{-7})$. Using Theorem 3.1.15, we see that $O_{\mathbb{Q}(\sqrt{-5})} = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ and $O_{\mathbb{Q}(\sqrt{-7})} = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-7}}{2}\right)$.

Recall that given an algebraic number field K of degree n and $\alpha \in K$ such that $K = \mathbb{Q}(\alpha)$, we defined the conjugates of α to be the roots of $irr_K(\alpha)$. What about the rest of the elements of K, do they also have conjugates relative to K? For $\beta \in K$, let us express β as

$$\beta = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}$$

where $c_0, \ldots, c_{n-1} \in \mathbb{Q}$. Intuitively we could define the conjugates of β relative to K as

$$\beta_k = c_0 + c_1\alpha_k + \ldots + c_{n-1}{\alpha_k}^{n-1}$$

where $k = 1, 2, \ldots, n$.

Definition 3.1.16. *The set of algebraic numbers $\{\beta_1 = \beta, \beta_2, \ldots, \beta_n\}$ is*

called a complete set of conjugates of β relative to K. Briefly, they are called the "K-conjugates of β" or the "conjugates of β relative to K".

Note [2] that the conjugates of β relative to K do not depend on the choice of α such that $K = \mathbb{Q}(\alpha)$. An important quantity related to the conjugates of β relative to K is the field polynomial of β over K.

Definition 3.1.17. *Let $\beta \in K$ where K is an algebraic number field of degree n. Suppose $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ are the K-conjugates of β. Then the field polynomial of β over K is defined as*

$$fld_K(\beta) = \prod_{k=1}^{n}(x - \beta_k)$$

Consider $K = \mathbb{Q}(\alpha)$, where $\alpha = \sqrt{2}$, we know $\alpha_1 = \sqrt{2}$ and $\alpha_2 = -\sqrt{2}$. Let $\beta \in K$ such that $\beta = \frac{1=\alpha}{2}$. Then

$$\begin{aligned} fld_K(\beta) &= \left(x - \frac{1+\alpha_1}{2}\right)\left(x - \frac{1+\alpha_2}{2}\right) \\ &= \left(x - \frac{1+\alpha}{2}\right)\left(x - \frac{1-\alpha}{2}\right) \\ &= \frac{1}{4}((2x-1)-\alpha)((2x-1)-\alpha) \\ &= \frac{1}{4}((2x-1)^2 - \alpha^2) \\ &= \frac{1}{4}(4x^2 - 4x + 1 - 2) \\ &= \frac{1}{4}(4x^2 - 4x - 1) \end{aligned}$$

Notice that $fld_K(\beta) \in \mathbb{Q}[x]$. This observation [2] can actually be made for all algebraic numbers in K:

Theorem 3.1.18. *Let K be an algebraic number field of degree n and $\beta \in K$, then $fld_K(\beta) \in \mathbb{Q}[x]$.*

3.2 Integral Basis of an Algebraic Number Field

In order to define the notion of a basis over an algebraic number field we need to define an important quantity called the discriminant.

Definition 3.2.1. *Let K be an algebraic number field of degree n and $\omega_1, \ldots, \omega_n \in K$. Suppose $\sigma_k : K \to \mathbb{C}$ where $k = 1, 2, \ldots, n$ denote the n distinct monomorphisms. For $i = 1, 2, \ldots, n$, let*

$$\omega_i^{(1)} = \sigma_1(\omega_i) = \omega_i, \omega_i^{(2)} = \sigma_2(\omega_i), \ldots, \omega_i^{(n)} = \sigma_n(\omega_i)$$

denote the conjugates of ω_i relative to K. Then the discriminant of $\{\omega_1, \ldots, \omega_n\}$ is

$$D(\omega_1, \ldots, \omega_n) = \begin{vmatrix} \omega_1^{(1)} & \omega_2^{(1)} & \ldots & \omega_n^{(1)} \\ \omega_1^{(2)} & \omega_2^{(2)} & \ldots & \omega_n^{(2)} \\ \vdots & \vdots & \ldots & \vdots \\ \omega_1^{(n)} & \omega_2^{(n)} & \ldots & \omega_n^{(n)} \end{vmatrix}$$

Definition 3.2.2. *Let K be an algebraic number field of degree n and $\beta \in K$. The discriminant of β denoted by $D(\beta)$ is defined as*

$$D(\beta) = \prod_{1 \leq i < j \leq n} (\beta^{(i)} - \beta^{(j)})^2$$

where $\beta^{(1)} = \beta, \beta^{(2)}, \ldots, \beta^{(n)}$ are the conjugates of β with respect to K.

As an example, take $K = \mathbb{Q}(\sqrt{2})$ and choose $\beta = \sqrt{2}$ then the conjugates of β are $\beta_1 = \sqrt{2}$ and $\beta_2 = -\sqrt{2}$. We have

$$\begin{aligned} D(\beta) &= (\beta_1 - \beta_2)^2 \\ &= (2\sqrt{2})^2 \\ &= 8 \end{aligned}$$

Now we can define a necessary and sufficient condition for an algebraic number field to be an extension of $\mathbb{Q}$:

Theorem 3.2.3. *Let K be an algebraic number field of degree n and $\beta \in K$. Then $K = \mathbb{Q}(\beta)$ if and only if $D(\beta) \neq 0$.*

It turns out that every ideal in the ring of integers $\mathcal{O}_K$ is finitely generated, in other words $\mathcal{O}_K$ is a Noetherian domain [2]. This fact helps us define the concept of a basis for an ideal

Definition 3.2.4. *Let K be an algebraic number field of degree n. Let $\mathfrak{I}$ be a nonzero ideal of $\mathcal{O}_K$. If $\{\eta_1, \eta_2, \ldots, \eta_n\}$ is a set of elements of $\mathfrak{I}$ such that every element $\alpha \in \mathfrak{I}$ can be expressed uniquely in the form*

$$\alpha = x_1\eta_1 + \ldots + x_n\eta_n$$

where $x_1, x_2, \ldots, x_n \in \mathbb{Z}$, then $\{\eta_1, \eta_2, \ldots, \eta_n\}$ is called a basis for the ideal $\mathfrak{I}$.

Consider $K = \mathbb{Q}(\sqrt{7})$, we already know that $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{7}$ (from Theorem 3.1.15). Let $\mathfrak{I}$ be the principal ideal of $\mathcal{O}_K$ generated by $2 + \sqrt{7}$, then

$$\begin{aligned}
\mathfrak{I} &= \{(a + b\sqrt{7})(2 + \sqrt{7}) | a, b \in \mathbb{Z}\} \\
&= \{(2a + 7b) + (a + 2b)\sqrt{7} | a, b \in \mathbb{Z}\} \\
&= \{(2(c - 2b) + 7b) + c\sqrt{7} | c, b \in \mathbb{Z}\} \\
&= \{3b + c(2 + \sqrt{7}) | c, b \in \mathbb{Z}\} \\
&= 3\mathbb{Z} + (2 + \sqrt{7})\mathbb{Z}
\end{aligned}$$

Thus $\{3, 2 + \sqrt{7}\}$ is a basis for $\mathfrak{I}$, note that $\{2 + \sqrt{7}, 7 + 2\sqrt{7}\}$ is another basis for $\mathfrak{I}$ and that $D(\{3, 2 + \sqrt{7}\}) = D(\{2 + \sqrt{7}, 7 + 2\sqrt{7}\}) = 252$. This observation brings us to the definition of the discriminant of an ideal [2]

Definition 3.2.5. *Let K be a algebraic number field of degree n, $\mathfrak{I}$ be a non-*

zero ideal of $\mathcal{O}_K$, and $\{\eta_1, \ldots, \eta_n\}$ be a basis for $\mathfrak{I}$. Then discriminant of the ideal $\mathfrak{I}$ is given by

$$D(I) = D(\{\eta_1, \ldots, \eta_n\})$$

Intuitively, a basis of the principal ideal of $\mathcal{O}_K$ generated by 1, that is $\mathcal{O}_K$ itself can be called an integral basis for K.

Definition 3.2.6. *A basis for $\mathcal{O}_K$ is called an integral basis for K.*

In light of this new notion, and Theorem 3.1.15, we can state the following:

Theorem 3.2.7. *Let K be a quadratic field and m be a unique squarefree integer such that $K = \mathbb{Q}(\sqrt{m})$. Then the integral basis for K is $\{1, \sqrt{m}\}$ when $m \not\equiv 1 \pmod 4$ and is $\left\{1, \left(\frac{1+\sqrt{m}}{2}\right)\right\}$ when $m \equiv 1 \pmod 4$.*

Similar to defining the discriminant of an ideal, we can define the discriminant of an algebraic number field as follows

Definition 3.2.8. *Let K be an algebraic number field of degree n and $\{\eta_1, \ldots, \eta_n\}$ be an integral basis for K. Then $D(\eta_1, \ldots, \eta_n)$ is called the discriminant of K and is denoted by $d(K)$.*

Ideally, it would be nice to have an integral basis for an algebraic number field K of degree n which looks something like $\{1, \eta, \eta^2, \ldots, \eta^{n-1}\}$ where every element $\alpha \in K$ is a linear combination of $1, \eta, \ldots, \eta^{n-1}$, the field in which this type of integral basis exists is called a monogenic number field [2].

Definition 3.2.9. *For an algebraic number field K of degree n, if there exists an element $\eta \in \mathcal{O}_K$ such that $\{1, \eta, \eta^2, \ldots, \eta^{n-1}\}$ is an integral basis for K, then K is said to be monogenic and $\{1, \eta, \eta^2, \ldots, \eta^{n-1}\}$ is called a power basis for K.*

It is clear to see that any quadratic number field is monogenic (from Theorem 3.2.7). But not every algebraic number field is monogenic. Dedekind showed this by proving that the cubic field $K = \mathbb{Q}(\theta)$ where θ is a root of $x^3 - x^2 - 2x - 8 \in \mathbb{Z}[x]$ does not have a power basis [9].

Let us describe the integral basis of a cyclotomic field. Recall that for a

positive integer n and a primitive nth root of unity ζ_n, the nth cyclotomic number field is defined as $K_n = \mathbb{Q}(\zeta_n)$. We can see that ζ_n is a root of

$$\Phi_n(x) = \prod_{\substack{r=1,\\(r,n)=1}}^{n} (x - \zeta_n^r)$$

since $\Phi_n(x) \in \mathbb{Z}[x]$ and is irreducible [10], we have that

$$irr_{\mathbb{Q}}(\zeta_n) = \Phi_n(x)$$

Observe that $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$. The following theorem is important to remember for future sections [2]:

Theorem 3.2.10. *The cyclotomic field $K_n = \mathbb{Q}(\zeta_n)$ is monogenic for every positive integer n.*

Consider $K_3 = \mathbb{Q}(\omega)$, then

$$\begin{aligned}
\Phi_3(x) &= \prod_{\substack{r=1,\\(r,3)=1}}^{3} (x - \omega^r) \\
&= (x - \omega)(x - \omega^2) \\
&= \left(x - \left(\frac{-1 + \sqrt{-3}}{2}\right)\right)\left(x - \left(\frac{-1 - \sqrt{-3}}{2}\right)\right) \\
&= 1 + x + x^2 \in \mathbb{Z}[x]
\end{aligned}$$

Observe that $\omega = \frac{-1}{2} \cdot 1 + \frac{1}{2} \cdot \sqrt{-3}$. It is clear that $K_3 = \mathbb{Q}(\sqrt{-3})$and from Theorem 3.2.7, the integral basis of $K_3 = \{1, \sqrt{-3}\}$.

Two other important quantities associated with an algebraic number field K are defined as follows:

Definition 3.2.11. *Let K be an algebraic number field of degree n. Let $\alpha \in K$. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be the K- conjugates of α. Then the trace of α is*

defined as

$$tr(\alpha) = \alpha_1 + \alpha_2 + \ldots + \alpha_n$$

and the norm of α *is defined by*

$$N(\alpha) = \alpha_1 \alpha_2 \ldots \alpha_n$$

One very simple example that we have seen since our middle school days is when $K = \mathbb{Q}(\sqrt{m})$ is a quadratic field. Take $\alpha \in K$ such that $\alpha = a + b\sqrt{m}$, the K-conjugates of α are $\alpha = a + b\sqrt{m}$ and $\alpha' = a - b\sqrt{m}$. The trace of α is

$$tr(\alpha) = \alpha + \alpha' = 2a$$

and the norm of α is

$$N(\alpha) = \alpha\alpha' = a^2 - b^2 m$$

3.3 Dedekind Domain and Unique Factorization

The motivation behind learning about Dedekind domains lies in the quest for finding unique factorization in algebraic structures. Under certain constraints, Dedekind domains can achieve unique factorization, as we shall see in this section.

Definition 3.3.1. *An integral domain D that is a Noetherian domain, integrally closed and in which every prime ideal of D is a maximal ideal is called a Dedekind domain.*

From the definition we can see that the following statement holds [2]:

Theorem 3.3.2. *The ring of integers $\mathcal{O}_K$ in an algebraic number field K is a Dedekind domain.*

Interestingly enough, the development of Dedekind domains came from the following result.

Proposition 3.3.3. *For an algebraic number field K, every non-zero ideal $\mathfrak{I}$ in $\mathcal{O}_K$ can be written uniquely as the product of powers of distinct prime ideals*

$$\mathfrak{I} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_n^{e_n}$$

where $\mathfrak{P}_1, \dots, \mathfrak{P}_n$ are distinct prime ideals and $e_i \geq 1$ for $i = 1, \dots, n$.

This property of the ring of integers led Dedekind to define Dedekind domains as any integral domain D in which every non-zero proper ideal $\mathfrak{I}$ can be written as a finite product of prime ideals [10]. Unique factorization of ideals in Dedekind domains means that we can define a notion of divisibility [2].

Definition 3.3.4. *If $\mathfrak{A}$ and $\mathfrak{B}$ are non-zero integral ideals of a Dedekind domain D, we say that $\mathfrak{A}|\mathfrak{B}$ if there exists an integral ideal $\mathfrak{C}$ of $\mathfrak{D}$ such that $\mathfrak{B} = \mathfrak{A}\mathfrak{C}$.*

Consider $K = \mathbb{Q}(\sqrt{-5})$, the ring of integers $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ is a Dedekind domain. Observe that $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, where $2, 3, (1 + \sqrt{-5}), (1 - \sqrt{-5})$ are irreducible in D. We illustrate how the use of prime ideals can represent the ideal $\langle 6 \rangle$ with a unique factorization. Take

$$\mathfrak{P}_1 = \langle 2, 1 + \sqrt{-5} \rangle$$
$$\mathfrak{P}_2 = \langle 3, 1 + \sqrt{-5} \rangle$$
$$\mathfrak{P}_3 = \langle 3, 1 - \sqrt{-5} \rangle$$

as three distinct prime ideals. Observe that $\mathfrak{P}_1^2 = \langle 2 \rangle$, $\mathfrak{P}_2\mathfrak{P}_3 = \langle 3 \rangle$, $\mathfrak{P}_1\mathfrak{P}_2 = \langle 1 + \sqrt{-5} \rangle$, $\mathfrak{P}_1\mathfrak{P}_3 = \langle 1 - \sqrt{-5} \rangle$. Then

$$\langle 6 \rangle = \langle 2 \rangle\langle 3 \rangle = \langle 1 + \sqrt{-5} \rangle\langle 1 - \sqrt{-5} \rangle = \mathfrak{P}_1^2\mathfrak{P}_2\mathfrak{P}_3$$

We can extend this concept of divisibility to fractional ideals, but first let us formally define them [2]

Definition 3.3.5. *Let D be an integral domain and K be the quotient field of D, then a non-empty subset $\mathfrak{A}$ of K with the following properties*

1. $\alpha \in \mathfrak{A}, \beta \in \mathfrak{A} \to \alpha + \beta \in \mathfrak{A}$.
2. $\alpha \in \mathfrak{A}, r \in D \to r\alpha \in \mathfrak{A}$.
3. *there exists $\gamma \in D$ with $\gamma \neq 0$ such that $\gamma\mathfrak{A} \subseteq D$.*

is called a fractional ideal of D.

Consider $\mathfrak{A} = \{\frac{n}{25} | n \in \mathbb{Z}\}$. For any $n_1, n_2 \in \mathbb{Z}$ we have $\frac{n_1}{25}, \frac{n_2}{25} \in \mathfrak{A}$ and $\frac{n_1+n_2}{25} \in \mathfrak{A}$. For any $r \in \mathbb{Z}$, $\frac{rn}{25} \in \mathfrak{A}$, since $rn \in \mathbb{Z}$. Also $25A = \mathbb{Z}$. Thus $\mathfrak{A}$ is a fractional ideal of $\mathbb{Z}$. Note that the quotient field of the ring of integers $\mathcal{O}_K$ is the algebraic number field K [10].

Observe that if $\mathfrak{A}$ is a fractional ideal of D and $\gamma \in D \setminus \{0\}$ is a common denominator for $\mathfrak{A}$ then $\gamma\mathfrak{A}$ is an integral ideal of D. We can define this notion formally for a prime ideal $\mathfrak{P}$ as follows

Definition 3.3.6. *Let D be an integral domain and K be the quotient field of D. For each prime ideal $\mathfrak{P}$ of D, we define the set*

$$\tilde{\mathfrak{P}} = \{\alpha \in K : \alpha\mathfrak{P} \subset D\}$$

It is clear to see that $\tilde{\mathfrak{P}}$ is a fractional ideal of D.We get the following property of a Dedekind domain from this observation:

Theorem 3.3.7. *Let D be a Dedekind domain and $\mathfrak{P}$ be a prime ideal of D. Then $\mathfrak{P}\tilde{\mathfrak{P}} = D$.*

Let us illustrate this theorem with the following example. Suppose $D = \mathbb{Z} + \mathbb{Z}\sqrt{6}$. D is the ring of integers of $K = \mathbb{Q}(\sqrt{6})$ and the quotient field of

D is K. Take the prime ideal $\mathfrak{P} = \langle 2, \sqrt{6} \rangle$, then

$$\begin{aligned}
\tilde{\mathfrak{P}} &= \{\alpha \in K | \alpha\mathfrak{P} \subseteq D\} \\
&= \{x + y\sqrt{6} | x, y \in \mathbb{Q}, (x + y\sqrt{6})\langle 2, 6 \rangle \subseteq \mathbb{Z} + \mathbb{Z}\sqrt{6}\} \\
&= \{x + y\sqrt{6} | x, y \in \mathbb{Q}, 2(x + y\sqrt{6}) \in \mathbb{Z} + \mathbb{Z}\sqrt{6}, \sqrt{6}(x + y\sqrt{6}) \in \mathbb{Z} + \mathbb{Z}\sqrt{6}\} \\
&= \{x + y\sqrt{6} | 2x \in \mathbb{Z}, 2y \in \mathbb{Z}, x \in \mathbb{Z}, 6y \in \mathbb{Z}\} \\
&= \{x + y\sqrt{6} | x \in \mathbb{Z}, 2y \in \mathbb{Z}\} \\
&= \left\{ a + \frac{b}{2}\sqrt{6} | a, b \in \mathbb{Z} \right\} \\
&= \left\{ \frac{2a + b\sqrt{6}}{2} | a, b \in \mathbb{Z} \right\} \\
&= \frac{1}{2}\{2a + b\sqrt{6} | a, b \in \mathbb{Z}\} \\
&= \frac{1}{2}(2\mathbb{Z} + \mathbb{Z}\sqrt{6}) \\
&= \frac{1}{2}\mathfrak{P}
\end{aligned}$$

Returning to the notion of defining divisibility for fractional ideals in a Dedekind domain, suppose $\mathfrak{A}$ is a fractional ideal in a Dedekind domain D and $\alpha, \beta \in D \setminus \{0\}$ are common denominators, then

$$\langle \alpha \rangle \mathfrak{A} = \mathfrak{B}, \ \langle \beta \rangle \mathfrak{A} = \mathfrak{C}$$

where $\mathfrak{B}$ and $\mathfrak{C}$ are integral ideals of $\mathfrak{D}$. We know that $\langle \alpha \rangle = \prod_{i=1}^{n} \mathfrak{P}_i^{r_i}$, $\langle \beta \rangle = \prod_{i=1}^{n} \mathfrak{P}_i^{t_i}$, $\langle \mathfrak{B} \rangle = \prod_{i=1}^{n} \mathfrak{P}_i^{s_i}$, $\langle \mathfrak{C} \rangle = \prod_{i=1}^{n} \mathfrak{P}_i^{u_i}$, where $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ are distinct prime ideals and r_i, s_i, u_i, t_i are nonnegative integers $(i = 1, 2, \ldots, n)$. Since

$$\langle \alpha \rangle \mathfrak{C} = \langle \alpha \rangle (\langle \beta \rangle \mathfrak{A}) = \langle \beta \rangle (\langle \alpha \rangle \mathfrak{A}) = \langle \beta \rangle \mathfrak{B}$$

we have

$$\prod_{i=1}^{n} \mathfrak{P}_i^{r_i + u_i} = \prod_{i=1}^{n} \mathfrak{P}_i^{s_i + t_i}$$

then

$$r_i + u_i = s_i + t_i$$

where $i = 1, 2, \ldots, n$. Now we can define the prime ideal factorization of the fractional ideal $\mathfrak{A}$ as $\prod_{i=1}^{n} \mathfrak{P}_i^{s_i - r_i}$, and this representation is unique [2]. This representation of fractional ideals lets us define the concept of an "inverse of an ideal". For any prime ideal $\mathfrak{P}$ of D, since $\mathfrak{P}\tilde{\mathfrak{P}} = \langle 1 \rangle$, we have $\tilde{\mathfrak{P}} = \mathfrak{P}^{-1}$. This means that we can define the inverse of any nonzero ideal I of a Dedekind domain. It turns out that the nonzero ideals of a Dedekind domain D form a multiplicative abelian group [2]. The following statement is a result of this fact:

Theorem 3.3.8. *Let K be an algebraic number field and $\mathcal{O}_K$ be the ring of integers of K. The set of all nonzero ideals of $\mathcal{O}_K$ forms a multiplicative abelian group $I(K)$.*

Now that we have an algebraic structure with unique factorization and divisibility, we can try to replicate other properties of the integers in this structure. One of the most important theorems that carry over is the Chinese Remainder Theorem [10]:

Theorem 3.3.9. *Suppose D is a Dedekind domain, $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ are distinct prime ideals in D and $r_1, r_2, \ldots, r_n$ are positive integers then*

$$D/\mathfrak{P}_1^{r_1} \ldots \mathfrak{P}_n^{r_n} \simeq D/\mathfrak{P}_1^{a_1} \times D/\mathfrak{P}_2^{a_2} \times \ldots \times D/\mathfrak{P}_n^{r_n}$$

Equivalently for elements $\alpha_1, \ldots, \alpha_n \in D$, then there exists $\alpha \in D$ then

$$\alpha \equiv \alpha_i \pmod{\mathfrak{P}_i^{r_i}}$$

where $i = 1, 2, \ldots, n$.

More generally, if $\mathfrak{I}_1, \ldots, \mathfrak{I}_n$ are pairwise relatively prime ideals of D and

$\alpha_1, \ldots, \alpha_n \in D$, *then there exists* $\alpha \in D$ *such that*

$$\alpha \equiv \alpha_i \pmod{\mathfrak{I}_i}$$

where $i = 1, 2, \ldots, n$.

3.4 Tensor Products

The tensor product representation of the mth cyclotomic number field $K = \mathbb{Q}(\zeta_m)$ is used extensively to make homomorphic operations more efficient in the encryption schemes. In this section we will cover the basics of modules and tensor products to gain a very general understanding of these structures. For more details, the reader is referred to [10].

Definition 3.4.1. *Let R be a commutative ring with unity. An R-module is an abelian group M with an action $R \times M \to M$, written as rv where $r \in R$ and $v \in M$ which satisfies the following conditions:*

1. $1v = v, \ \forall v \in M$
2. $(rs)v = r(sv), \ \forall r, s \in R, \ \forall v \in M$
3. $(r + s)v = rv + sv, \ \forall r, s \in R, \ \forall v \in M$
4. $r(v + w) = rv + rw, \ \forall r \in R, \ \forall v, w \in M$

A submodule $N \subset M$ is an abelian group which is closed under the scaling operation. N almost behaves like an ideal of a ring - given $r \in R$, $rv \in N$ if $v \in N$. Keeping this in mind, one can define M/N to be the set of cosets of N in M with the R-action defined as $r(v + N) = (rv) + N$, which shows that M/N is also an R-module.

An example that we are familiar with from linear algebra is when R is a field, then the R-module is just a vector space over R. Any additive abelian group A is a $\mathbb{Z}$-module where the R-action can be defined as the map $(n, a) \to na$

from $\mathbb{Z} \times A \to A$.
For R-modules M and N, their tensor product $M \otimes_R N$ is an R-module spanned by all symbols $m \otimes n$ where $m \in M$ and $n \in N$ and these symbols satisfy the following laws:

1. $(m + m') \otimes n = m \otimes n + m' \otimes n$, $m \otimes (n + n') = m \otimes n + m \otimes n'$.
2. $r(m \otimes n) = (rm) \otimes n = m \otimes (rn)$.

The essence of these two conditions is captured in the definition of bilinearity as follows:
Definition 3.4.2. *Let M, N and P be R-modules, a map $B : M \times N \to P$ is R-bilinear if*

- $B(m_1 + m_2, n) = B(m_1, n) + B(m_2, n)$, *and* $B(rm, n) = rB(m, n)$.
- $B(m, n_1 + n_2) = B(m, n_1) + B(m, n_2)$, *and* $B(m, rn) = rB(m, n)$.

For example, the dot product of two vectors $\mathbf{v} \cdot \mathbf{w}$ is a bilinear map $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$ given by

- $(\mathbf{v_1} + \mathbf{v_2}) \cdot \mathbf{w} = \mathbf{v_1 w} + \mathbf{v_2 w}$, and $(r\mathbf{v}) \cdot \mathbf{w} = r(\mathbf{v} \cdot \mathbf{w})$.
- $\mathbf{v} \cdot (\mathbf{w_1} + \mathbf{w_2}) = \mathbf{v w_1} + \mathbf{v w_2}$, and $r(\mathbf{v}) \cdot \mathbf{w} = r(\mathbf{v} \cdot \mathbf{w})$.

The tensor product has what is called the universal mapping property. Informally this means that for R-modules M and N, their tensor product $M \otimes_R N$ is a universal object that turns bilinear maps on $M \times N$ into linear maps. We can define the tensor product more formally as follows:
Definition 3.4.3. *Let M and N be R-modules, their tensor product $M \otimes_R N$ is an R-module equipped with the bilinear map*

$$M \times N \xrightarrow{\otimes} M \otimes_R N$$

such that for any bilinear map $M \times N \xrightarrow{B} P$ there is a unique linear map $M \otimes_R N \xrightarrow{L} P$ making the following commute

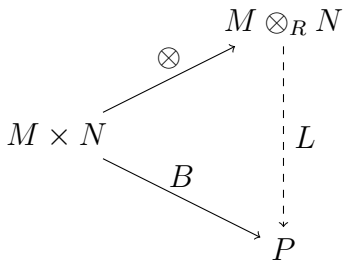

Figure 3.3: Universal Mapping Property of $M \otimes_R N$

Let us see some simple examples of tensor products. Consider $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z}$. Since $3a = a$ for all $a \in \mathbb{Z}/2\mathbb{Z}$, we have

$$a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes 0 = 0$$

Thus $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = 0$. Note that $a \otimes 0 = a \otimes (0 + 0) = a \otimes 0 + a \otimes 0$, thus $a \otimes 0 = 0$.

Now consider $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$, this is generated by $0 \otimes 0 = 1 \otimes 0 = 0 \otimes 1$ and $1 \otimes 1$, note that $1 \otimes 1 \neq 0$ since we can find a non-zero bilinear map from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by $(a, b) \to ab$. Also $2(1 \otimes 1) = 2 \otimes 1 = 0 \otimes 1 = 0$, which implies that $1 \otimes 1$ is of order 2. Thus $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$.

The following theorem is one that is used later in representing a cyclotomic number field as a tensor product of its sub-fields [30].

Theorem 3.4.4. *For ideals $\mathfrak{I}$ and $\mathfrak{J}$ in R, there is a unique R-module isomorphism*

$$R/\mathfrak{I} \otimes_R R/\mathfrak{J} \simeq R/(\mathfrak{I} + \mathfrak{J})$$

where $\bar{x} \otimes \bar{y} \to \overline{xy}$.

3.5 Lattices and Minkowski Theory

This section combines the concepts we learned in Chapters 2 and 3 by applying lattice theory to number fields $K/\mathbb{Q}$ of degree n. We can think of the number field as an n dimensional vector space and we will see that $\mathcal{O}_K$ forms a lattice in this vector space.
Suppose K is a number field and $[K : \mathbb{Q}] = n$, then we have n embeddings $\tau_i : K \to \mathbb{C}$ for all $i \in \{1, 2, \ldots, n\}$. Consider the mapping

$$j : K \to K_{\mathbb{C}}$$

where $K_{\mathbb{C}} := \prod_{\tau_i} \mathbb{C}$, in other words $K_{\mathbb{C}}$ is the direct product of the image of K under each embedding. This mapping is often called the Minkowski embedding and is defined as follows

$$a \to ja = (\tau_1 a, \tau_2 a \ldots, \tau_n a)$$

where $\tau_1, \ldots, \tau_n$ are the n embeddings. Note that the usual inner product definition holds on $K_{\mathbb{C}}$ [25]:

$$\langle x, y \rangle = \sum_{\tau} x_\tau \bar{y}_\tau$$

The goal of this section is to somehow relate K to a Euclidean space so that we can define a lattice structure on it. In order to do this, observe that the real embeddings of K already map into $\mathbb{R}$, so our only concern is the complex embeddings which can be thought of as embeddings into $\mathbb{R}^2$, by splitting them into their real and imaginary components. Finally, note that the complex embeddings are in pairs of complex conjugates. Thus we can ignore half of the complex embeddings and still retain all the information about our n embeddings. This leads us to the description of the Minkowski

space [25],

$$K_{\mathbb{R}} = \{(z_\tau) \in K_{\mathbb{C}} | z_\rho \in \mathbb{R}, z_{\bar{\sigma}} = \bar{z}_\sigma\}$$

where $\rho_1, \ldots, \rho_r$ are the real embeddings and $\sigma_1, \bar{\sigma}_1, \ldots, \sigma_s, \bar{\sigma}_s$ are the complex embeddings such that $n = r + 2s$. The Minkowski space allows us to think of K as an n-dimensional Euclidean space, and the following proposition allows us to interpret the ring of integers of K and its ideals as lattices [25].

Proposition 3.5.1. *Let K be a finite extension of $\mathbb{Q}$ and $\mathfrak{a}$ a non-zero ideal of $\mathcal{O}_K$. Let j be the map from K into the Minkowski space $K_{\mathbb{R}}$. Then $\mathrm{T} = j\mathfrak{a}$ is full-rank lattice in $K_{\mathbb{R}}$ and its fundamental domain has volume*

$$vol(\mathrm{T}) = \sqrt{|d(K)|}(\mathcal{O}_K : \mathfrak{a})$$

Let us illustrate these concepts with an example. Take $K = \mathbb{Q}(\sqrt[3]{2})$, the minimal polynomial is given by $x^3 - 2$ so $[K : \mathbb{Q}] = 3$ and we have three embeddings of K into $\mathbb{C}$ which we can denote by τ_1, τ_2 and τ_3 and are defined as:

$$\begin{aligned}
\tau_1(\sqrt[3]{2}) &= \sqrt[3]{2} \\
\tau_2(\sqrt[3]{2}) &= \sqrt[3]{2}\left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) \\
\tau_3(\sqrt[3]{2}) &= \sqrt[3]{2}\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right)
\end{aligned}$$

Note that τ_1 is a real embedding and $\tau_2 = \bar{\tau}_3$. Then the map $j : K \to K_{\mathbb{R}}$ gives us

$$j(\sqrt[3]{2}) = \left(\sqrt[3]{2}, -\frac{\sqrt[3]{2}}{2}, \frac{\sqrt[3]{2}\sqrt{3}}{2}\right)$$

Recall that for quadratic number fields are monogenic, so a $\mathbb{Z}$ basis for $\mathcal{O}_K$

is given by $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$. We can define a basis for our lattice as

$$
\begin{aligned}
j(1) &= (1, 1, 1) \\
j(\sqrt[3]{2}) &= \left(\sqrt[3]{2}, -\frac{\sqrt[3]{2}}{2}, \frac{\sqrt[3]{2}\sqrt{3}}{2} \right) \\
j((\sqrt[3]{2})^2) &= \left((\sqrt[3]{2})^2, -\frac{(\sqrt[3]{2})^2}{4}, \frac{3(\sqrt[3]{2})^2}{4} \right)
\end{aligned}
$$

Chapter 4

Galois Theory

In the previous chapter, we studied how the $\mathbb{Q}$ can be extended to a field which includes roots of polynomials that have no rational roots and the properties of these algebraic extensions. In this chapter we will delve into the main theory of understanding roots of polynomials in different number fields, and cyclotomic number fields in particular. Our main purpose is to understand how different properties of cyclotomic number fields and their Galois groups help prove the hardness of Ring-LWE in a subsequent chapter.

4.1 Splitting Fields

We define the notion of a splitting field as the following

Definition 4.1.1. *Let $f \in F[x]$ have degree $n > 0$. Then an extension L of F is a splitting field of f over F if*

1. *$f = c(x - \alpha_1)(x - \alpha_2)\dots(x - \alpha_n)$ where $c \in F$ and $\alpha_i \in L$*
2. *L=$F(\alpha_1, \alpha_2, \dots, \alpha_n)$*

Note that not all algebraic extensions of f over F can be splitting fields, for example, consider $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2})$, its minimal polynomial is $x^4 - 2$, but $\mathbb{Q}(\sqrt[4]{2})$ is not the splitting field of $x^4 - 2$ over $\mathbb{Q}$. In fact, $\mathbb{Q}(i, \sqrt[4]{2})$ is a splitting field of $x^4 - 2$ over $\mathbb{Q}$.

Splitting fields of a given polynomial $f \in F[x]$ are not necessarily unique. For example $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}[t]/\langle t^2 - 2\rangle$ are both splitting fields of $x^2 - 2$ over $\mathbb{Q}$. But they are isomorphic to each other [7].

Theorem 4.1.2. *Given $f_1 \in F_1[x]$ and an isomorphism $\Psi : F_1 \simeq F_2$, there is an isomorphism $\bar{\Psi} : L_1 \simeq L_2$ such that $\Psi = \bar{\Psi}|_{F_1}$.*

$$\begin{array}{ccc} L_1 & \xrightarrow{\bar{\Psi}} & L_2 \\ \cup & & \cup \\ F_1 & \xrightarrow{\Psi} & F_2 \end{array}$$

Figure 4.1: Diagram depicting Theorem 4.1.2

An important concept that follows from Theorem 4.1.2 is the following:

Proposition 4.1.3. *Let L be a splitting field of a polynomial in $F[x]$ and suppose that $h \in F[x]$ is irreducible and has roots $\alpha, \beta \in L$. Then there is a field isomorphism $\sigma : L \to L$ that is the identity on F and takes α to β.*

$$\begin{array}{ccc} L & \xrightarrow{\sigma} & L \\ \cup & & \cup \\ F(\alpha) & \to & F(\beta) \end{array}$$

Figure 4.2: Diagram depicting Proposition 4.1.3

As an example, consider $L = \mathbb{Q}(\sqrt{2})$ a splitting field of $x^2 - 2$ over $\mathbb{Q}$. We can easily check that $x^2 - 2$ is irreducible over $\mathbb{Q}$ and has roots $\pm\sqrt{2} \in L$. Then by Proposition 4.1.3, there is an isomorphism $\sigma : L \to L$ such that $\sigma(\sqrt{2}) = -\sqrt{2}$.

Proposition 4.1.3 becomes very useful when constructing elements of Galois

groups. We will see how in the next section. The rest of this section is devoted to studying important properties of splitting fields.

Definition 4.1.4. *An algebraic extension L of F is normal if every irreducible polynomial in $F[x]$ that has a root in L splits completely over L.*

The following theorem relates normal extensions to splitting fields [7]:

Theorem 4.1.5. *Suppose that $F \subset L$. Then L is the splitting field of some $f \in F[x]$ if and only if the extension L is normal and finite.*

We consider a polynomial to be separable if it has distinct roots. More formally:

Definition 4.1.6. *A polynomial $f \in F[x]$ is separable if it is nonconstant and all its roots in a splitting field are simple.*

We can extend the concept of separability to algebraic extensions:

Definition 4.1.7. *Let $F \subset L$ be an algebraic extension.*

1. *$\alpha \in L$ is separable over F if its minimal polynomial over F is separable.*
2. *$F \subset L$ is a separable extension if every $\alpha \in L$ is separable over F.*

It turns out that $f \in F[x]$ is separable only when it is a product of irreducible polynomials, each of which is separable and no two of which are multiples of each other. The following proposition gives us an easy way of determining when an irreducible polynomial is separable.

Proposition 4.1.8. *Let $f \in F[x]$ be an irreducible polynomial of degree n. Then f is separable if either of the following conditions is satisfied.*

1. *F has characteristic 0, or*
2. *F has characteristic $p > 0$ where p is prime and $p \not| n$.*

4.2 The Galois Group

It is fairly straightforward to define a vector space on a field extension, and although this measures the size (the degree of $[L : F]$ is given by the dimension of L considered as a vector space over F), it does not tell us anything deeper about the structure. Galois associated the roots of any polynomial with the permutation of its roots. This group is now called the Galois group in his honor and is formally defined as follows.

Definition 4.2.1. *Let $F \subset L$ be a finite extension. Then $Gal(L/F)$ is*

$$\{\sigma : L \to L | \sigma \text{ is an automorphism and } \sigma(a) = a \ \forall a \in F\}$$

$Gal(L/F)$ consists of all the automorphisms of L that "fix" the elements of F. This forms a group under composition [31].

Proposition 4.2.2. *If L is the splitting field of a separable polynomial in $F[x]$ then the Galois group of $F \subset L$ has order $|Gal(L/F)| = [L : F]$.*

For example, consider the complex numbers, where $\mathbb{C} = \mathbb{R}(i)$. We know $\mathbb{C}$ is the splitting field of the polynomial $x^2 + 1$ in $\mathbb{R}[x]$. Let $\sigma \in Gal(\mathbb{C}/\mathbb{R})$. Since $\sigma(r) = r$ for all $r \in \mathbb{R}$, $\sigma(i) = \pm i$. In other words,

$$\sigma_1 : x + iy \to x + iy$$
$$\sigma_2 : x + iy \to x - iy$$

It can be easily shown that both σ_1 and σ_2 are indeed automorphisms of $\mathbb{C}$, and also $\sigma_2^2 = \sigma_1$. Thus $Gal(\mathbb{C}/\mathbb{R}) = \{1_{\mathbb{C}}, \sigma_2\}$ forms a cyclic group of order 2. It follows that $Gal(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}$. Note that $|Gal(\mathbb{C}/\mathbb{R})| = [\mathbb{C} : \mathbb{R}] = 2$.

Now we can finally come to the main point that Galois associated polynomials and their roots with many years ago. For a splitting field L of a separable polynomial of degree n, $f \in F[x]$, the Galois group $Gal(L/F)$ forms a sub-

group of S_n [7]. When regarding Galois groups in terms of permutations, it is natural to ask how these permutations relate to the corresponding field extension. Let us define a term that will help us in this regard:

Definition 4.2.3. *A subgroup $H \subset S_n$ is transitive if for every pair of elements $i, j \in \{1, \ldots, n\}$, there is a $\tau \in H$ such that $\tau(i) = j$.*

Note that not all subgroups of S_n are transitive. Consider $\{e, (12), (34), (12)(34)\} \subset S_4$. Since no element of the subgroup takes 1 to 3, this is not transitive.
How does transitivity relate to Galois groups and their corresponding field extension? The following very important result was proved by Camille Jordan [7]:

Proposition 4.2.4. *Let L be the splitting field of a separable polynomial $f \in F[x]$ of degree n. Then the subgroup of S_n corresponding to $Gal(L/F)$ is transitive if and only if f is irreducible over F.*

This property is also important with regard to our Ring-LWE discussion later on.

4.3 The Galois Correspondence

Associating the automorphisms on the roots of a polynomial with the permutation group is only scratching the surface of Galois Theory. In this section, we will cover the fundamental properties of the Galois correspondence between a field extension and its Galois group. But first we need to establish some more terminology:

Definition 4.3.1. *Suppose that we have a finite extension $F \subset L$ with Galois group $Gal(L/F)$. Given a subgroup $H \subset Gal(L/F)$, we define the fixed field of H as*

$$L_H = \{\alpha \in L | \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$$

Now we are ready for our first important theorem in this section [7].

Theorem 4.3.2. *Let $F \subset L$ be a finite extension. Then the following are equivalent*

1. *L is the splitting field of a separable polynomial in $F[x]$.*
2. *F is the fixed field of $Gal(L/F)$ acting on L.*
3. *$F \subset L$ is a normal separable extension.*

This theorem lets us make the following definition

Definition 4.3.3. *An extension $F \subset L$ is called a Galois extension if it is a finite extension satisfying any of the equivalent conditions of Theorem 4.3.2.*

For example, the extension $\mathbb{R} \subset \mathbb{C}$ is Galois, since $\mathbb{C} = \mathbb{R}(i)$ is the splitting field of $x^2 + 1$ over $\mathbb{R}$ (by part 1 of Theorem 4.3.2). The following case is one where being a Galois extension is straighforward.

Proposition 4.3.4. *Suppose that $F \subset L$ is a Galois extension and that we have an intermediate field $F \subset K \subset L$. Then $K \subset L$ is a Galois extension.*

In order to understand the fundamental theorem of Galois Theory, we need to understand the relation between normal subgroups and normal extensions. Let us cover some terminology in this regard

Definition 4.3.5. *Suppose that we have finite extensions $F \subset K \subset L$. Then for an automorphism $\sigma \in Gal(L/F)$, we define a conjugate field of K as*

$$\sigma(K) = \{\sigma(\alpha) | \alpha \in K\}$$

Now we can state the main theorem relating normal subgroups to normal extensions [7].

Theorem 4.3.6. *Suppose we have the fields $F \subset K \subset L$ where $F \subset L$ is a Galois extension. Then the following conditions are equivalent:*

1. *$K = \sigma(K)$ for all $\sigma \in Gal(L/F)$.*
2. *$Gal(L/K)$ is a subgroup of $Gal(L/F)$.*

3. *$F \subset K$ is a Galois extension.*

4. *$F \subset K$ is a normal extension.*

In group theory, we learned that normal subgroups are important because we can form quotient groups - recall that if G is a group and N is a normal subgroup, then G/N forms a quotient group. The above theorem shows that normal subgroups occur naturally in Galois theory and we can take full advantage of their properties. We can now state the fundamental theorem of Galois Theory as follows:

Theorem 4.3.7. *Let $F \subset L$ be a Galois extension.*

1. *For an intermediate field $F \subset K \subset L$, its Galois group $Gal(L/K) \subset Gal(L/F)$ has fixed field*

$$L_{Gal(L/k)} = K$$

Furthermore $|Gal(L/K)| = [L : K]$ and $[Gal(L/F) : Gal(L/K)] = [K : F]$.

2. *For a subgroup $H \subset Gal(L/F)$, its fixed field $F \subset L_H \subset L$ has Galois group*

$$Gal(L/L_H) = H$$

Furthermore $[L : L_H] = |H|$ and $[L_H : F] = [Gal(L/F) : H]$.

3. *The maps between intermediate fields $F \subset K \subset L$ and subgroups $H \subset Gal(L/F)$ given by*

$$K \to Gal(L/K)$$
$$H \to L_H$$

reverse inclusions and are inverses of each other. Furthermore if a subfield K corresponds to a subgroup H under these maps then K is Galois

over F if and only if H is normal in $Gal(L/F)$. When this happens there is a natural isomorphism

$$Gal(L/F)/H \simeq Gal(K/F)$$

Let us illustrate these concepts with an example. Consider $\mathbb{Q} \subset \mathbb{Q}(\omega, \sqrt[3]{2})$ which is a splitting field of $x^3 - 2$ over $\mathbb{Q}$. The intermediate fields are shown in

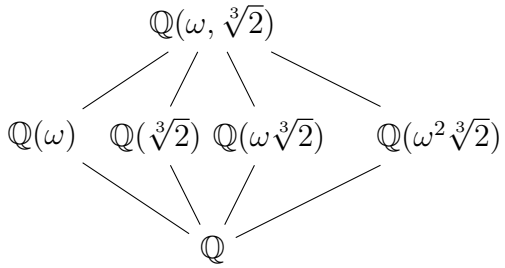

Figure 4.3: Structure of $\mathbb{Q}(\omega, \sqrt[3]{2})$ and its sub-fields.

Figure 4.3. Observe that there are automorphisms $\sigma, \tau \in Gal(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ such that

$$\sigma(\omega) = \omega, \sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$$
$$\tau(\omega) = \omega^2, \tau(\sqrt[3]{2}) = \sqrt[3]{2}$$

Let us label the roots of $x^3 - 2$ as $\alpha_1 = \sqrt[3]{2}$, $\alpha_2 = \omega\sqrt[3]{2}$ and $\alpha_3 = \omega^2\sqrt[3]{2}$. It is easy to see that

$$\sigma \to (123),\ \tau \to (23)$$

Since these permutations generate S_3, we can conclude that $Gal(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}) \simeq S_3$ and that σ and τ generate $Gal(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$. Now σ has order 3, so $\langle\sigma\rangle = \{e, \sigma, \sigma^2\}$, similarly it is easy to check that $\langle\tau\rangle, \langle\sigma^2\tau\rangle$ and $\langle\sigma\tau\rangle$ are subgroups of order 2. This gives rise to the structure shown in Figure 4.4. From Theorem 4.3.7, and our discussion above, we can see the Galois correspondence between the subgroups of $Gal(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ (shown in Figure

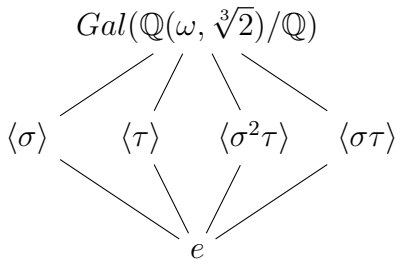

Figure 4.4: Structure of $Gal(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ and its sub-groups.

4.4) and the subfields of $\mathbb{Q}(\omega, \sqrt[3]{2})$ (shown in Figure 4.3). Note that Theorem 4.3.7 tells us that Figure 4.4 shows us *all* subgroups of $Gal(\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q})$ and Figure 4.3 shows us *all* the subfields of $\mathbb{Q}(\omega, \sqrt[3]{2})$ containing $\mathbb{Q}$.

4.4 Galois Group of a Cyclotomic Extension

Recall that given:

$$x^n - 1 = \prod_{r=0}^{n} (x - \zeta_n^r)$$

we define the nth cyclotomic polynomial $\Phi_n(x)$ to be the product

$$\Phi_n(x) = \prod_{\substack{r=1, \\ (r,n)=1}}^{n} (x - \zeta_n^r)$$

Let us look at some examples of cyclotomic polynomials. For $n = 2$, we know that $\Phi_2(x) = x - (-1) = x + 1$. When $n = 4$, the fourth roots of unity whose powers are relatively prime to n are i and $i^3 = -i$, thus $\Phi_4(x) = (x - i)(x - (-i)) = (x - i)(x + i) = x^2 + 1$. An elementary property of cyclotomic polynomials is stated as follows [7]:

Proposition 4.4.1. *The nth cyclotomic polynomial $\Phi_n(x)$ is a monic polynomial with integer coefficients and has degree $\phi(n)$. Furthermore, these poly-*

nomials satisfy the identity

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

In this section, we are particularly interested in computing the Galois group $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. In order to do this, we need to know the minimal polynomial of ζ_n over $\mathbb{Q}$. Intuitively we would think that $\Phi_n(x)$ would be the minimal polynomial, but in order to conclude this, we need the following theorem [10]:
Theorem 4.4.2. *The cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.*

This implies that $\mathbb{Q}(\zeta_n)$ is the splitting field of $\Phi_n(x)$ over $\mathbb{Q}$ and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ which also means $\mathbb{Q} \subset \mathbb{Q}(\zeta_n)$ is a Galois extension (Theorem 4.3.2). Equipped with these tools, we can now understand how the Galois group of a cyclotomic extension is given by the following [7]:
Theorem 4.4.3. *There is an isomorphism $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$ such that $\sigma \in Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ maps to $[l] \in (\mathbb{Z}/n\mathbb{Z})^*$ if and only if $\sigma(\zeta_n) = \zeta_n^l$.*

4.5 Cyclotomic Polynomials modulo a Prime

In a characteristic 0 field, the minimal polynomial of a primitive d^{th} root of unity in $\mathbb{C}$ is the cyclotomic polynomial $\Phi_d(x)$. But what happens when we are working in a field of characteristic p, where p is a prime? Recall that in $\mathbb{Z}[x]$, $\Phi_d(x)$ has the factorization

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

In studying the reduction of $\Phi_d(x)$ modulo p, we will restrict ourselves to the case when $(d, p) = 1$ [7].
Proposition 4.5.1. *Let F be a field of characteristic p and let $\alpha \in F$ be a*

root of unity, then there exists a $d \geq 1$ relatively prime to p such that α is a dth root of unity.

Recall that a dth root of unity α is primitive if d is the smallest positive integer such that $\alpha^d = 1$. The roots of $\Phi_d(x)$ can be described as follows [7]:

Theorem 4.5.2. *If $(d, p) = 1$ and $q = p^n$ then the following are equivalent:*

1. $q \equiv 1 \pmod{d}$.
2. $\Phi_d(x)$ *splits completely in* $\mathbb{F}_q$.
3. $\Phi_d(x)$ *has a root in* $\mathbb{F}_q$.

Furthermore when these conditions are satisfied, the roots of $\Phi_d(x)$ in $\mathbb{F}_q$ consist of the primitive dth roots of unity.

In order to compute the irreducible factors of $\Phi_d(x)$, observe that since $(d, p) = 1$, then $[p] \in (\mathbb{Z}/d\mathbb{Z})^*$. Suppose m is the order of $[p]$ in this group, then $[p]^m = [1]$ or $p^m \equiv 1 \pmod{d}$. Thus m is the smallest positive integer such that $d | p^m - 1$. Formally stated [7]:

Theorem 4.5.3. *Given d, let m be the order of $[p]$ in $(\mathbb{Z}/d\mathbb{Z})^*$. Then $\Phi_d(x)$ is the product of $\phi(d)/m$ irreducible polynomials in $\mathbb{F}_p[x]$ of degree m.*

Let us illustrate this concept with an example. Consider $p = 2$ and $d = 5$. It is easy to check that the order of $[2]$ in $(\mathbb{Z}/5\mathbb{Z})^*$ is 4, thus $m = 4$. Using Theorem 4.5.3, $\Phi_5(x)$ is the product of $\phi(5)/4 = 1$ irreducible polynomials of degree 4 in $\mathbb{F}_2[x]$. Thus we can conclude that $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. By Theorem 4.5.2, the roots of $\Phi_5(x)$ are the primitive 5th roots of unity in $\mathbb{F}_{16}$.

4.6 Prime Splitting

In this section, we discuss how to factor ideals in rings of integers of number fields. This section overlaps considerably with the previous section but it is

important to understand this concept from an algebraic number theory point of view. Hence this overlap is a small consequence. Suppose we have number fields $K \subseteq L$ ($\mathcal{O}_K \subseteq O_L$), for an ideal $\mathfrak{a}$ of $\mathcal{O}_\mathcal{K}$, we want to know how $\mathfrak{a}O_L$ factors in $\mathcal{O}_K$. In particular, we are interested in the case when $\mathfrak{a}$ is prime and K is a cyclotomic number field in $K/\mathbb{Q}$.

Proposition 4.6.1. *Let K be a number field and $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. Then $\mathfrak{p}$ contains a rational prime.*

From the above proposition [32] and our knowledge of ideals, we can conclude that all non-zero primes of $\mathcal{O}_K$ divide an ideal of the form $p\mathcal{O}_K$ for some prime $p \in \mathbb{Z}$. This tells us that we can determine all primes of $\mathcal{O}_K$ by determining the factorization of the ideals $p\mathcal{O}_K$.
We want to focus on K being the mth cyclotomic number field. But before we can discuss this case, we must become familiar with some definitions and notations. For a number field of degree n, if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and p is a rational prime, we say that $\mathfrak{p}$ lies above p, if $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ (see Figure 4.5). Recall that the residue field is the quotient of a commutative ring by a

$$\begin{array}{ccccc} \mathfrak{p} & \subset & \mathcal{O}_K & \subset & K \\ & & | & & \\ p\mathbb{Z} & \subset & \mathbb{Z} & \subset & \mathbb{Q} \end{array}$$

Figure 4.5: Depiction of $\mathfrak{p}$ lying above p

maximal ideal, thus in this case, the residue field of $p\mathbb{Z}$ is $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We are interested in the residue field $\mathcal{O}_K/\mathfrak{p}$, it can be shown that this is an $\mathbb{F}_p$-vector space of finite dimension [32].
Definition 4.6.2. *Let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$ lying above $p \in \mathbb{Z}$. We define the ramification index $e(\mathfrak{p}/p)$ to be the exact power of $\mathfrak{p}$ dividing $p\mathcal{O}_K$.*
Definition 4.6.3. *The dimension of the $\mathbb{F}_p$-vector space $\mathcal{O}_K/\mathfrak{p}$ is called the*

inertial degree $f(\mathfrak{p}/p)$

$$f_{\mathfrak{p}} = dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})$$

The factorization of $p\mathcal{O}_K$ can thus be written as [17].

$$\prod_{\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}} \mathfrak{p}^{e(\mathfrak{p}/p)}$$

It is useful to have a notion of size when dealing with these ideals. For $\mathfrak{a}$ in $\mathcal{O}_K$, we can define the ideal norm to be $N_{K/\mathbb{Q}}(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. For a prime ideal $\mathfrak{p}$, we have $N_{K/\mathbb{Q}}(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = |\mathbb{F}_p^{\dim_{\mathbb{F}_p}(\mathcal{O}_K/\mathfrak{p})}| = |\mathbb{F}_p|^{f(\mathfrak{p}/p)} = p^{f(\mathfrak{p}/p)}$. Like the regular norm, the ideal norm is also multiplicative. The following gives us the fundamental relationship between the ramification index, inertial degree and degree of a number field [17]:

Proposition 4.6.4. *Let K be a number field of degree n and p be a rational prime such that*

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$$

is the prime factorization of $p\mathcal{O}_K$ in $\mathcal{O}_K$ where $e_i = e(\mathfrak{p}_i/p)$. Let $f_i = f(\mathfrak{p}_i/p)$. Then

$$\sum_i^r e_i f_i = n$$

Even though it might be difficult to write down the explicit factors, we can now describe a good way of factorizing cyclotomic polynomials. One of the main results is that the mth cyclotomic polynomial is the "universal" polynomial for testing if an element of a field is a primitive mth root of unity [32].

Proposition 4.6.5. *Let m be a positive integer and let K be a field of characteristic not dividing m. Let α be an element of K. Then $\Phi_m(\alpha) = 0$ if and only if α is a primitive mth root of unity.*

Let $K = \mathbb{Q}(\zeta_m)$ and p be a rational prime. Suppose $\mathfrak{p}$ is a prime ideal of

$\mathcal{O}_K = \mathbb{Z}[\zeta_m]$ lying above p. We want to determine e and f for this particular case. Since K is a Galois extension of $\mathbb{Q}$, the following proposition is useful [32]:

Proposition 4.6.6. *Let $K \subset L$ be a Galois extension of degree n and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Let*

$$\mathfrak{p}O_L = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$$

be the factorization of $\mathfrak{p}$ in O_L where $e_i = e(\mathfrak{P}_i/p)$. Let $f_i = f(\mathfrak{P}_i/p)$. Then

$$f_1 = f_2 = \dots = f_r$$
$$e_1 = e_2 = \dots = e_r$$

In particular, $re_if_i = n$ for all i.

It follows that $\Phi_m(x)$ factors in $\mathbb{F}_p[x]$ as

$$\Phi_m(x) = (g_1(x) \dots g_r(x))^e$$

where $deg(g_i) = f$ for all i and $efr = \phi(m)$.

Let us consider the case that $p \nmid m$, recall that $x^m - 1 = \prod_{d|m} \Phi_d(x)$. Since $x^m - 1$ does not have any repeated roots in $\mathbb{F}_p[x]$, $x^m - 1$ does not have any repeated roots either. Specifically $e = 1$. Now we have to determine f and r. We will focus on the special case of $f = 1$, then $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$ and $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$ which means that $\Phi_m(x)$ has roots in $\mathbb{F}_p$. By Proposition 4.6.5, this means that $\mathbb{F}_p$ has primitive mth roots of unity. Since $\mathbb{F}_p$ is a cyclic group of order $p-1$, it has elements of exact order $m-1$ if and only if $p-1 \equiv 0 \pmod{m}$. Thus we have shown that a rational prime p splits $\mathbb{Q}(\zeta_m)$ if and only if $p \equiv 1 \pmod{m}$. The general case is covered in [32]. We obtain the result that we have already seen in Theorem 4.5.3 but restated in terms of ramification theory:

Proposition 4.6.7. *Let p be a rational prime such that $p \nmid m$ and let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[\zeta_m]$ lying over p. Then $e(\mathfrak{p}/p) = 1$, $f(\mathfrak{p}/p)$ is the order of*

p in $(\mathbb{Z}/m\mathbb{Z})^*$ and there are exactly $\phi(m)/f(\mathfrak{p}/p)$ primes of $\mathbb{Z}[\zeta_m]$ lying over p.

Let us consider the following example where $K = \mathbb{Q}(\zeta_5)$. The behavior of a rational prime in $\mathcal{O}_K$ is determined by the residue class of p in $(\mathbb{Z}/m\mathbb{Z})^*$. If $p \equiv 1 \pmod 5$, then p splits completely in $\mathcal{O}_K$. Consider $p = 11 \equiv 1 \pmod 5$. We know that $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, thus in modulo 11, we have

$$x^4 + x^3 + x^2 + x + 1 = (x+2)(x+6)(x+7)(x+8) \pmod{11}$$

so

$$(11) = (11, \zeta_5 + 2)(11, \zeta_5 + 6)(11, \zeta_5 + 7)(11, \zeta_5 + 8)$$

Chapter 5

Ring Learning With Errors

5.1 The LWE Problem

The Learning With Errors (LWE) problem was first introduced by Oded Regev [28]. This was a huge breakthrough in cryptography, since cryptographic constructions could now be based off the hardness of this problem which was proven to be as hard as worst-case lattice problems. Given $q \geq 2$ and $n \in \mathbb{Z}^+$, the LWE problem can be simply stated as recovering $s \in \mathbb{Z}_q^n$ from a sequence of "approximate" linear equations. If the equations were exact, this problem could be solved very easily in polynomial time, using Gaussian elimination. Stated formally [29]:
Define a probability distribution χ on $\mathbb{Z}_q$. Let $A_{s,\chi}$ be the probability distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$, obtained by choosing a vector $\mathbf{a} \in \mathbb{Z}_q^n$ uniformly at random and $e \in \mathbb{Z}_q$ according to χ. An algorithm solves the LWE problem if for any $\mathbf{s} \in \mathbb{Z}_q^n$, given a set of independent samples from $A_{s,\chi}$, it outputs s with a high probability.

Definition 5.1.1. *We denote poly(n) as*

$$poly(n) = \{f | f \in O(n^c), for\ some\ c > 0\}$$

Alternatively, the LWE problem can be stated as, given a set of samples (polynomial in n), to determine whether they originated from the $A_{s,\chi}$ oracle for some $\mathbf{s}$ or whether they follow the uniform distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$. The decision version of the LWE problem (DLWE) is the problem of distinguishing between LWE samples from the $A_{s,\chi}$ oracle and samples taken from a uniform distribution [5]:

$$\{\mathbf{a_i}, \langle \mathbf{a_i} \cdot \mathbf{s} \rangle + e_i\}_{i=1}^{\text{poly(n)}} \approx \{\mathbf{a_i}, u_i\}_{i=1}^{\text{poly(n)}}$$

where $u_i \in \mathbb{Z}_q$ is drawn uniformly at random. For a number q which is polynomial in n and a normal distribution we can show that there is a reduction from LWE to DLWE. One way to do this is to guess each coordinate of $\mathbf{s}$ individually. Let s_1 be our guess for the first coordinate of $\mathbf{s}$, $(\mathbf{a}, b)$ be our LWE pair and r drawn uniformly at random from $\mathbb{Z}_q$. We can send $(\tilde{\mathbf{a}}, \tilde{b}) = (\mathbf{a} + (r, 0, \ldots, 0), b + rs_1)$ to the decision oracle. Note that

$$\begin{aligned} b &= \langle \mathbf{a} \cdot \mathbf{s} \rangle + e_1 \\ &= \langle (a_1, \ldots, a_n) \cdot (s_1, \ldots, s_n) \rangle + e_1 \\ &= a_1 s_1 + \ldots + a_n s_n + e_1 \end{aligned}$$

so we have,

$$\begin{aligned} \tilde{b} &= \langle \tilde{\mathbf{a}} \cdot \mathbf{s} \rangle + e_1 \\ &= \langle (a_1 + r, a_2, \ldots, a_n) \cdot (s_1, \ldots, s_n) \rangle + e_1 \\ &= a_1 s_1 + \ldots + a_n s_n + e_1 + r s_1 \\ &= b + r s_1 \end{aligned}$$

Now, if s_1 is correct then the sample originated from the $A_{s,\chi}$ oracle, if it is incorrect, then the sample originated from a uniform distribution. Thus we can find the correct s_1 after at most q attempts. This process can be repeated n times to recover all the coordinates of $\mathbf{s}$.

The best known algorithm for solving LWE is given by Blum, Kalai and Wasserman [4] which requires $2^{O(n)}$ samples and time. For cryptographic applications, the modulus q is typically taken to be polynomial in n. The hardness of LWE for polynomial moduli q is based on the fact that GAPSVP or SIVP are hard to approximate to within polynomial factors even with a quantum computer [29].

5.2 Probability Distributions

In this section we will provide a brief overview of the probability distributions used and their role in Learning With Errors, but for further details, the reader is directed to [28]. The Gaussian distribution is the continuous probability distribution on $\mathbb{R}$ given by the probability density function $\frac{1}{\sigma\sqrt{2\pi}} \exp\left(\frac{-(x-\mu)^2}{2\sigma^2}\right)$. When $\mu = 0$, we have the density function $\frac{1}{\sigma\sqrt{2\pi}} \exp\left(\frac{-x^2}{2\sigma^2}\right)$. Since we are dealing with lattices, we want to define a normal distribution on vectors.

Recall that the sum of two independent normal variables with mean 0 and variances σ_1^2 and σ_2^2 is also a normal variable with mean 0 and variance $\sigma_1^2 + \sigma_2^2$. Then for a vector $\mathbf{x}$ and $s > 0$ we define the Gaussian function over $\mathbb{R}^n$ by

$$\rho_s(\mathbf{x}) = \exp(-\pi \|\mathbf{x}/s\|^2).$$

Note that $\int_{\mathbf{x}\in\mathbb{R}^n} \rho_s(\mathbf{x})\, d\mathbf{x} = s^n$. We can then define the n dimensional probability density function of this distribution as:

$$\nu_s = \rho_s / s^n$$

We now have all the necessary tools to define a discrete Gaussian probability distribution.

Definition 5.2.1. *Given a countable set $A \subset \mathbb{R}^n$ and a parameter $s > 0$, the discrete Gaussian probability distribution $D_{A,s}$ for all $\mathbf{x} \in A$ is defined as*

$$D_{A,s}(\mathbf{x}) = \frac{\rho_s(\mathbf{x})}{\rho_s(A)},$$

where $\rho_s(A) = \sum_{\mathbf{y} \in A} \rho_s(\mathbf{y})$

For a probability density function ϕ on $\mathbb{T}$, where $\mathbb{T}$ is the segment $(0, 1]$ with addition modulo 1, we can define the distribution on $\mathbb{Z}_p^n \times \mathbb{T}$ (denoted by $A_{\mathbf{s},\phi}$) as the following: choose a vector $\mathbf{a} \in \mathbb{Z}_p^n$ uniformly at random, choose $e \in \mathbb{T}$ according to ϕ and output $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle / p + e)$.
Relating this back to the LWE problem: For an integer $p \geq 2$, define $\chi : \mathbb{Z}_p \to \mathbb{R}^+$ to be some probability distribution on $\mathbb{Z}_p$ and for an integer n, let $\mathbf{s} \in \mathbb{Z}_p^n$. The discrete Gaussian distribution on $\mathbb{Z}_p^n \times \mathbb{Z}_p$, denoted by $A_{\mathbf{s},\chi}$ is obtained by choosing $\mathbf{a} \in \mathbb{Z}_p^n$ uniformly at random, choosing $e \in \mathbb{Z}_p$ according to χ and outputting $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)$. Here, additions are performed in $\mathbb{Z}_p$.

5.3 Classical and Quantum Reductions of LWE

In Chapter 1, we learned about two worst case lattice problems - the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP). The classical and quantum reductions of LWE rely heavily on the following variations of these problems:

Definition 5.3.1. *For $\lambda_1 \geq 1$, the γ-approximate Shortest Independent Vectors Problem ($SIVP_\gamma$), given a basis B of an n-dimensional lattice $L = L(B)$, asks to find linearly independent vectors $\mathbf{v_1}, \mathbf{v_2}, \ldots, \mathbf{v_n} \in L$ such that $\max_i ||\mathbf{v_i}|| \leq \gamma \lambda_1(L)$, where λ_1 is the smallest positive real r such that $N(\mathbf{0}, r) = \{\mathbf{x} : ||x|| \leq r\}$ of radius r centered at the origin contains at least n linearly*

independent vectors.

Definition 5.3.2. *$GAPSVP_\gamma$, given a basis B of an n-dimensional lattice $L = L(B)$ and a positive real d, asks to determine if $\lambda_1(L) \leq d$ or $\lambda_1(L) > \gamma d$.*

Definition 5.3.3. *$GAPSVP_{\zeta,\gamma}$, for $\zeta(n) \geq \gamma(n) \geq 1$, given a basis B and d which satisfy the following conditions:*

- *B is a basis of an n-dimensional lattice L for which $\lambda_1(L) \leq \zeta(n)$*
- $\min_i ||\tilde{\mathbf{b_i}}||$
- $1 \leq d \leq \zeta(n)/\gamma(n)$

asks to determine if $\lambda_1(L) \leq d$ or if $\lambda_1(L) > \gamma(n) \cdot d$.

The following lattice problem is similar in nature to CVP:

Definition 5.3.4. *BDD_α, given a basis B of an n-dimensional lattice $L = L(B)$ and a vector $\mathbf{t}$ such that $dist(\mathbf{t}, B) < \alpha\lambda_1(B)$, find the lattice vector $\mathbf{v} \in L$ closest to $\mathbf{t}$.*

The dual of the lattice is a very important concept that is also used in defining the Ring Learning with Errors (RLWE) later in the chapter.

Definition 5.3.5. *L^* is the dual of the lattice L, defined as the set of all vectors $\mathbf{y}$ such that $\langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}$ for all vectors $\mathbf{x} \in L$.*

Definition 5.3.6. *The smoothing parameter ($\eta_\epsilon(L)$) for an n dimensional lattice L and positive real $\epsilon > 0$ is defined as the smallest s such that $\rho_{1/s}(L^* \setminus 0) \leq \epsilon$.*

Definition 5.3.7. *A negligible function denoted by $negl(n)$, is an $f(n)$ such that $f(n) = o(n^{-c})$ for every fixed constant c.*

We can define a Gaussian distribution on L as $D_{L,r}$ that assigns mass proportional to $\exp(-\pi||\mathbf{x}/r||^2)$ to each point $\mathbf{x} \in L$. Samples from $D_{L,r}$ are lattice vectors of norm roughly $\sqrt{nr}$. Note that if r is too small, $D_{L,r}$ would essentially be a deterministic distribution on the origin, thus we require r to be *not too small* (specific lower bounds on r are given in [29]). Gentry et al.

, showed how to sample from a discrete Gaussian distribution over a lattice L using the following proposition [13]:

Proposition 5.3.8 (Theorem 4.1)**.** *There exists a probabilistic polynomial-time algorithm that, given an n-dimensional lattice $L = L(B)$ and $r \geq \max_i ||\tilde{\mathbf{b_i}}|| \cdot \omega(\sqrt{\log n})$ outputs a sample that is within negligible statistical distance of $D_{L,r}$.*

The core of the LWE hardness result lies in the proposition that assuming we have access to an LWE oracle with modulus q and error α, and the following inputs: lattice L, a polynomial number of samples from a discrete Gaussian distribution $D_{L^*,r}$, and a point $\mathbf{x}$ within distance $\alpha q/(\sqrt{2}r)$ of any point in L, solving LWE can be reduced to solving the BDD_α problem in polynomial time.

Regev [26] gave a quantum reduction from worst-case $GAPSVP$ and SVP to LWE. This result holds as long as there is no quantum algorithm that solves $GAPSVP$ or $SIVP$, thus in a way, this is weaker than a classical reduction. Peikert showed that the LWE problem can be reduced classically to a variant of $GAPSVP_\gamma$, namely $GAPSVP_{\zeta,\gamma}$. This variant is equivalent to $GAPSVP_\gamma$ for large values of ζ, and occurs when q is exponential in n. In order to achieve this, he used the classical part of Regev's reduction [28]:

Lemma 5.3.9. *Let $\epsilon(n)$ be a negligible function, $q(n) \geq 2$ be an integer and $\alpha(n) \in (0,1)$ be a real number. Given a polynomial number of samples, assume that we have access to an oracle W that solves LWE_{q,Ψ_α}. Then there exists a constant $c > 0$ and an efficient algorithm R that given as input: basis B of a lattice L, a parameter $r \geq \sqrt{2}q \cdot \eta_e(L^*)$ and n^c samples from $D_{L^*,r}$, solves $BDD_{\alpha q/\sqrt{2}r}$.*

Here Ψ_α is a discrete Gaussian distribution, η_ϵ is the smoothing parameter. The main theorem is the following [26]:

Theorem 5.3.10. *Suppose $\alpha(n) \in (0,1)$ and $\gamma(n) \geq n/(\alpha\sqrt{\log n})$. Let $\zeta(n) \geq \gamma(n)$ and $q(n) \geq \zeta(n) \cdot \omega(\sqrt{(\log n)/n})$. Then there is a probabilistic polynomial-time reduction from solving $GAPSVP_{\zeta,\gamma}$ in the worst case to*

solving LWE_{q,Ψ_α} using poly(n) samples.

In order to efficiently generate samples from a Gaussian distribution that is within a fixed statistical distance in Regev's quantum reduction part, lattice reduction algorithms like the Lenstra-Lenstra-Lovasz (LLL) are used [19]. This approximation algorithm outputs a short vector, not necessarily the shortest vector and a whole reduced basis. As seen in chapter 1, LLL can approximate SVP within a factor of $O((2/\sqrt{3})^n)$.
The Blockwise Korkine-Zolotarev (BKZ) Algorithm is the best lattice reduction algorithm known in practice [6]. It outputs a BKZ-reduced basis with blocksize $\beta \geq 2$ and reduction factor $\epsilon > 0$, from an input basis B of a lattice L. It starts by LLL-reducing the basis B, then iteratively reduces each local block to make sure that the first vector of each such block is the shortest in the projected lattice. No good upper bound is known for the time complexity of this algorithm.

5.4 The Ring-LWE Problem

Although the Learning With Errors (LWE) problem has been used in many cryptographic applications due to its strong security assumptions, these applications are relatively inefficient due to requiring at least n vectors. This leads to key sizes of order n^2 which means there is an inherent quadratic overhead. In order to produce an alternative that improves upon this efficiency, the Ring-LWE problem was introduced [21].
Let $K = \mathbb{Q}(\zeta_m)$ where $\zeta_m \in \mathbb{C}$ is a primitive mth root of unity, define $R = \mathcal{O}_K = \mathbb{Z}[\zeta_m]$ as its ring of integers. Let $q \equiv 1 \bmod m$ be a prime that is polynomial in n. Then, informally, the ring-LWE problem can be described as follows:
Assuming that the search version of SVP is considered to be hard to approximate by polynomial time quantum algorithms in the worst case on ideal

lattices in R to within a fixed $poly(n)$ factor, then any $poly(n)$ number of samples drawn from the Ring-LWE distribution are pseudorandom to any polynomial time (possibly quantum) attacker.

The proof for this statement is done in two components, the first component is a quantum reduction from the worst-case SVP on ideal lattices to the search version of Ring-LWE. Assuming that the search version of Ring-LWE is hard, the authors then prove that the Ring-LWE distribution is indeed pseudorandom. In this section, we discuss the mathematical tools and properties used by the authors to achieve this [21]. In the next section we focus on the properties of cyclotomic number fields that make them a good fit for this proof.

Duality. For any lattice L in K, i.e, for the $\mathbb{Z}$-span of any $\mathbb{Q}$-basis of K, its dual is defined by

$$L^* = \{\beta \in K : tr(\beta L) \in \mathbb{Z}\}$$

Error Distribution. Although the error distribution is an essential part of this proof, we will not go into its discussion in great detail. The reader is advised to look at [21] for further clarifications. Recall that in the LWE problem, the Gaussian distribution used was one-dimensional, in the Ring-LWE problem, the error is an n-dimensional Gaussian where n is the degree of the mth cyclotomic number field K. The error is chosen according to a discretized Gaussian with respect to a special basis of the space in which R is embedded using the Minkowski embedding. In this way, an n dimensional Gaussian distribution is simply represented by n parameters.

The Ring-LWE problem is associated with the Ring-LWE distribution which is parameterized by a number field K with ring of integers $R = \mathcal{O}_K$ and a rational integer modulus $q \geq 2$. Let R^* denote the dual of R. The number field K is mapped to $\mathbb{C}^n$ using the Minkowski embedding that we saw in Chapter 3. Recall that the resulting vector space $\mathbb{C}^n$ endowed with a standard inner product. The discretized Gaussian distribution $\mathbb{T} = K_{\mathbb{R}}/R^*$ is the

spherical Gaussian with respect to this inner product, discretized to R^* [11]. The Ring-LWE distribution is formally defined as [21]:

Definition 5.4.1. *For secret $s \in R_q^*$ and error distribution ψ over the Minkowski space $K_\mathbb{R}$, a sample from the ring-LWE distribution $A_{s,\Psi}$ over $R_q \times \mathbb{T}$ is generated by choosing $a \leftarrow R_q$ uniformly at random, choosing $e \leftarrow \psi$, and outputting $(a, b = (a \cdot s)/q + e \pmod{R^*})$.*

For cryptographic applications, we are interested in the average case decision version of the Ring-LWE problem whose hardness means that the ring-LWE distribution is pseudorandom.

Definition 5.4.2. *Let Υ be a distribution over a family of error distributions, each over $K_\mathbb{R}$. The average case decision version of the ring-LWE problem denoted by R-DLWE$_{q,\Upsilon}$ is to distinguish with non-negligible advantage between arbitrarily many independent samples from $A_{s,\psi}$ for a random choice of $(s, \psi) \leftarrow U(R_q^*) \times \Upsilon$ and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$.*

The main theorem is stated as follows [21]:

Theorem 5.4.3. *Let K be the mth cyclotomic number field having dimension $n = \phi(m)$ and $R = \mathcal{O}_K$ be its ring of integers. Let $\alpha = \alpha(n) > 0$ and let $q = q(n) \geq 2$, $q = 1 \pmod{m}$ be a poly(n)-bounded prime such that $\alpha q \geq \omega(\sqrt{\log n})$. Then there is a polynomial-time quantum reduction from $\tilde{O}(\sqrt{n}/\alpha)$-approximate SIVP (or SVP) to R-DLWE$_{q,\Upsilon_\alpha}$.*

5.5 Cyclotomic Number Fields

Let $K = \mathbb{Q}(\zeta_m)$ where m is a primitive root of unity which has a minimal polynomial $\Phi_m(x)$ of degree $n = \phi(m)$ and $R = \mathcal{O}_K = \mathbb{Z}[\zeta_m]$ is its ring of integers. Many properties of cyclotomic number fields are useful both in the proof to show that the Ring-LWE distribution is pseudorandom as well as to perform efficient computations in the number field. We have seen most of

these properties in previous chapters, in this section we will summarize the properties that are used in proving the pseudorandomness of Ring-LWE in a concise manner. The properties of cyclotomic fields pertaining to efficiency will be discussed in the next chapter.

Galois extension. From Theorem 4.4.3, we know that $\mathbb{Q}(\zeta_m)$ is a Galois extension of $\mathbb{Q}$, more precisely

$$Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$$

where each $\sigma \in Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ maps to $[k] \in (\mathbb{Z}/m\mathbb{Z})^*$ if and only if $\sigma(\zeta_m) = \zeta_m^k$. Thus there are $n = \phi(m)$ automorphisms σ_k given by the above. Since $\Phi_m(x)$ is irreducible (Theorem 4.4.2), the transitive property applies (Theorem 4.2.4) to the permutation group corresponding to $Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.

Prime splitting. Given a prime $q \equiv 1 \pmod{m}$, from Theorem 4.5.3, we know that q splits $\Phi_m(x)$ completely into linear factors which can be written as $\Phi_m(x) = \prod_{i \in \mathbb{Z}_m^*}(x - \omega^i)$. In Chapter 3.6, we have seen that the ideal $\mathfrak{q}$ lying above q can be factored in K as $\mathfrak{q} = \prod_{i \in \mathbb{Z}_>^*} \mathfrak{q}_i$ where $\mathfrak{q}_i = \langle q, \zeta_m - \omega^i \rangle$ where $N_{K/\mathbb{Q}}(\mathfrak{q}) = q$. The above properties are heavily relied upon when proving the search-to-decision reduction in Ring-LWE [21].

Chapter 6

Efficiency of Homomorphic Operations

This chapter exploits the Ring-LWE hardness problem in a cryptographic setting and shows experimental results for measuring the performance of homomorphic multiplication by varying the different parameters associated with the cipherspace ring in this cryptosystem.

6.1 Homomorphic Encryption System

The following encryption scheme has been described in [20] with some changes regarding Key Switching and Ring Tunneling introduced in [8]. The reader is advised to read [8] for a more detailed discussion. The main parameters in this cryptosystem are the rings of integers of $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_{m'})$, denoted by $R = \mathbb{Z}[\zeta_m] = \mathcal{O}_m$ and $R' = \mathbb{Z}[\zeta_{m'}] = \mathcal{O}_{m'}$ where $m|m'$, making R a subring of R'. Thus we can embed R into R' by identifying ζ_m with $\zeta_{m'}^{m'/m}$. In the reverse direction we can 'twace' from R' to R. The "twace" is an R linear function that fixes R pointwise.

The dual ideal is the principal fractional ideal $R^* = (g_m/\hat{m})R$ where $\hat{m} = m/2$ if m is even and $\hat{m} = m$ otherwise. The special element $g_m \in R$ is defined as follows:

- when $m = p^e$ for prime p and $e \geq 1$, we have

$$g_m = \begin{cases} g_p = 1 - \zeta_p, & p \text{ is odd} \\ g_p = 1, & p = 2 \end{cases}$$

- when $m = \prod_l m_l$ where m_l are powers of distinct primes, we have $g_m = \prod_l g_{m_l}$.

This is used for managing error terms in the following encryption system. Although the secret s is sampled from R^* to prove the Ring-LWE hardness, it is more convenient to use R for practical purposes when sampling s. This can be done without any loss in security or efficiency [8] by working with an equivalent "tweaked" form of the problem, which is obtained by multiplying the noisy products b_i by a certain factor $t = t_m \in R_m$ for which $t \cdot R^* = R$. The new noisy products are now

$$b'_i = t \cdot b_i = a_i \cdot (t \cdot s) + t \cdot e_i \mod qR$$

The error term $t \cdot e_i$ now comes from the "tweaked" distribution $t \cdot \psi$.

- **Key Space, Plaintext Space, Ciphertext Space**
  The secret key s is an element of R'. For a small positive integer p that is coprime with every prime factor of m', the plaintext space is defined as $R_p = R/pR$. For an integer modulus $q \geq p$ that is coprime to p, we define the ciphertext space as $R'_q = R'/qR'$. Note that although the Ring-LWE hardness was initially proven for prime $q \equiv 1 \pmod{m}$, recent developments [26] show that the hardness can be extended to any integer q [20]. For an (unknown) secret key S, consid-

ered an indeterminant, we can think of a ciphertext as a polynomial $c(S) \in R'_q[S]$. An alternate way to think of $c(S)$ is as a vector of coefficients $(c_0, c_1, \ldots, c_d) \in (R'_q)^{d+1}$, where d is the degree of $c(S)$. Additionally a ciphertext is parameterized by a non-negative integer k and a factor $l \in \mathbb{Z}_p$.

- **Encryption**

  In order to encrypt a message $\mu \in R_p$ under a secret key $s \in R'$, sample an error term $e \in \mu + pR'$, a uniformly random element $c_1 \leftarrow R'_q$ and output $c(S) = (e - c_1 \cdot s) + c_1 \cdot S \in R'_q[S]$ with $k = 0$ and $l = 1$. Note that this particular form of $c(S)$ is called the LSD (Least Significant Digit) form. Formally, a ciphertext in LSD form satisfies

  $$\begin{aligned} c(s) &\equiv c_0 + c_1 s + \ldots + c_d s^d \equiv e \pmod{qR'} \\ &\text{for some sufficiently small error term } e \in R' \text{ such that} \\ e &\equiv l^{-1} \cdot g_{m'}^k \cdot \mu \pmod{pR'} \end{aligned}$$

  An alternate form that is more convenient for homomorphic operations is the MSD (Most Significant Digit) form defined by

  $$c(s) \approx \frac{q}{p} \cdot (l^{-1} \cdot g_{m'}^k \mu) \pmod{qR'}$$

  A ciphertext can be converted from LSD to MSD form and vice-versa in linear time.

- **Decryption**

  Decrypting the LSD-form ciphertext $c(S) \in R'_q[S]$ under the secret key $s \in R'$ involves evaluating $c(s) \in R'_q$ first and then lifting the result to R' in order to recover the error term $e \equiv l^{-1} \cdot g_{m'}^k \cdot \mu \pmod{pR'}$. Computing $l \cdot g_{m'}^{-k} \cdot e \pmod{pR'}$ yields the embedding of the message μ which is recovered in R_p by taking the twace [27].

- **Homomomorphic Addition and Multiplication**
  If k and l of two ciphertexts are the same, then the homomorphic addition simply involves converting both to the same form (LSD or MSD) and then adding their polynomials. If the k and l values are different, then they are adjusted as needed by multiplying the polynomial by an appropriate factor which only slightly increases the error.
  The more complicated operation is homomorphic multiplication. Consider two messages μ_1 and μ_2 encrypted as ciphertexts $c_1(S)$ and $c_2(S)$ in LSD form with auxiliary values k_1, l_1 and k_2, l_2 respectively. Recall that the LSD form of the ciphertexts are $c_1(s) = e_1 \pmod{qR'}$ and $c_2(s) = e_2 \pmod{qR'}$. Then the multiplication is performed as follows:

$$c_1(s) \cdot c_2(s) \cdot g'_m \equiv e_1 \cdot e_2 \cdot g'_m \pmod{qR'}$$

  We know $e_1 = l_1^{-1} \cdot g_m^{k_1} \cdot \mu_1$ and $e_2 = l_2^{-1} \cdot g_m^{k_2} \cdot \mu_2$, then

$$e_1 \cdot e_2 \cdot g'_m \equiv (l_1 l_2)^{-1} \cdot g_{m'}^{k_1+k_2+1} \cdot (\mu_1, \mu_2) \pmod{pR'}$$

  Since the error term $e = e_1 \cdot e_2 \cdot g_{m'}$ satisfies the invariant, we can conclude that the LSD-form resultant ciphertext is given by

$$c(S) = c_1(S) \cdot c_2(S) \cdot g_{m'} \in R'_q[S]$$

  In other words, $c(S)$ encrypts $\mu_1\mu_2 \in R_p$ with auxiliary values $k = k_1 + k_2 + 1$ and $l = l_1 l_2 \in \mathbb{Z}_p$.
  In order to handle the increase in the degree of the ciphertext polynomial with every homomorphic multiplication, a method called Key Switching is performed. This method allows us to convert the ciphertext under one secret key to another secret key (may or may not be different) while preserving the secrecy of the messages and the keys and also reducing the degree of the ciphertext, typically back to linear [27].

6.2 Efficiency of Cyclotomic Number Fields

As seen in the previous chapter, cyclotomic number fields offer very nice properties that help prove the pseudorandomness of the Ring-LWE distribution. In this section, we highlight the properties of cyclotomic number fields that make homomorphic multiplication more efficient. Keep in mind that although we may denote the ring of integers as R and the cyclotomic index as m for ease of notation, these properties are mainly pertaining to the cyclotomic index m' where $R' = \mathcal{O}_{m'}$, since R'_q is where all the operations on ciphertexts occur.

Tensor Product Representation. In Chapter 2.4 we learned about tensor products over R-modules. Since $K = \mathbb{Q}(\zeta_m)$ is a field extension of $\mathbb{Q}$, it behaves as a vector space over $\mathbb{Q}$. If $m = \prod_l m_l$ is the prime power decomposition of m, then

$$K \simeq \mathbb{Q}[X_1, X_2, \ldots]/(\Phi_{m_1}(X_1), \Phi_{m_2}(X_2), \ldots).$$

Extending Theorem 3.4.4 to l ideals $(\Phi_{m_l}(X_l))$, we have

$$\mathbb{Q}[X]/(\Phi_m(X)) \simeq \otimes_l \mathbb{Q}[X_l]/(\Phi_{m_l}(X_l)).$$

Equivalently we can write

$$K \simeq \otimes_l K_l.$$

This decomposition allows for efficient algorithms by modularly reducing operations in K to their prime-power-indexed cyclotomic counterparts in K_l. This method altogether avoids working with polynomials modulo $\Phi_m(X)$ which might lead to slower computations depending on m.

Choice of cipherspace modulus. Although [21] requires $q \equiv 1 \pmod{m}$ for proving the hardness of Ring-LWE, the pseudorandomness can now be shown for any q by using modulus switching techniques [26]. Thus this re-

striction is not imposed in the paper that describes efficient algorithms [20]. It is still desirable, however to choose prime $q \equiv 1 \pmod{m}$ in order to make operations more efficient. This is because for $q \equiv 1 \pmod{m}$ we know that $f(\mathfrak{q}/q) = 1$, and by Proposition 4.6.7 there are $\phi(m)$ primes of R lying over q. In other words

$$R/(q) \simeq \prod_{i \in \mathbb{Z}_m^*} (R/\mathfrak{q}_i)$$

where $\mathfrak{q}_i$'s are the prime ideals in R above q and $R = \mathcal{O}_m$. This special case supports efficient operations in R/qR.

Discrete Fourier Transform. In order to understand fast polynomial multiplication algorithms, we will use the concept of a Discrete Fourier Transform (DFT). For a commutative ring R and primitive mth root of unity ω,

Definition 6.2.1.

- *The R-linear map*

$$DFT_m : \begin{cases} R^m & \to R^m \\ f & \to (f(1), f(\omega), f(\omega), \ldots, f(\omega^{m-1})) \end{cases}$$

which evaluates a polynomial at the powers of ω is called the Discrete Fourier Transform (DFT_m). Here $f = \sum_{0 \le j < m} f_j x^j \in R[x]$ of degree less than n with its coefficient vector $(f_0, f_1, \ldots, f_{m-1}) \in R^m$.

- *The convolution of two polynomials $f = \sum_{0 \le j < m} f_j x^j$ and $g = \sum_{0 \le k < m} g_k x^k$ in $R[x]$ is the polynomial*

$$h = f *_m g = \sum_{0 \le l < m} h_l x^l \in R[x]$$

where

$$h_l = \sum_{j+k \equiv l \pmod{m}} f_j g_k = \sum_{0 \le j < m} f_j g_{l-j} \text{ for } 0 \le l < m$$

If we regard the coefficients as vectors in R^m then h is called the cyclic convolution of the vectors f and g.

This idea of convolution is equivalent to polynomial multiplication in the ring $R[x]/\langle x^n - 1\rangle$, and this relationship is exploited to obtain fast polynomial multiplication algorithms. The DFT is a special multipoint evaluation at the powers of $1, \omega, \omega^2, \ldots, \omega^{m-1}$. It can be shown that both the DFT and its inverse (the interpolation at the powers of ω_n) can be computed with $O(n \log n)$ operations in R, as opposed to the naive polynomial multiplication which is $O(n^2)$. An important algorithm that computes the DFT is the Fast Fourier Transform (FFT) [12].

Theorem 6.2.2. *Let R be a commutative ring which has a primitive nth root of unity where $n = 2^k$ for some $k \in \mathbb{N}$. Then convolution in $R[x]/\langle x^n - 1\rangle$ and multiplication of polynomials $f, g \in R[x]$ with $\deg(fg) < n$ can be performed using $3n \log n$ additions in R, $\frac{3}{2}n \log n + n - 2$ multiplications by powers of ω, n multiplications in R and n divisions by n, in total $\frac{9}{2}n \log n + O(n)$ arithmetic operations.*

The case where $m = 2^k$, such that $k \in \mathbb{N}$ is a special case. This is because using the FFT algorithm makes multiplication in R' significantly faster (Theorem 6.2.2). Note that even though in principle, all cases of m can be implemented in $O(n \log n)$, the generic algorithms that can achieve this have large constants hidden in the $O(\,\cdot\,)$ notation [20]. This special power-of-two case has been exploited by previous work done in this area [18]. In order to make efficient algorithms that perform polynomial multiplication in $O(n \log n)$ for any cyclotomic index, the tensor decomposition of DFT_m is taken advantage of:

$$DFT_m = \otimes_l DFT_{m_l}$$

Let m_l be a power of some prime p, using the Cooley-Tukey decompostion, DFT_{m_l} can be reduced to m_l/p parallel applications of DFT_p where each DFT_p takes $O(p \log p)$ time. The total runtime can be applied in $O(n \log n)$

time where $n = \phi(m)$.
In [20], the authors also use the definition of DFT_m to define the Chinese Remainder Transform (CRT_m) obtained by restricting the rows of DFT_m matrix to those indexed by $\mathbb{Z}_m^*$ and columns indexed by $[\phi(m)]$.

$$CRT_m = \otimes_l CRT_{m_l}$$

Applying this tensor decomposition reduces to $\phi(m/m_l)$ parallel applications of CRT_{m_l}. Each CRT_{m_l} can be done in $O(m_l \log m_l)$ time, thus making the total runtime $O(m \log m)$.

Powerful Basis. Recall from Theorem 3.2.10 that cyclotomic number fields are monogenic. This means that K has an integral basis of the form $\mathbf{p} = \{1, \zeta_m, \zeta_m^2, \ldots \zeta_m^{\phi(m)-1}\}$. $\mathbf{p}$ is often called the power basis of K. For prime power m, the power basis coincides with the definition of the powerful basis. For an arbitrary m having prime power factorization $m = \prod_l m_l$ the powerful basis is defined to be $\mathbf{p} = \otimes_l \mathbf{p}_l$ where $\mathbf{p}_l$ is the power basis of each $K_l = \mathbb{Q}(\zeta_{m_l})$. A strong property of the powerful basis is that its elements are close to orthogonal. This helps in making the algorithms that use Gram-Schmidt orthogonalization of the powerful basis for sampling from discrete Gaussians over R execute in substantially less time [20].

6.3 Experiments

Homomorphic multiplication has always been the crutch of homomorphic encryption schemes, since multiplying two ciphertexts increases the noise multiplicatively which gets out of hand after a certain level of mutliplicaitons, making it impossible to recover the original plaintext from the resulting ciphertext. Homomorphic addition on the other hand is not a big issue since the error terms grow at a smaller rate with each addition, and it is easy

to handle this error growth. This section describes the different experiments performed using the library for ring-based lattice cryptography ($\Lambda \circ \lambda$). The experiments test the performance of homomorphic multiplication by varying different parameters associated with this operation including the cyclotomic index m' and the cipherspace modulus q.

6.3.1 Criterion Package

The Criterion Package is used to benchmark the multiplication of two ciphertexts. Instead of recording the raw timings of each multiplication performed, this package gives an indication of *which* times occur more frequently. More specifically, it uses a boxplot technique to develop a quick sense of the quality of the timing data. One of the interesting features of this package is that Criterion figures out how many times it needs to evaluate a given function in order to get the most accurate performance measurements by characterizing the system's clock and figuring out how expensive it is to use the clock. Another important feature is its use of bootstrapping to perform some statistical analysis to report the mean and standard deviation of our data along with the 95% confidence intervals for those values. Most importantly, it reports outliers in our measurements and tells us whether they are relevant. In other words, when running performance benchmarks, if there are other processes running at the same time, these processes can affect the results of our benchmark. The bootstrap feature tells us whether our results are relatively accurate or completely insignificant.

6.3.2 Experiment One

The first experiment tests the performance of homomorphic multiplication when the cyclotomic index m' falls under three test cases - m' being prime, prime square and composite. Each test case has ten sample points which

are "comparable" in magnitude to the sample points in the corresponding test cases (see Table 6.1). The benchmark for homomorphic multiplication is run with the m' values given as below and fixed tensor RT, plaintext ring cyclotomic index $m = m'$ as well as plaintext ring modulus $p = 2$. The modulus for the ciphertext ring q is chosen by a function *goodQs* that takes a lower bound and m' and produces an infinite list of primes which satisfy $q \equiv 1 \pmod{m'}$. Because we are not concerned about the security in this experimentg, we set the lower bound to be m' as well.

	Primes	*Prime Squares*	*Composites*
1	47	$49{=}7^2$	$45 = 5 \cdot 3^2$
2	127	$121{=}11^2$	$125 = 5^3$
3	167	$169{=}13^2$	$171 = 3^2 \cdot 19$
4	293	$289 = 17^2$	$291 = 3 \cdot 97$
5	359	$361 = 19^2$	$365 = 5 \cdot 73$
6	523	$529 = 23^2$	$531 = 3^2 \cdot 59$
7	839	$841 = 29^2$	$845 = 5 \cdot 13^2$
8	967	$961 = 31^2$	$965 = 5 \cdot 193$
9	1367	$1369 = 37^2$	$1371 = 3 \cdot 457$
10	1693	$1681 = 41^2$	$1683 = 3^2 \cdot 11 \cdot 17$

Table 6.1: Sample values for m' in Experiment 1

Figure 6.1 shows that homomorphic multiplication where the cyclotomic index is a large prime takes much longer time than a prime square or a composite of comparable magnitude. Since the tensor decomposition of a prime m' is just R'_q itself, this means that polynomial multiplication is done naively $O(n^2)$, where $n = \phi(m')$, as opposed to the fast polynomial multiplication that is done when m' is a composite or a prime power. For the prime square and composite case, the library uses the tensor decomposition $R'_q \simeq \otimes_l \mathbb{Z}_q[\zeta_{m'_l}]$ where $m' = \prod_l m'_l$ to run parallel computations on its corresponding base rings, therefore making this operation more efficient.

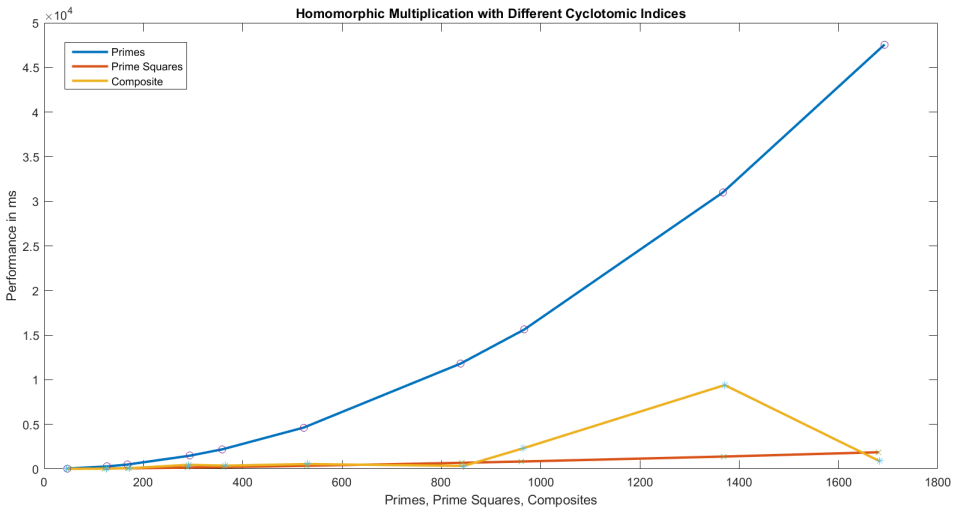

Figure 6.1: Experiment One Results

6.3.3 Experiment Two

Recall that when $m' = 2^k$ where k is a positive integer, the ability to compute polynomial multiplications using Fast Fourier Transforms makes the set-up very efficient. The homomorphic multiplication is thus tested on cases of m' where it is either a power of two or composite (See Table 6.2). Figure 6.2 shows that the performance of homomorphic multiplication increases linearly with increase in cyclotomic index for the power of two case. It also shows that the power of two case is on average faster than the composite case. This is because for the power of two case ($m' = 2^k$), the tensor decomposition of $R'_q \simeq \otimes \mathbb{Z}_q[\zeta_{2^k}]$, as opposed to the composite case ($m' = \prod_l m_l$) where $R'_q \simeq \otimes_l \mathbb{Z}_q[\zeta_{m_l}]$ and each m_l could be a power of 2 or a power of a prime that is greater than 2.

Notice that the performance is affected by both the size of each prime, say p_l where $p_l^{k_l} = m'_l$ and the magnitude of the power k_l where $m' = \prod_l m'_l$ in $R'_q \simeq \otimes_l \mathbb{Z}_q[\zeta_{m'_l}]$. In Experiment 1, consider line 10 of Table 6.1, although

	Power of Twos	*Composites*
1	$32{=}2^5$	$35 = 5 \cdot 7$
2	$64{=}2^6$	$62 = 31 \cdot 2$
3	$128{=}2^7$	$130 = 5 \cdot 13 \cdot 2$
4	$256 = 2^8$	$253 = 11 \cdot 23$
5	$512 = 2^9$	$518 = 2 \cdot 7 \cdot 37$
6	$1024 = 2^{10}$	$1025 = 5^2 \cdot 41$
7	$2048 = 2^{12}$	$2050 = 2 \cdot 5^2 \cdot 41$
8	$4096 = 2^{13}$	$4100 = 2^2 \cdot 5^2 \cdot 41$
9	$8192 = 2^{14}$	$8200 = 2^3 \cdot 5^2 \cdot 41$
10	$16384 = 2^{15}$	$16376 = 2^3 \cdot 23 \cdot 89$

Table 6.2: Sample values for m' in Experiment 2

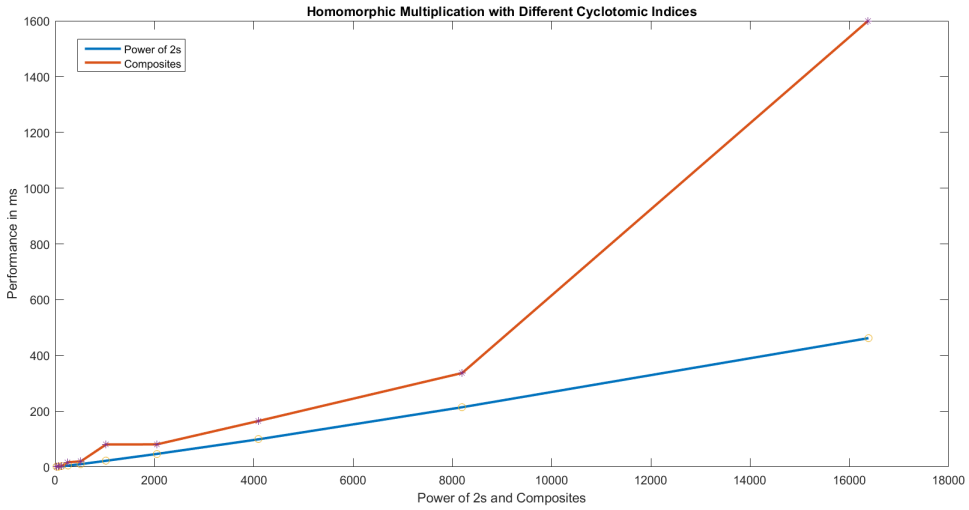

Figure 6.2: Experiment Two Results

$41^2 = 1681 < 1683 = 3^2 \cdot 11 \cdot 17$, the performance with the latter is better than the former (See Figure 6.1). A similar observation can be made about the 10th entry of Table 6.2, although $2^{13} \leq 16376 = 2^3 \cdot 23 \cdot 89 \leq 2^{15}$, we see that the performance of homomorphic multiplication with $m' = 16376$ is considerably higher than with $m' = 2^{15}$ (See Figure 6.2). These experimental

results indicate that the magnitude of the prime affects the performance more than the power of the prime. Theoretically, since each $CRT_{m'_l}$ can be done in $O(m'_l \log m'_l) = O(p_l^{k_l} \log p_l^{k_l}) = O(p_l^{k_l} \cdot k_l \log p_l)$, for cyclotomic indices of comparable magnitude, the trade-off is between the relatively bigger power k_l, but smaller $\log p_l$ of a smaller prime and the relatively smaller k_l, but bigger $\log p_l$ of a bigger prime.

6.3.4 Experiment Three

In order to ensure that the choice of the modulus q did not affect the performance of homomorphic multiplication, we ran an experiment in which we fixed the cyclotomic indices to be the power of two case as before (see Table 6.2) and varied q by using some of the elements of the potentially infinite list generated by the function *goodQs*, where our choice was $n = 1, 10, 50, 500$. Recall that given a lower bound and a cyclotomic index m, *goodQs* generates an infinite list of primes q above the lower bound which satisfy the condition $q \equiv 1 \pmod{m}$. Figure 6.3 shows that the change in q does not affect the performance of homomorphic multiplication significantly.

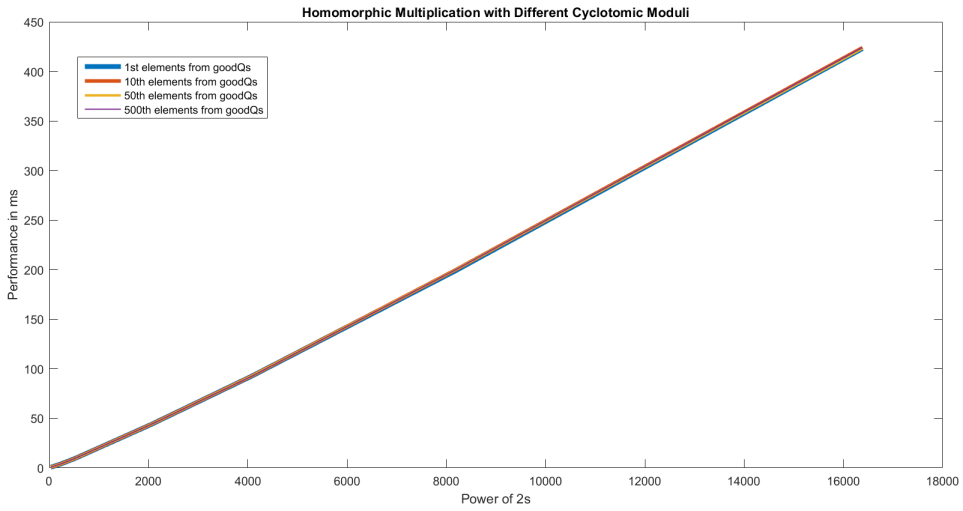

Figure 6.3: Experiment Three Results

Chapter 7

Conclusions

The main goal behind this work was to explore the mathematical properties offered by cyclotomic number fields that make them the ideal candidate for the underlying plaintextspace and ciphertextspace in current homomorphic encryption schemes. The main questions that we wanted to answer was - Why use cyclotomic number fields? How do they contribute to the efficiency of such schemes?

Although we have answered these questions to a certain extent, there is plenty more to investigate in this regard. From a theoretical standpoint, the use of Gaussian distributions and how they tie into the rest of the components can be explained in much more detail than in this work. From the efficiency standpoint, the performance of key-switching and ring tunneling needs to be investigated by varying the cyclotomic index and modulus.

There are two main factors that affect the performance of homomorphic multiplication when changing the underlying cyclotomic index m' of the ciphersapce ring R'_q - the magnitude of each prime and the power of the prime in the prime power of factorization of $m' = \prod_l m_l$. Our experiments indicate that the magnitude of the prime affects the performance more than the power of the prime in cyclotomic indices of comparable magnitude.

The homomorphic encryption scheme used in our experiments (from $\Lambda \circ \lambda$ library) is not recommended for use in production because it may be prone to timing or side-channel attacks. Although the library implements fast algorithms for sampling from Gaussian distributions as described by the literature, their current implementation is not very exact in terms of precision and the repercussions of this imprecision in terms of security is yet to be analyzed [8].

References

[1] Miklós Ajtai, *The shortest vector problem in l2 is np-hard for randomized reductions (extended abstract)*, Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '98, ACM, 1998, pp. 10–19.

[2] Saban Alaca and Kenneth S. Williams, *Introductory algebraic number theory*, Cambridge University Press, 2003, Cambridge Books Online.

[3] G. B. Arfken and H. J. Weber, *Gram-Schmidt Orthogonalization*, 6 ed., ch. 9.3, Academic Press, 2005.

[4] A. Blum, A.and Kalai and H. Wasserman, *Noise-tolerant learning, the parity problem, and the statistical query model*, Journal of the ACM (JACM) **50** (2003), no. 4, 506–519.

[5] Z. Brakerski and V. Vaikuntanathan, *Efficient Fully Homomorphic Encryption from (Standard) LWE*, SIAM Journal On Computing **43** (2014), no. 2, 831–871.

[6] Yuanmi Chen and Phong Q. Nguyen, *Bkz 2.0: Better Lattice Security Estimates*, Proceedings of the 17th International Conference on The Theory and Application of Cryptology and Information Security (Berlin, Heidelberg), ASIACRYPT'11, Springer-Verlag, 2011, pp. 1–20.

[7] D.A. Cox, *Galois theory*, Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts, Wiley, 2004.

[8] Eric Crockett and Chris Peikert, $\lambda \circ \lambda$*: A functional library for lattice cryptography*, Cryptology ePrint Archive, Report 2015/1134, 2015, `http://eprint.iacr.org/`.

[9] R. Dedekind, *Ueber den zusammenhang zwischen der theorie der ideale und der theorie der höheren congruenzen*, Abhandlungen der Königlichen Gesellschaft der Wissenschaften in Göttingen **23** (1878), 3–38.

[10] D.S. Dummit and R.M. Foote, *Abstract algebra*, Wiley, 2004.

[11] Yara Elias, Kristin E Lauter, Ekin Ozman, and Katherine E Stange, *Ring-lwe cryptography for the number theorist*, arXiv preprint arXiv:1508.01375 (2015).

[12] Joachim Von Zur Gathen and Jurgen Gerhard, *Modern computer algebra*, 2 ed., Cambridge University Press, New York, NY, USA, 2003.

[13] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan, *Trapdoors for Hard Lattices and New Cryptographic Constructions*, Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '08, ACM, 2008, pp. 197–206.

[14] O. Goldreich, D. Micciancio, S. Safra, and J. P. Seifert, *Approximating shortest lattice vectors is not harder than approximating closet lattice vectors*, Inf. Process. Lett. **71** (1999), no. 2, 55–61.

[15] Jeffrey Hoffstein, Jill C. Pipher, Joseph H. Silverman, and Inc ebrary, *An Introduction to Mathematical Cryptography*, Springer, New York;London;, 2008;2009;.

[16] Donald L. Kreher and Douglas Robert Stinson, *Combinatorial algorithms: generation, enumeration, and search*, CRC Press, 1999.

[17] S. Lang, *Algebraic number theory*, Applied Mathematical Sciences, Springer, 1994.

[18] Kristin Lauter, Michael Naehrig, and Vinod Vaikuntanathan, *Can homomorphic encryption be practical?*, Tech. Report MSR-TR-2011-61, May 2011.

[19] A. K. Lenstra and H. W. Lenstra, *Factoring polynomials with rational coefficients*, Muth. Ann (1982), 515–534.

[20] Vadim Lyubashevsky, Chris Peikert, and Oded Regev, *Advances in cryptology – eurocrypt 2013: 32nd annual international conference on the theory and applications of cryptographic techniques, athens, greece, may 26-30, 2013. proceedings*, ch. A Toolkit for Ring-LWE Cryptography, pp. 35–54, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[21] Vadim Lyubashevsky, Chris Peikert, and Oded Regev, *On Ideal Lattices and Learning with Errors over Rings*, Journal of the ACM (JACM) **60** (2013), no. 6, 1–35.

[22] Henry B. Mann, *Introduction to algebraic number theory. with a chapter by Marshall Hall, Jr*, Ohio State University Press, 1955.

[23] Daniele Micciancio, *The shortest vector problem is NP-hard to approximate to within some constant*, SIAM Journal on Computing **30** (2001), no. 6, 2008–2035, Preliminary version in FOCS 1998.

[24] Daniele Micciancio and Shafi Goldwasser, *Complexity of lattice problems, a cryptographic perspective*, Springer, 2002.

[25] Jürgen Neukirch, *Algebraic Number Theory*, Springer, 1999.

[26] C. Peikert, *Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem*, Proc. 41st ACM Symp. on Theory of Computing (STOC) (2009), 333–342.

[27] Chris Peikert, *A decade of lattice cryptography*, Cryptology ePrint Archive, Report 2015/939, 2015.

[28] O. Regev, *On Lattices, Learning with Errors, Random Linear Codes, and Cryptography*, Journal of the ACM (JACM) **56** (2009), no. 6, 1–40.

[29] ———, *The Learning with Errors Problem (Invited Survey)*, 2010, pp. 191–204.

[30] William Stein, *Algebraic number theory. a computational approach.*

[31] I. Stewart, *Galois theory, third edition*, Chapman Hall/CRC Mathematics Series, Taylor & Francis, 2003.

[32] Tom Weston, *Algebraic number theory*, 1999.