Enhancing Ring-LWE Hardness using Dedekind Index Theorem

Charanjit S. Jutla[1] and Chengyu Lin[2] *

[1] IBM T. J. Watson Research Center
[2] Columbia University

Abstract. In this work we extend the known pseudorandomness of Ring-LWE (RLWE) to be based on ideal lattices of non Dedekind domains. In earlier works of Lyubashevsky et al (EUROCRYPT 2010) and Peikert et al (STOC 2017), the hardness of RLWE was based on ideal lattices of ring of integers of number fields, which are known to be Dedekind domains. While these works extended Regev's (STOC 2005) quantum polynomial-time reduction for LWE, thus allowing more efficient and more structured cryptosystems, the additional algebraic structure of ideals of Dedekind domains leaves open the possibility that such ideal lattices are not as hard as general lattices.

We now show that for any number field $\mathbb{Q}[X]/(f(X))$, for all prime integers p such that the factorization of $f(X)$ modulo p passes the Dedekind index theorem criterion, which is the case for almost all p, we can base p-power RLWE in the polynomial ring $\mathbb{Z}[X]/(f(X))$ itself and its hardness on worst-case hard problems of ideal lattices of this ring. This ring can potentially be a strict sub-ring of the ring of integers of the field, and hence not be a Dedekind domain. We also give natural examples and prove that certain ideals require at least three generators, as opposed to two sufficient for Dedekind domains. Such rings also do not satisfy many other algebraic properties of Dedekind domains such as ideal invertibility. Our proof technique is novel as it builds a self-contained algebraic theory for general such rings that also works for cyclotomic q-RLWE, for every q.

1 Introduction

In a ground-breaking work, Regev [Reg05] showed a (quantum) polynomial-time reduction from worst-case lattice problems to a learning problem called *learning with error* (LWE). He also obtained public-key cryptosystems using LWE whose security is then based on worst-case lattice problems such as closest vector problem (CVP) and shortest independent vectors problem (SIVP). The fact that that there are no known efficient quantum algorithms for these hard problems, makes this approach to obtaining encryption schemes even more significant, and has led to numerous applications in cryptography.

* Part of this work was done when the author was a summer intern at IBM T. J. Watson Research Center.

As a more efficient variant of LWE, Lyubashevsky *et al.* introduced the Ring Learning With Errors problem (RLWE) [LPR10] over the ring of integers $\mathcal{O}_{\mathbf{K}}$ of a number field $\mathbf{K}$. The hardness of RLWE is then based on lattice problems restricted to ideal lattices in the ring $\mathcal{O}_K$, instead of general integer lattices. Since addition and multiplication in the ring of integers can be viewed as polynomial addition and multiplication, it allows for more efficient cryptosystems, with almost a quadratic improvement in the security parameter. Additionally, it has allowed for a more sound security setting for many (fully) homomorphic encryption schemes [Gen09], where the ring structure naturally allows for homomorphic ring-operations [BGV12,Bra12,FV12,GSW13,DM15,CGGI16,CKKS17]. For conjectured hardness of RLWE, [LPR10] provide a quantum polynomial-time reduction from the (seemingly) hard Approximate Shortest Independent Vectors Problem (ApproxSIVP) over ideal lattices. While the original [LPR10] reduction, especially for the decisional version of RLWE, was restricted to cyclotomic number fields, in another technical tour-de-force work [PRS17] extend the hardness of decisional-RLWE to arbitrary number fields $\mathbf{K}$, basing the hardness on worst-case lattice problems restricted to ideal lattices in $\mathcal{O}_{\mathbf{K}}$.

Since the ring of integers of a number field enjoy remarkable algebraic properties, namely that such rings are Dedekind domains, and all ideals in the rings are invertible and have a unique prime ideal factorization, the question naturally arises if the normally hard lattice problems may be at a risk of being weaker due to the additional algebraic structure. In particular, while all ideal lattices are also full-ranked over the integers $\mathbb{Z}$, and of the same rank as the rank of the number field $\mathbf{K}$ as an extension of $\mathbb{Q}$, every ideal of a Dedekind domain can be generated by only two elements of the domain. Moreover, one of the generators can be taken to be just the integer that is the norm of the ideal. In light of this, it is natural to ask if the class of lattices can be expanded to a class having lesser algebraic properties and still basing a polynomial algebra cryptosystem on these lattices. Ideally, one would like to base the hardness of RLWE on worst-case general integer lattices as is the case for LWE.

In this work, we show that one can base hardness of decisional-RLWE on ideal lattice problems in non Dedekind domains. In particular, instead of setting the RLWE instance in the ring of integers $\mathcal{O}_{\mathbf{K}}$ of a number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$, we set our RLWE instances in the polynomial ring $\mathcal{R}_{\mathbf{K}} = \mathbb{Z}[X]/(f(X))$, which is anyway easier to work with from a cryptosystem perspective; the ring $\mathcal{O}_{\mathbf{K}}$ can have polynomials with rational coefficients and is a super-ring of $\mathcal{R}_{\mathbf{K}}$. We then show that, for all q that are not divisible by a small number of excluded primes, the q-RLWE instances are as hard as the worst-case lattice problems, such as CVP and SIVP, of ideal lattices of this non Dedekind domain. These (finitely many) excluded primes are the primes p such that p divides $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}]$, i.e. the index of $\mathcal{R}_{\mathbf{K}}$ in the ring of integers of $\mathbf{K}$. We obtain exactly the same security and noise parameters as [PRS17], and most of our reduction uses the main technical lemmas from [PRS17], but replaces the so called “ideal clearing lemma” of [LPR10] with a new proof that does not use properties of Dedekind domains. The main technical contribution of this paper is developing a theory for such non Dedekind domains which allow us to prove the ideal clearing lemma in a novel way. The ideal clearing lemma also guarantees an efficient mapping that can take an arbitrary basis of an ideal as input. We give a new randomized algorithm to obtain this mapping which completely bypasses the usual prime ideal factorization technique of [LPR10]. In this respect, our technique and novel randomized algorithm are also applicable to number fields where $\mathcal{O}_{\mathbf{K}}$ is same as $\mathcal{R}_{\mathbf{K}}$, for example the popular cyclotomic number fields.

It is worth remarking that for every number field $\mathbf{K}$, there is a finite number m (namely, $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}]$) such that every ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbf{K}}$ can be scaled by m, so that $m \cdot \mathcal{I}$ is an ideal of $\mathcal{R}_{\mathbf{K}}$. Thus, the ideals (and corresponding lattices) in $\mathcal{R}_{\mathbf{K}}$ include all hard ideal lattices coming from $\mathcal{O}_{\mathbf{K}}$. However, we show later that the reverse is not true. In the following, when it is clear from context, we will drop the subscript $\mathbf{K}$ from $\mathcal{R}_{\mathbf{K}}$.

Dedekind Index Theorem. We now specify the good primes p (i.e. excluding a few bad primes) for each number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$, for which we can get a reduction from worst-case ideal lattice problems of the polynomial ring to the p-power RLWE instances. A hint comes from one of the many celebrated theorems of Dedekind which gives an easy necessary and sufficient test of when a prime p *does not* divide the index of $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ as a subgroup of $\mathcal{O}_{\mathbf{K}}$. The test involves checking the factorization of $f(X)$ modulo p into irreducible polynomials (modulo p) for a specific property, which we will describe later. If p does not divide this index, then another theorem of Dedekind shows that the prime ideal factorization of ideal (p) of $\mathcal{O}_{\mathbf{K}}$ can be read off from the the factorization of $f(X)$ modulo p. We show in this work that in this case the ideal (p) of $\mathcal{R}$ also factors into prime ideals of $\mathcal{R}$, i.e. (p) is well-behaved even in $\mathcal{R}$. We will refer to these as the good primes. However, if some other prime p' fails the test, and hence $p' | [\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$, then $\mathcal{R}$ is a strict sub-ring of $\mathcal{O}_{\mathbf{K}}$, and is then definitely not a Dedekind domain. We will refer to these p' as the bad primes. It is well known that a prime p' can divide $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$ only if ${p'}^2$ divides the discriminant of the field $\mathbf{K}$, and hence the number of bad p' are already restricted to being factors of the discriminant, and hence are finite in number and usually few. Thus, the trick is to find a p for which the factorization of (p) is well-behaved and another p' which is bad (so that we are guaranteed a non Dedekind domain). Then the RLWE can be set modulo any power of p in the non Dedekind domain $\mathcal{R}$, and the hardness reduction will still go through. In fact, one can set RLWE modulo any q whose prime factors exclude the small number of bad p'.

Example. Consider the polynomial $f(X) = X^{3^n} + 26$. By Eisenstein criterion, $f(X)$ is irreducible over $\mathbb{Q}$, and thus $\mathbb{Q}[X]/(f(X))$ is a number field. Consider the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$. The discriminant of $f(X)$ is just the determinant of the multiplication matrix of $f'(X) = 3^n X^{3^n - 1}$, and a little calculation shows that only $3, 13$ and 2 can divide the discriminant, and hence are the only possible bad candidates for the Dedekind index test. The factorization of $f(X)$ modulo 2 is just X^{3^n}, and hence has only one irreducible polynomial, i.e. X, as a factor with multiplicity 3^n. Any factor that has multiplicity more than one is said to ramify (mod 2), and factors that have multiplicity one are called unramified. Now, write $f(X)$ as $X^{3^n} + 2 \cdot t(X)$, and note that $t(X)$ is just the trivial polynomial 13. The Dedekind index theorem says that $t(X)$ is divisible by a ramified factor (modulo 2), in this case the factor X, *iff* 2 divides $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$. In this case, X does not divide 13 mod 2, and hence 2 does not divide $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$, and 2 is a good prime. Hence we can base our RLWE modulo any power of two, and still be assured hardness based on worst case ideal lattices in $\mathcal{R}$. Now, let's check that 3 divides the index, so that $\mathcal{R}$ is a strict sub-ring of $\mathcal{O}_{\mathbf{K}}$. The factorization of $f(X)$ modulo 3 is $X^{3^n} - 1 = (X-1)^{3^n}$. Thus, $(X-1)$ is the only factor and it is ramified. Writing $f(X)$ as $f(X) = (X-1)^{3^n} + 3 \cdot t(X)$, we find that $t(X)$ is divisible by ramified $(X-1)$ modulo 3. Thus, by Dedekind Index theorem 3 divides $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$ and hence $\mathcal{R}$ is not a Dedekind domain. We give more examples in Section 6, where we also prove that some ideal requires at least three generators.

One may wonder that since the number of bad p' is small, it maybe the case that only a few ideals are lacking algebraic structure (i.e. of the Dedekind domain kind). While it is true that there are only a few *prime* ideals lacking algebraic structure, the number of non-prime ideals contained in these prime ideals is unlimited, and are hidden as usual by giving a bad basis of the ideal. Another important point to be raised is if one can demonstrate that non-trivial ideals in such non Dedekind domains require more than two generators. In this work, we also prove that there are non-trivial ideals, i.e. which do not have a diagonal Hermite normal form, for which at least three generators are required, and which cannot be scaled by a rational number to become an ideal of $\mathcal{O}_{\mathbf{K}}$.

On Clearing the Ideal. As mentioned earlier, one of the main technical challenges in the hardness reduction, starting from Regev's LWE reduction, is setting up a q-RLWE instance which is somehow not dependent on the worst-case lattice instance, especially given only some basis $\boldsymbol{B}(\mathcal{L})$ of the lattice $\mathcal{L}$. While in the LWE instance, since the multiplication in LWE is just inner product, it is compatible with the lattice and the dual lattice clearing each other out, and the issue of inverting the lattice-basis modulo q does not come up. In the case of RLWE, since it is more "efficient", the multiplication in RLWE is not the trace-product, but polynomial multiplication. Thus, it is not enough that a lattice $\mathcal{L}$ and its dual lattice $\mathcal{L}^\vee$ have the property that $\mathcal{L}^\top \mathcal{L}^\vee = I$. To solve this problem, the ideal clearing lemma of [LPR10] obtains an efficiently invertible (module-) isomorphism between $\mathcal{I}/q\mathcal{I}$ and the whole polynomial ring[3] modulo q, for any ideal $\mathcal{I}$. This isomorphism is not easy to obtain as lattice corresponding to $\mathcal{I}$ may not be invertible modulo q, and in fact (q) as an ideal may have additional factorization into prime ideals. Nevertheless, an efficient isomorphism is obtained by computing prime ideal factorization or effectively inverting the ideal $\mathcal{I}$ itself (instead of inverting its lattice-basis).

In our case, i.e. where $\mathcal{R}$ is a non Dedekind domain, the ideal $\mathcal{I}$ may not be invertible. However, we prove a more general clearing lemma that suffices

[3] More precisely, $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$, for general fields

for the reduction, and only requires that $\mathcal{I}$ be a principal ideal modulo $q\mathcal{I}$. Note, principal ideals are trivially invertible, as their $\mathbb{Z}$-basis is their (circulant) multiplication matrix. This approach can also be taken for Dedekind domains, as it is well known that Dedekind domains modulo any ideal are principal ideal domains. However, we show that even though our ring $\mathcal{R}$ may not be a Dedekind domain, for any prime p, such that p is good with respect to the Dedekind index theorem, $\mathcal{R}/p^r\mathcal{R}$ is a principal ideal domain, for any positive integer r. Further, we show that for any ideal $\mathcal{I}$, $\mathcal{I}$ is principal modulo $p^r\mathcal{I}$. Using Chinese Remainder theorem, the result can then be extended to any q that is product of powers of good primes. We also give a highly efficient randomized algorithm to find a generator for the above mentioned principal ideals, which essentially takes a random $\mathcal{R}/p\mathcal{R}$-linear combination of the columns of the $\mathbb{Z}$-basis of the ideal $\mathcal{I}$.

On Cyclotomic Rings. As mentioned earlier, it is well-known that for cyclotomic fields $\mathbf{K}$, the ring of integers $\mathcal{O}_{\mathbf{K}}$ is same as the polynomial ring $\mathcal{R}_{\mathbf{K}}$. A proof of this fact using the Dedekind index theorem can be found in Appendix C. This also means that every prime p is good with respect to the cyclotomic polynomials, since $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}_{\mathbf{K}}] = 1$. Thus, our theory and reduction applies with respect to every integer q in showing hardness of q-RLWE. Hence this gives an alternate proof of hardness of q-RLWE for cyclotomic rings, i.e. as far as clearing the ideal is concerned and also efficiently obtaining the invertible isomorphisms required by the clearing lemma. In fact, this makes our reduction computationally more efficient.

Since our proofs are elementary, requiring only basic knowledge of ideals, another contribution of the paper can be seen as obtaining the clearing lemma by elementary means and not employing the Dedekind domain prime ideal factorization theory. We remark that our proof does not employ the Dedekind index theorem, but the proofs and the setting are inspired by the theorem. We also employ the index theorem to give example fields and underlying polynomial rings. Another interesting feature of our reduction is that it does not require a known factorization of modulus q of RLWE, whereas [LPR10] requires a known factorization of q in order to do prime ideal factorization of the integer prime factors of q. Finally, the algebraic theory we build in this work does not require $f(X)$ to be irreducible over $\mathbb{Q}$, but merely that $f(X)$ has distinct complex roots.

Related Work. In [BBPS19], a generalization of the RLWE problem is described, wherein the ambient ring is not the ring of integers of a number field, but rather an order (i.e. a full-ranked sub-ring). They show that this Order-LWE problem enjoys worst-case hardness with respect to short-vector problems of *invertible*-ideal lattices of the order, which naturally are also known to follow prime ideal factorization and other good properties of Dedekind domain ideals (see e.g. [Cona, Theorem 6.1]). This is in contrast to our result where we show worst-case hardness with respect to all ideal lattices of the non-maximal order.

In [RSW18], a reduction from decision (resp. search) RLWE in $\mathbf{K} = \mathbb{Q}[X]/(f(X))$ to decision (resp. search) polynomial-LWE [SSTX09] (i.e. with the ring $\mathcal{R} = \mathbb{Z}[X]/\ (f(X)))$ is obtained, Since, the hardness of RLWE in $\mathbf{K} = \mathbb{Q}[X]/(f(X))$ was only known based on hardness of ideals in $\mathcal{O}_{\mathbf{K}}$, this result only ties the hardness of polynomial-LWE to hardness of Dedekind-domain ideal lattices.

Outline. The rest of the paper is organized as follows. Section 2 covers preliminaries of lattices, smoothing lemma, and hard problems over lattices. Section 3 covers basics of ideals and states the Dedekind Index theorem. Section 4 introduces the polynomial ring calculus including dual ideals and dual rings. Section 5 introduces the notion of Dedekind-special primes w.r.t. a separable polynomial which sets up the primes p for each number field for which our reduction works. The section also proves that ideal $\mathfrak{a}$ is principal modulo $p^r\mathfrak{a}$. Section 6 gives examples and gives a novel proof that certain ideals require at least three generators. Section 7 gives a novel randomized algorithm to find a generator for above principal ideal. Section 8 proves the pseudo-randomness of q-RLWE using earlier works and the novel formulation of the clearing lemma and its proof using the theory and algorithms developed in earlier sections. We also give and prove our version of the clearing lemma for ring of integers of arbitrary number fields.

2 Preliminaries

We'll be working with the polynomial rings modulo a monic polynomial $f(X) \in \mathbb{Z}[X]$ of degree n whose (complex) roots are distinct. Each ring element is a polynomial $g(X) = \sum_{i=0}^{n-1} g_i X^i$ of degree less than n, which can be viewed as a length-n (column) vector of its coefficients $(g_0, \ldots, g_{n-1})$. We will denote this vector by boldface g, i.e. $\mathbf{g}$, and we will use this as a general notational principle. More formally, we define a mapping φ from the polynomials to its coefficient representation, i.e. $\varphi(g(X)) = \mathbf{g}$, and it has an inverse $\varphi^{-1}(\mathbf{g}) = g(X)$.

In particular, we are interested in the following three rings: the integer polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, its modulo q version $\mathcal{R}_q = \mathbb{Z}_q[X]/(f(X))$ for some $q \in \mathbb{Z}$, and the rational polynomial ring $\mathcal{R}_{\mathbb{Q}} = \mathbb{Q}[X]/(f(X))$.

For clarity, we use operator "$*$" for polynomial multiplication in $\mathbb{Z}[X]$ or quotient rings such as $\mathbb{Z}[X]/(f(X))$, operator "$\cdot$" for scalar multiplication, operator "$\times$" for matrix (vector) multiplication and cartesian product.

2.1 The Canonical Space $\mathcal{H}$ and Lattices

The ring $\mathcal{R}_{\mathbb{Q}}$ is definitely a $\mathbb{Q}$-algebra, and a (possibly degenerate) extension of the field $\mathbb{Q}$. Since, $\mathbb{C}$ is the completion of algebraic closure of $\mathbb{Q}$, $\mathcal{R}_{\mathbb{Q}}$ naturally embeds in $\mathbb{C}$, with $\mathbb{Q} \subseteq \mathcal{R}_{\mathbb{Q}}$ embedding identically in $\mathbb{C}$. However, there are n such distinct embeddings in $\mathbb{C}$. These n embeddings are automorphic (i.e. automorphisms of the image of $\mathcal{R}_{\mathbb{Q}}$ in C) if $\mathcal{R}_{\mathbb{Q}}$ is a Galois field extension. However, in our general case, we will get n embeddings which are not necessarily automorphic. The n embeddings viewed together can be seen as mapping to the following space $\mathcal{H}$, which we will refer to as the *canonical embedding* in the general case, i.e. whether $\mathcal{R}_{\mathbb{Q}}$ is a Galois extension or not even a field extension.

The canonical space $\mathcal{H}$ is defined as follow where $s_1 + 2s_2 = n$:

$$\mathcal{H} = \left\{ (x_0, \ldots, x_{n-1}) \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} \middle| \forall i \in [s_2] : x_{s_1+i} = \overline{x_{s_1+s_2+i}} \right\} \subseteq \mathbb{C}^n$$

We then describe the canonical embedding from the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ to this space $\mathcal{H}$ given by a matrix.

Vandermonde Matrix and Discriminant Let the n distinct roots of $f(X)$ be $(z_0, \ldots, z_{n-1})$. Note the complex roots of $f(X)$ come in conjugate pairs, because for integer polynomial, $f(\bar{z}) = \overline{f(z)}$. We can order the roots such that $z_i \in \mathbb{R}$ for $i \in [s_1]$ and $z_{s_1+i} = \overline{z_{s_1+s_2+i}}$ for $i \in [s_2]$, where $s_1 + 2s_2 = n$.

The (square) *Vandermonde matrix* $\boldsymbol{V}$ of the roots of $f(X)$ is given by

$$\boldsymbol{V} = \begin{bmatrix} 1 & z_0 & z_0^2 & \cdots & z_0^{n-1} \\ 1 & z_1 & z_1^2 & \cdots & z_1^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & z_{n-1} & z_{n-1}^2 & \cdots & z_{n-1}^{n-1} \end{bmatrix}$$

whose determinant is $\det(\boldsymbol{V}) = \prod_{0 \le i < j < n}(z_j - z_i)$. Because all roots are distinct, $\det(\boldsymbol{V}) \neq 0$ and hence $\boldsymbol{V}$ is invertible. We will abuse notation, and call the Vandermonde matrix of z_i's, to be also the Vandermonde matrix of $f(X)$.

The **discriminant** Δ_f of a polynomial is defined to be the square of the determinant of the Vandermonde matrix of $f(X)$. In corollary 4.9 we will relate the discriminant to the determinant of the multiplication matrix (in $\mathbb{Q}[X]/(f(X))$) of the derivative of $f(X)$.

Given a polynomial $g(X) \in \mathcal{R}_{\mathbb{Q}}$ and its vector representation $\mathbf{g} \in \mathbb{Q}^n$, we have $(1, z, z^2, \ldots, z^{n-1})^\top \times \mathbf{g} = g(z)$. The product of $\boldsymbol{V}$ and $\mathbf{g}$ is essentially the evaluation of polynomial $g(X)$ at roots of $f(X)$: $(g(z_0), g(z_1), \ldots, g(z_{n-1})) \in \mathcal{H}$. Therefore, the Vandermonde matrix $\boldsymbol{V}$ of $f(X)$ canonically embeds the polynomial in $\mathcal{R}_{\mathbb{Q}}$ into the canonical space $\mathcal{H}$: first view the polynomial as vector of coefficients over $\mathbb{Q}$ ($\subseteq \mathbb{R} \subseteq \mathbb{C}$). The first s_1 rows of $\boldsymbol{V}$ maps this vector into $\mathbb{R}^{s_1}$, and the remaining rows of $\boldsymbol{V}$ maps this vector into $\mathbb{C}^{2s_2}$, with conjugate pairs. Note that $\boldsymbol{V}(\mathbf{g} * \mathbf{h})$ is same as point-wise product of $\boldsymbol{V}\mathbf{g}$ and $\boldsymbol{V}\mathbf{h}$, for any polynomials $\mathbf{g}$ and $\mathbf{h}$.

Lattice The lattice $\mathcal{L}$ is defined as an additive subgroup of $\mathcal{H}$ given by a set of basis vectors $\{\mathbf{b_0}, \ldots, \mathbf{b_{m-1}}\}$ from $\mathcal{H}$:

$$\mathcal{L} = \left\{ \sum_{i=0}^{m-1} z_i \cdot \mathbf{b_i} \middle| (z_0, \ldots, z_{n-1}) \in \mathbb{Z}^n \right\}.$$

It's dual is defined as $\mathcal{L}^\vee = \left\{ \mathbf{y} \in \mathcal{H} \middle| \forall \mathbf{x} \in \mathcal{L} : \langle \mathbf{y}, \mathbf{x} \rangle = \mathbf{y}^H \mathbf{x} \in \mathbb{Z} \right\}$. Here $(\cdot)^H$ denotes the Hermitian (conjugate) transpose. It's easy to verify that $(\mathcal{L}^\vee)^\vee = \mathcal{L}$.

The minimum distance of a lattice is defined as the length of the shortest non-zero lattice vector: $\lambda_1(\mathcal{L}) = \min_{\mathbf{0} \neq \mathbf{x} \in \mathcal{L}} \{\|\mathbf{x}\|\}$.

Gaussians Define $G = \left\{ \mathbf{r} \in \mathbb{R}_+^n \middle| \mathbf{r}_{s_1+i} = \mathbf{r}_{s_1+s_2+i}, 0 \leq i < s_1 \right\}$. For any $\mathbf{r} \in G$, the *elliptical Gaussian distribution* $D_{\mathbf{r}}$ over the space $\mathcal{H}$ is defined to have a probability density function proportional to $\rho_{\mathbf{r}}(\mathbf{x}) = \exp\left(-\sum_{i=0}^{n-1} |\mathbf{x}_i/\mathbf{r}_i|^2\right)$. For real $r > 0$, We also define the spherical Gaussian distribution D_r as $D_{r\cdot\mathbf{1}}$.

Definition 2.1 (Smoothing Condition). *For any lattice $\mathcal{L} \subset \mathcal{H}$, a positive real $\epsilon > 0$ and $\mathbf{r} \in G$, we say $\mathbf{r} \geq \eta_\epsilon(\mathcal{L})$ if $\rho_{1/\mathbf{r}}(\mathcal{L}^\vee \backslash \{0\}) \leq \epsilon$ where $1/\mathbf{r} = (1/r_0, 1/r_1, \ldots, 1/r_{n-1})$.*

Lemma 2.1 ([MR07,PRS17]). (**Smoothing Lemma**) *For any lattice $\mathcal{L} \subset \mathcal{H}$, $\epsilon > 0$ and $\mathbf{r} \geq \eta_\epsilon(\mathcal{L})$. the statistical distance between $(D_{\mathbf{r}} \bmod \mathcal{L})$ and the uniform distribution over $\mathcal{H}/\mathcal{L}$ is at most 2ϵ.*

Lemma 2.2 ([MR07]). *For any lattice $\mathcal{L} \subset \mathcal{H}$ and $c \geq 1$, we have $c\sqrt{n}/\lambda_1(\mathcal{L}^\vee) \geq \eta_\epsilon(\mathcal{L})$ where $\epsilon = \exp(-c^2 n)$.*

Proposition 2.3 ([MR07]). *For any lattice $\mathcal{L} \subset \mathcal{H}$ and $\epsilon \in (0,1)$, we have $\eta_\epsilon(\mathcal{L}) \geq \sqrt{\frac{\log(1/\epsilon)}{\pi}}/\lambda_1(\mathcal{L}^\vee)$.*

For a lattice $\mathcal{L} \subset \mathcal{H}$ and $\mathbf{r} \in G$, the *discrete Gaussian* distribution $D_{\mathcal{L},\mathbf{r}}$ is defined to have support $\mathcal{L}$ and mass function $D_{\mathcal{L},\mathbf{r}}(\mathbf{x}) = \rho_{\mathbf{r}}(\mathbf{x})/\rho_{\mathbf{r}}(\mathcal{L})$ for $\mathbf{x} \in \mathcal{L}$.

2.2 Lattice Problems

We introduce the following (seemingly hard) lattice problems.

Definition 2.2 (SVP and SIVP). *On the canonical space $\mathcal{H}$ endowed with some geometric norm (such as the ℓ_2 norm), let $\gamma > 1$, given a lattice $\mathcal{L}$, the* Shortest Vector Problem *SVP$_\gamma$ asks for an element $\mathbf{x} \in \mathcal{L}$ such that $\|\mathbf{x}\| \leq \gamma \cdot \lambda_1(\mathcal{L})$, and the* Shortest Independent Vectors Problem *SIVP$_\gamma$ asks for n linearly independent elements in $\mathcal{L}$ whose norms are at most $\gamma \cdot \lambda_n(\mathcal{L})$.*

Definition 2.3 (DGS). *Let $\gamma > 0$. The* Discrete Gaussian Sampling problem *DGS$_\gamma$ is, given a lattice $\mathcal{L} \subseteq \mathcal{H}$ and $r \geq \gamma$, output samples from the distribution $D_{\mathcal{L},r}$.*

More specifically, in this work, we consider the above problems restricted to the *ideal lattices*, when lattices are generated by ideals of the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$. See section 4.2.

Definition 2.4 (GDP). *For a lattice $\mathcal{L} \subseteq \mathcal{H}$, the* Gaussian Decoding Problem *GDP$_{\mathcal{L},r}$ asks, given a coset $\mathbf{e} + \mathcal{L}$ where $\mathbf{e} \in \mathcal{H}$ is sampled from Gaussian D_r, find $\mathbf{e}$.*

3 Ideal Basics

Let R be any commutative ring with unity. An (integral) *ideal* $\mathfrak{a} \subseteq R$ is an additive subgroup that is closed under multiplication by the elements from R. A fractional ideal $\mathfrak{a}$ is a subset of R, such that there exists an element $r \in R$ that makes $r \cdot \mathfrak{a}$ an integral ideal of R. An ideal $\mathfrak{a}$ generated by finitely many $g_1, g_2, ...g_k$ is denoted by $(g_1, g_2, ..., g_k)$. Note, $(1) = R$. A **prime ideal** of a ring R is an ideal $\mathfrak{p}$ such that $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. A **maximal ideal** of a ring R is a non-trivial ideal (i.e. not same as R) that is maximal under the subset relation. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called **co-prime** if $\mathfrak{a} + \mathfrak{b} = (1)$. An element $c \in R$ will be called **invertible modulo an ideal** $\mathfrak{a}$ if there exists a $\mu \in R$ and $\lambda \in \mathfrak{a}$ such that $\mu c = 1 + \lambda$. In other words, c is a **unit** of quotient ring $R/\mathfrak{a}$. We now enumerate a list of well-known facts about ideals, which also have elementary proofs (see e.g. [AM69] or [Cla84] for proofs, if not provided in the appendix A).

Lemma 3.1. (i) *If a prime ideal $\mathfrak{p}$ contains product of two ideal $\mathfrak{a}\mathfrak{b}$, then at least one of $\mathfrak{a}$ or $\mathfrak{b}$ is in $\mathfrak{p}$.*

(ii) *If an ideal $\mathfrak{a}$ is co-prime to two ideals, say $\mathfrak{b}$ and $\mathfrak{c}$, then $\mathfrak{a}$ is co-prime to $\mathfrak{b}\mathfrak{c}$.*

(iii) *If ideals $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime, then for any positive integers r, s, their powers $\mathfrak{a}^r$ and $\mathfrak{b}^s$ are also co-prime.*

(iv) *If a maximal ideal $\mathfrak{m}$ contains product of powers of distinct maximal ideals $\mathfrak{n}_1, ..., \mathfrak{n}_k$, then $\mathfrak{m}$ must be one of $\mathfrak{n}_1, ..., \mathfrak{n}_k$.*

Lemma 3.2. *For any ring R, and any maximal ideal $\mathfrak{a} = (a_1, a_2)$ of R, let $x \in R$ be such that x is not in $\mathfrak{a}$. Then for any positive integers r, s, x is invertible modulo (a_1^r, a_2^s).*

See appendix A for a proof.

Noetherian Ring A ring R is called **Noetherian** if every ideal of R is finitely generated. We show that $\mathbb{Z}[X]/(f(X))$ is finitely generated for any polynomial $f(X) \in \mathbb{Z}[X]$, and hence Noetherian.

Lemma 3.3. *If a ring R is Noetherian, then for any ideal $\mathfrak{a}$ of R, the ring $R/\mathfrak{a}$ is Noetherian.*

Corollary 3.4. *(see [Cond]) The ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ is Noetherian for any polynomial $f(X) \in Z[X]$.*

Theorem 3.5 (Krull Intersection Theorem). *Let R be a Noetherian ring, and $\mathcal{I}$ an ideal in R. Then*

$$\mathcal{I} * \bigcap_{i=1}^{\infty} \mathcal{I}^i = \bigcap_{i=1}^{\infty} \mathcal{I}^i$$

For an elementary proof see [Kap73, Theorem 74].

We will directly prove the following corollary in lemma 5.10 using theorem 3.5 for certain requisite maximal ideals in the ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, even when $f(X)$ is not irreducible over $\mathbb{Q}$, i.e. when $\mathcal{R}$ is not necessarily an integer domain. However, we state this more general corollary here for high-level discussion.

Corollary 3.6 (See e.g. [Eis13]). *For any Noetherian ring R that is also an integral domain, for any ideal $\mathcal{I}$ of R,*

$$\bigcap_{i=1}^{\infty} \mathcal{I}^{\,i} \;=\; 0$$

For a proof of the general form of CRT below, see e.g. [Eis13].

Theorem 3.7 (Chinese Remainder Theorem (CRT)). *Let $\mathfrak{a}_1, ..., \mathfrak{a}_k$ be a set of pairwise co-prime ideals of a ring R. Then,*

$$R/\mathfrak{a}_1 \cdots \mathfrak{a}_k \;\equiv\; \prod_i R/\mathfrak{a}_i$$

For a proof of the following celebrated theorem see [Conb] or [Coh93, Theorem 6.1.4]. Recall, for a prime p, $\mathbb{Z}_p[X]$ is a unique factorization domain.

Theorem 3.8 (Dedekind Index Theorem). *Let p be a prime integer. For any monic polynomial $f(X) \in \mathbb{Z}[X]$ that is irreducible over $\mathbb{Q}$, let $\mathcal{O}_{\mathbf{K}}$ be the ring of integers of the number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$. Let the following be the (unique) factorization of $f(X)$ modulo p into powers of m irreducible polynomials $h_i(X) \in \mathbb{Z}_p[X]$ $(i \in [m])$:*

$$f(X) = h_1(X)^{e_1}...h_m(X)^{e_m} \;+\; p \cdot t(X),$$

where e_i are positive integers, and $t(X) \in \mathbb{Z}_p[X]$. Then, $p \nmid [\mathcal{O}_{\mathbf{K}} : \mathbb{Z}[X]/(f(X))]$ if and only if for all $i \in [m]$ such that $e_i \geq 2$, polynomial $h_i(X)$ does not divide $t(X)$ in $\mathbb{Z}_p[X]$.

4 Polynomial Ring Calculus

4.1 Circulant Matrices

Definition 4.1 (Circulant Matrices modulo $f(X)$). *On polynomial ring modulo $f(X)$, the circulant matrix (modulo $f(X)$) for a ring element $g(X)$ is given by an n-by-n matrix $\boldsymbol{C}_g$ whose i-th column is the coefficients of $g(X) * X^i$ modulo $f(X)$ for $i = 0, 1, \ldots, n-1$.*

We could take the underlying polynomial ring to be any of $\mathcal{R}, \mathcal{R}_{\mathbb{Q}}$ and $\mathcal{R}_q$. For simplicity, in the following part, we abuse the notion of circulant matrix without explicitly mentioning the underlying modulo polynomial $f(X)$.

Proposition 4.1. *For any two ring elements $g(X)$ and $h(X)$, $\boldsymbol{C}_g \times \mathbf{h}$ corresponds to the their product $g(X) * h(X)$.*

Corollary 4.2. *For any two ring elements $g(X)$ and $h(X)$, $\boldsymbol{C}_g \times \boldsymbol{C}_h = \boldsymbol{C}_{g*h}$.*

It's not difficult to see that circulant matrices are closed under addition and multiplication. Moreover, the multiplication commutes.

Corollary 4.3. *On polynomial ring modulo $f(X)$, all the circulant matrices form a commutative subring under matrix addition and multiplication.*

Lemma 4.4. *On polynomial ring modulo $f(X)$, a circulant matrix $\boldsymbol{C}_g$ has an inverse $\boldsymbol{C}_g^{-1} = \boldsymbol{C}_{g^{-1}}$ iff $g(X)$ is invertible modulo $f(X)$.*

For rational polynomial ring $\mathcal{R}_{\mathbb{Q}} = \mathbb{Q}[X]/(f(X))$, the inverse of the circulant matrix can also be given as $\boldsymbol{C}_g^{-1} = \frac{1}{\det(\boldsymbol{C}_g)} \cdot \mathrm{adj}(\boldsymbol{C}_g)$ where $\mathrm{adj}(\boldsymbol{C}_g)$ is the adjugate matrix of $\boldsymbol{C}_g$ with $\mathrm{adj}(\boldsymbol{C}_g)_{i,j} = (-1)^{i+j} \cdot \det(M_{j,i})$. Here, $M_{i,j}$, commonly known as the minor, is obtained by removing the i-th row and j-th column from $\boldsymbol{C}_g$. If $g(X)$ is from $\mathcal{R}$ and $\boldsymbol{C}_g$ is integer, its inverse $\boldsymbol{C}_g^{-1}$ is also integer except for a common (integer) denominator $\det(\boldsymbol{C}_g)$.

Another view of the canonical embedding. Take the Vandermonde matrix $\boldsymbol{V}$ of $f(X)$. It defines an embedding from the polynomial ring $\mathcal{R}$ to its evaluation domain $\mathcal{H}$. Let $\boldsymbol{D}_g$ be the diagonal matrix with its diagonal being the canonical embedding of $g(X)$, i.e. $(\boldsymbol{D}_g)_{i,i} = g(z_i)$. Consider $(\boldsymbol{V} \times \boldsymbol{C}_g)_{i,j} = p_j(z_i)$ where $p_j(X) = g(X) * X^j$. Note that the polynomial multiplication is under the polynomial ring modulo $f(X)$. Because $p_j(X) = g(X)X^j - t_j(X)f(X)$ for some polynomial $t_j(X)$, we have

$$(\boldsymbol{V} \times \boldsymbol{C}_g)_{i,j} = p_j(z_i) = g(z_i) \cdot z_i^j - t_j(z_i) \cdot 0 = g(z_i) \cdot z_i^j = (\boldsymbol{D}_g \times \boldsymbol{V})_{i,j}$$

and hence $\boldsymbol{V}\boldsymbol{C}_g = \boldsymbol{D}_g\boldsymbol{V}$ or $\boldsymbol{V}\boldsymbol{C}_g\boldsymbol{V}^{-1} = \boldsymbol{D}_g$.

In other words, in the polynomial ring modulo $f(X)$, the diagonal matrix of $g(X)$'s evaluations (at roots of $f(X)$) can be obtained by a similarity transformation (given by Vandermonde matrix V of $f(X)$) of the circulant matrix of $g(X)$.

The determinant of the circulant matrix $\boldsymbol{C}_g$ can be then calculated as

$$\det(\boldsymbol{C}_g) = \frac{\det(\boldsymbol{D}_g)}{\det(\boldsymbol{V})\det(\boldsymbol{V}^{-1})} = \det(\boldsymbol{D}_g) = \prod_{i=0}^{n-1} g(z_i) \tag{1}$$

where z_i's are the roots of $f(X)$. Note that this is just the product of all the entries in the embedding of $g(X)$. When $f(X)$ is irreducible, and thus $\mathcal{R}_{\mathbb{Q}}$ is a field, then this quantity, i.e. the determinant $\det(\boldsymbol{C}_g)$ is called the norm of $g(X)$ in the extension field $\mathcal{R}_{\mathbb{Q}}$ of $\mathbb{Q}$.

4.2 Ideals and Ideal Lattices

In this section, we focus on $\mathcal{R}_{\mathbb{Q}} = \mathbb{Q}[X]/(f(X))$ and its sub-ring, the integer polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$. When $f(X)$ is irreducible over $\mathbb{Q}$, $\mathcal{R}_{\mathbb{Q}}$ is a field, denoted by $\mathbf{K}$. It's ring of integers $\mathcal{O}_{\mathbf{K}}$ is the integral extension of $\mathcal{R}$, and is quite often not the same as $\mathcal{R}$.

Ideal. As shown in corollary 3.4, ideals of $\mathcal{R}$ are finitely generated. Thus, any ideal $\mathcal{I}$ can be given by a finite set of generators, say, $g_0, g_1, \ldots, g_{t-1} \in \mathcal{R}$ as

$$\begin{aligned}\mathcal{I} &= \{\, a_0 g_0 + a_1 g_1 + \ldots, a_{t-1} g_{t-1} \mid a_i \in \mathcal{R}\} \\ &= \left\{\, \boldsymbol{C}_{g_0}\mathbf{a_0} + \boldsymbol{C}_{g_1}\mathbf{a_1} + \boldsymbol{C}_{g_{t-1}}\mathbf{a_{t-1}} \middle|\, \mathbf{a_i} \in \mathbb{Z}^n\right\} \\ &= \left\{\, \left[\boldsymbol{C}_{g_0} | \boldsymbol{C}_{g_1} | \cdots | \boldsymbol{C}_{g_{t-1}}\right] \times \mathbf{a} \middle|\, \mathbf{a} \in \mathbb{Z}^{t \times n}\right\}\end{aligned}$$

It's not difficult to see that, one can derive an n-by-n integer basis matrix by computing the Hermite normal form of $\left[\boldsymbol{C}_{g_0} | \boldsymbol{C}_{g_1} | \cdots | \boldsymbol{C}_{g_{t-1}}\right]$, or simply by iteratively using the fact that Euclid's algorithm gives a unimodular transformation from $[a\ b]$ to $[\gcd(a,b)\ 0]$ (for any intgers a, b). We denote by $\boldsymbol{B}(\mathcal{I})$ the basis matrix of $\mathcal{I}$. Note that all basis matrices are close under integer unimodular transformation, and hence their determinants are the same. Specifically, a *principal ideal* is an ideal generated by only one element g, whose basis matrix could be given as a circulant matrix $\boldsymbol{C}_g$.

If not explicitly mentioned, we focus on *full rank* ideals $\mathcal{I}$ whose basis matrix is invertible over $\mathbb{Q}$; this is always the case when $f(X)$ is irreducible. For a principal ideal given by $\boldsymbol{C}_g$ this is equivalent to requiring that $g(X)$ is invertible in $\mathbb{Q}[X]/(f(X))$.

Ideal Lattice. Since an ideal $\mathcal{I}$ of $\mathcal{R}$ has a $\mathbb{Z}$-basis, say $\boldsymbol{B}(\mathcal{I})$, it defines a lattice in $\mathcal{R} \subseteq \mathcal{R}_{\mathbb{Q}}$. We can also embed this lattice in $\mathcal{H}$, and consider the embedding as a lattice in $\mathcal{H}$. The canonical embedding given by the Vandermonde matrix $\boldsymbol{V}$ of $f(X)$ naturally induces an *ideal lattice* $\mathcal{L}(\mathcal{I})$ in $\mathcal{H}$, given by matrix $\boldsymbol{V}\boldsymbol{B}(\mathcal{I})$.

Ideal Lattice Dual. For an ideal $\mathcal{I}$, the dual of its ideal lattice $\mathcal{L}(\mathcal{I})$ in $\mathcal{H}$ is defined to be $\mathcal{L}(\mathcal{I})^{\vee} = \left\{\mathbf{y} \in \mathcal{H} \middle|\, \forall \mathbf{x} \in \mathcal{L}(\mathcal{I}),\ \mathbf{y}^H \cdot \mathbf{x} \in \mathbb{Z}\right\} = \left\{\mathbf{y} \in \mathcal{H} \middle|\, \forall \mathbf{z} \in \mathbb{Z}^n,\ \mathbf{y}^H \cdot \boldsymbol{V}\boldsymbol{B}(\mathcal{I})\mathbf{z} \in \mathbb{Z}\right\}$ $= \left\{\boldsymbol{V}^{-H}\boldsymbol{B}(\mathcal{I})^{-H}\mathbf{z} \middle|\, \mathbf{z} \in \mathbb{Z}^n\right\}$. As mentioned above, the basis $\boldsymbol{B}(\mathcal{I})$ also defines a lattice in $\mathcal{R}_{\mathbb{Q}}$, and one can define a dual of the ideal itself using trace pairing. Recall the mapping φ between a polynomial and its coefficients represented as a vector. The trace pairing of $a(X), b(X) \in \mathcal{R}_{\mathbb{Q}}$, $\mathrm{Tr}(a(X), b(X))$ is defined to be trace of $\boldsymbol{V} \cdot \varphi(a(X) * b(X))$ which is same as $(\boldsymbol{V} \cdot \varphi(a(X)))^{\top} \cdot (\boldsymbol{V} \cdot \varphi(b(X))$. Thus, we can define the dual $\mathcal{I}^{\vee}$ of ideal $\mathcal{I}$ to be the set

$$\{\, b(X) \in \mathcal{R}_{\mathbb{Q}} |\, \forall a(X) \in \mathcal{I},\ \mathrm{Tr}(a(X), b(X)) \in \mathbb{Z}\}\,.$$

Note that this is the pre-image in $\mathcal{R}_{\mathbb{Q}}$ of the complex conjugate of $\mathcal{L}(\mathcal{I})^{\vee}$. We prove below that this is indeed a (fractional) ideal of $\mathcal{R}$. Hence, we will refer to $\mathcal{I}^{\vee}$ as the **dual ideal** of $\mathcal{I}$.

Lemma 4.5. *For an ideal $\mathcal{I}$ of $\mathcal{R}$ with basis $\boldsymbol{B}(\mathcal{I})$* [4]*,*

i) *the dual $\mathcal{I}^\vee$ is the $\mathbb{Z}$-span of $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}$,*
ii) *the matrix $\det(\boldsymbol{B}(\mathcal{I})) \cdot \det(\boldsymbol{V}^\top \boldsymbol{V}) \cdot (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot \boldsymbol{B}(\mathcal{I})^{-\top}$ is an integer matrix,*
iii) *the dual $\mathcal{I}^\vee$ is a fractional ideal of $\mathcal{R}$.*

Proof. For part (i), since the dual $\mathcal{I}^\vee$ is the pre-image (under $\boldsymbol{V}$) of the complex conjugate of $\mathcal{L}(\mathcal{I})^\vee$, and the latter has $\mathbb{Z}$-basis $\boldsymbol{V}^{-H}\boldsymbol{B}(\mathcal{I})^{-H}$, the matrix $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}$ forms a $\mathbb{Z}$-basis for $\mathcal{I}^\vee$.

For part (ii), we only need to show that $(\boldsymbol{V}^\top \boldsymbol{V})$ is integer, since $\boldsymbol{B}(\mathcal{I})$ is always an integer matrix for $\mathcal{I} \subseteq \mathcal{R}$. Consider its entry $(\boldsymbol{V}^\top \boldsymbol{V})_{i,j} = \sum_{k=0}^{n-1} z_k^{i+j}$. We argue that the power sums of roots, $p_t = \sum_{k=0}^{n-1} z_k^t$, is an integer for $0 \leq t \leq 2n$. Note that the coefficients of $f(X) = \prod_{t=0}^{n-1}(X - z_t) = \sum_{t=0}^{n} e_t X^t$ are elementary symmetric polynomials $e_t = e_t(z_0, \ldots, z_{n-1})$ in the roots of $f(X)$. Starting from $p_0 = n$ and $p_1 = e_1 \in \mathbb{Z}$, by Newton's identity, every power sum p_t is an integer linear combination of $\{p_0, \ldots, p_{t-1}\}$ and $\left\{e_0, \ldots, e_{\min(t,n)}\right\}$.

Now we prove (iii). We need to show that for every $\mathbf{g} \in \mathcal{R}$ and $\mathbf{a} \in \mathcal{I}^\vee$, $\mathbf{g} * \mathbf{a}$ is in $\mathcal{I}^\vee$, i.e. for all $\mathbf{b} \in \mathcal{I}$, $\mathrm{Tr}(\mathbf{g} * \mathbf{a} * \mathbf{b})$ is integer. By commutativity of polynomial multiplication, this is same as requiring that $\mathrm{Tr}(\mathbf{a} * \mathbf{g} * \mathbf{b})$ is integer. But $\mathbf{c} = \mathbf{g} * \mathbf{b}$ is in $\mathcal{I}$, as it is an ideal, and hence $\mathrm{Tr}(\mathbf{a} * \mathbf{c})$ is an integer as $\mathbf{a}$ is in $\mathcal{I}^\vee$ and $\mathbf{c}$ is in $\mathcal{I}$. Thus, $\mathcal{I}^\vee$ is closed under multiplication by $\mathcal{R}$. Now, again by commutativity, for every $\mathbf{d} \in \mathcal{R}$, $\mathbf{d}\mathcal{I}^\vee$ is also closed under multiplication by $\mathcal{R}$. Thus (iii) follows from (i) and (ii).

The Dual Ring. When the entire ring $\mathcal{R}$ is considered as an ideal, i.e. (1), its dual, by lemma 4.5, is a fractional ideal given by the $\mathbb{Z}$-basis matrix $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}$, and is referred to as the **dual ring**[5] $\mathcal{R}^\vee$.

Lemma 4.6. *For an ideal $\mathcal{I}$ of $\mathcal{R}$, for any $\mathbf{a} \in \mathcal{I}$ and any $\mathbf{b} \in \mathcal{I}^\vee$, $\mathbf{a} * \mathbf{b} \in \mathcal{R}^\vee$.* [6]

Proof. Since by lemma 4.5, $\mathcal{I}^\vee$ is a (fractional ideal), we have that for any $\mathbf{c} \in \mathcal{R}$, since $\mathbf{b} * \mathbf{c}$ is also in $\mathcal{I}^\vee$. Thus, by definition of the dual-ideal (applied to dual of $\mathcal{I}$), $\mathrm{Tr}(\mathbf{a}, \mathbf{b} * \mathbf{c}) \in \mathbb{Z}$. Since the trace is same as $\boldsymbol{V} \times (\mathbf{a} * \mathbf{b} * \mathbf{c})$, this also implies that $\mathrm{Tr}(\mathbf{a} * \mathbf{b}, \mathbf{c}) \in \mathbb{Z}$. Since this holds for all $\mathbf{c} \in \mathcal{R}$, again by definition of dual ideal (applied to dual of $\mathcal{R}$), $\mathbf{a} * \mathbf{b}$ is in dual of $\mathcal{R}$, i.e. $\mathcal{R}^\vee$.

Let $f(X) = \sum_{i=0}^{n} f_i \cdot X^i$ with $f_n = 1$. Take its derivative $f'(X) = \sum_{i=0}^{n-1}(i + 1) \cdot f_{i+1} \cdot X^i$. First, notice that $f'(X)$ is invertible in $\mathcal{R}_\mathbb{Q} = \mathbb{Q}[X]/(f(X))$.

Proposition 4.7. *Given $f(X)$ with all distinct roots, its derivative $f'(X)$ shares no common root with $f(X)$.*

[4] This lemma actually holds for any sub-ring of $\mathcal{R}_\mathbb{Q}$, e.g. the ring of integers of a number field with $f(X)$ irreducible over $\mathbb{Q}$.

[5] This is really a misnomer, as $\mathcal{R}^\vee$ is not closed under multiplication by $\mathcal{R}^\vee$, but only closed under multiplication by $\mathcal{R}$. Hence it is not a ring, but merely a $\mathcal{R}$-module. We will continue to call this the dual ring as in [DD12].

[6] This lemma also holds for every sub-ring of $\mathcal{R}_\mathbb{Q}$.

The proof of the above proposition is standard. When $f(X)$ is irreducible over $\mathbb{Q}$, it is known that $f(X)$ has distinct roots over the complex numbers.

We now show that, the dual ring $\mathcal{R}^\vee$ has the circulant matrix of the inverse of $f'(X)$ as a $\mathbb{Z}$-basis, and since $\mathcal{R}^\vee$ is also a fractional ideal of $\mathcal{R}$, it can also be seen as the fractional ideal [7] generated by the inverse of $f'(X)$. More precisely, the basis matrix $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}$ is same as $\boldsymbol{C}_{f'}^{-1}\boldsymbol{M}$, where $\boldsymbol{M}$ is the following n-by-n unimodular matrix:

$$\boldsymbol{M} = \begin{bmatrix} f_1 & f_2 & \cdots & f_n \\ f_2 & \iddots & f_n & 0 \\ \vdots & f_n & \ddots & \vdots \\ f_n & 0 & \cdots & 0 \end{bmatrix}$$

i.e. where $\boldsymbol{M}_{i,j} = f_{i+j+1}$ if $i + j < n$ and $\boldsymbol{M}_{i,j} = 0$ otherwise.

Lemma 4.8. $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} = \boldsymbol{C}_{f'}^{-1}\boldsymbol{M}$.

Proof. It suffices to show that $\boldsymbol{M} \times \boldsymbol{V}^\top \boldsymbol{V} = \boldsymbol{C}_{f'}$. This is equivalent to

$$\begin{aligned} \boldsymbol{V}\boldsymbol{M}\boldsymbol{V}^\top \boldsymbol{V}\boldsymbol{V}^{-1} &= \boldsymbol{V}\boldsymbol{C}_{f'}\boldsymbol{V}^{-1} \\ \boldsymbol{V}\boldsymbol{M}\boldsymbol{V}^\top &= \boldsymbol{D}_{f'}. \end{aligned}$$

Here $\boldsymbol{D}_{f'}$ is a diagonal matrix with $(\boldsymbol{D}_{f'})_{i,i} = f'(z_i)$ where z_i's are (complex) roots of $f(X)$. Next we verify that

$$(\boldsymbol{V}\boldsymbol{M}\boldsymbol{V}^\top)_{i,j} = \sum_{s=0}^{n-1}\sum_{t=0}^{n-s-1} f_{s+t+1} \cdot z_i^s \cdot z_j^t = \sum_{p=0}^{n-1} f_{p+1} \cdot \left(\sum_{s=0}^{p} z_i^s z_j^{p-s}\right)$$

If $i = j$, we have

$$(\boldsymbol{V}\boldsymbol{M}\boldsymbol{V}^\top)_{i,i} = \sum_{p=0}^{n-1} f_{p+1} \cdot \sum_{s=0}^{p} z_i^p = \sum_{p=0}^{n-1} f_{p+1} \cdot (p+1) \cdot z_i^p = f'(z_i).$$

Otherwise when $i \neq j$, we have

$$\begin{aligned} (\boldsymbol{V}\boldsymbol{M}\boldsymbol{V}^\top)_{i,j} &= \sum_{p=0}^{n-1} f_{p+1} \cdot \left(\sum_{s=0}^{p} z_i^s z_j^{p-s}\right) = \sum_{p=0}^{n-1} f_{p+1} \cdot \left(\frac{z_i^{p+1} - z_j^{p+1}}{z_i - z_j}\right) \\ &= \frac{f(z_i) - f_0 - f(z_j) + f_0}{z_i - z_j} = 0. \end{aligned}$$

Corollary 4.9. *For monic $f(X)$, $\Delta_f = |\det(\boldsymbol{C}_{f'})|$.*

Moreover, this particular matrix $\boldsymbol{M}$ also has an interesting property, that it symmetricizes every circulant matrices by right multiplication:

[7] It is well known [Conc] that the dual $\mathcal{O}_K^\vee$ of the ring of integers $\mathcal{O}_K$ of a number field K is *not* always generated by the inverse of $f'(X)$.

Proposition 4.10. *For $g(X) \in \mathcal{R}_{\mathbb{Q}}$, $\boldsymbol{C}_g\boldsymbol{M}$ is symmetric.*

Proof. Recall that the circulant matrix $\boldsymbol{C}_g$ is diagonalized by similarity transformation of the Vandermonde matrix $\boldsymbol{V}$ of $f(X)$: $\boldsymbol{D}_g = \boldsymbol{V}\boldsymbol{C}_g\boldsymbol{V}^{-1}$.Thus, $\boldsymbol{C}_g\boldsymbol{M}$ $= \boldsymbol{C}_{f'} \times \boldsymbol{C}_{f'}^{-1}\boldsymbol{C}_g\boldsymbol{M} = \boldsymbol{C}_{f'} \times \boldsymbol{C}_g \times \boldsymbol{C}_{f'}^{-1}\boldsymbol{M} = \boldsymbol{C}_{f'} \times \boldsymbol{C}_g \times (\boldsymbol{V}^\top\boldsymbol{V})^{-1} = \boldsymbol{C}_{f'}(\boldsymbol{V}^\top\boldsymbol{V})^{-1}$ $\times\ \boldsymbol{V}^\top\boldsymbol{V}\boldsymbol{C}_g(\boldsymbol{V}^\top\boldsymbol{V})^{-1} = \boldsymbol{M} \times \boldsymbol{V}^\top\boldsymbol{D}_g\boldsymbol{V}^{-\top} = \boldsymbol{M}\boldsymbol{C}_g^\top$.

We claim that $\boldsymbol{C}_g\boldsymbol{M}$ is symmetric since $\boldsymbol{M}$ is symmetric.

Corollary 4.11. *For $g(X) \in \mathcal{R}_{\mathbb{Q}}$, $\boldsymbol{C}_g(\boldsymbol{V}^\top\boldsymbol{V})^{-1} = (\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{C}_g^\top$ and $(\boldsymbol{V}^\top\boldsymbol{V})\boldsymbol{C}_g = \boldsymbol{C}_g^\top(\boldsymbol{V}^\top\boldsymbol{V})$.*

Corollary 4.12. *For any principal ideal $\mathfrak{a}$ of $\mathcal{R}$, $\mathfrak{a}^\vee = \mathfrak{a}^{-1}\mathcal{R}^\vee$.*

Proof. Let $\mathbf{g}$ be a generator of the principal ideal $\mathfrak{a}$. By lemma 4.5, $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{C}_g^{-\top}$ is a $\mathbb{Z}$-basis of the dual ideal $\mathfrak{a}^\vee$. By corollary 4.11, this is same as $\boldsymbol{C}_g^{-1}(\boldsymbol{V}^\top\boldsymbol{V})^{-1}$. Since $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}$ is a $\mathbb{Z}$-basis for $\mathcal{R}^\vee$, the claim follows.

For the ring of integers, the above lemma generalizes to all ideals $\mathfrak{a}$ of the domain, and not just principal ideals (see e.g. [Conc]). The above corollary can also be extended to all invertible ideals of $\mathcal{R}$, but for our purposes this suffices. This corollary, along with lemma 4.6, will be used in proving the ideal clearing lemma.

5 Ideal $\mathfrak{a}$ modulo $p^r\mathfrak{a}$ is Principal for Dedekind-Special primes p

In this section we will show that for every monic and separable $f(X)$ and special primes p, we can prove that the ring $\mathcal{R}$ modulo p^r, for any positive integer r, is a principal ideal ring (PIR). Moreover, we show that every ideal $\mathfrak{a}$ of $\mathcal{R}$, modulo the ideal $p^r\mathfrak{a}$, is principal. Normally, such a claim holds for Dedekind domains, and the proofs require the unique prime decomposition theorem for Dedekind domains. We show that even if the ring is not a Dedekind domain, for some commonly used Noetherian rings, it can directly be shown that the ring $\mathcal{R}$ modulo p^r is a PIR, and further, every ideal $\mathfrak{a}$ is principal modulo $p^r\mathfrak{a}$.

Let p be a prime such that in the factorization of $f(X)$ modulo p in terms of irreducible polynomials (mod p), i.e.

$$f(X) = \prod_{i=1}^{m} h_i(X)^{e_i} + p * t(X),$$

for all $i \in [m]$, for which e_i is more than one, it is the case that $t(X)$ is invertible modulo the ideal $(p, h_i(X))$ of $\mathbb{Z}[X]$. In other words, for all i such that $h_i(X)$ has multiplicity more than one, it is the case that $t(X)$ is not divisible by $h_i(X)$ modulo p. The *Dedekind index theorem* (theorem 3.8) states that for irreducible (over $\mathbb{Q}$) $f(X)$ and such primes p, prime p does not divide $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$. Here, as usual, $\mathcal{O}_{\mathbf{K}}$ is the ring of integers[8] of the number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$, and $\mathcal{R}$, i.e. $\mathbb{Z}[X]/(f(X))$, is a sub-ring of $\mathcal{O}_{\mathbf{K}}$.

Fix a polynomial $f(X)$, *not* necessarily irreducible over $Z[X]$. For any prime p such that the factorization of $f(X)$ modulo p has the above property, p will be called a **Dedekind-special prime** [9]. The polynomial $t(X)$ (more precisely, its representative in $\mathbb{Z}_p[X]$) will be referred to as the **quotient** in the factorization of $f(X)$ modulo p. In this section we will fix p to be a Dedekind-special prime, and as usual, $\mathcal{R}$ will stand for the ring $\mathbb{Z}[X]/(f(X))$.

For each $i \in [m]$, define the following ideals $\mathfrak{p}_i$ of $\mathcal{R}$: $\mathfrak{p}_i = (h_i(X), p)$. Also, define the following ideals $\mathfrak{s}_i$ of $\mathcal{R}$: $\mathfrak{s}_i = (h_i(X)^{e_i}, p)$.

Lemma 5.1. *In the ring $\mathcal{R}$, for $i \in [m]$,*

(i) *the ideal $\mathfrak{p}_i$ is maximal.*
(ii) $\mathfrak{s}_i = \mathfrak{p}_i^{e_i}$.

Proof. (i) The proof is straightforward by noting that $h_i(X)$ is irreducible modulo p.

(ii) If $e_i = 1$, there is nothing to prove. Otherwise, $\mathfrak{p}_i^{e_i}$ is contained in $\mathfrak{s}_i = (h_i(X)^{e_i}, p)$ follows simply because the only term in $\mathfrak{p}_i^{e_i}$ that is not in (p) is $h_i(X)^{e_i}$. For the other direction, we only need to show that p is contained in $\mathfrak{p}_i^{e_i}$. We show that $p \in (h_i(X)^{e_i}, p * h_i(X)^{e_i-1}, p^{e_i}) \subseteq \mathfrak{p}_i^{e_i}$. Note that ideal $(h_i(X)^{e_i})$ contains $p * t(X)$ by the factorization of $f(X)$, and where $t(X)$ is the quotient in the factorization. Moreover, by the Dedekind-special property of p (w.r.t. $f(X)$), and given that $e_i \geq 2$, $t(X)$ is not in $(h_i(X), p) = \mathfrak{p}_i$. Thus, since $\mathfrak{p}_i$ is maximal by (i), $t(X)$ is invertible modulo $(h_i(X), p)$. Then, by lemma 3.2, $t(X)$ is invertible modulo $(h_i(X)^{e_i-1}, p^{e_i-1})$. Thus, $(t(X), h_i(X)^{e_i-1}, p^{e_i-1}) = (1)$, and further $p*(t(X), h_i(X)^{e_i-1}, p^{e_i-1}) = (p)$, and the claim follows.

The proof of the following two lemmas is similar to that of the proof of lemma 5.1(ii). Detailed proofs can be found in appendix A.

Lemma 5.2. *In the ring $\mathcal{R}$, let $w = \sum_{i=1}^{m} e_i$. If $w \geq 2$, and some $e_i = 1$ (w.l.o.g. $e_m = 1$), then $p^{w-2} * h_m(X)$ is invertible modulo the ideal $(p^{w-1}, \prod_{j=1}^{m-1} h_j(X)^{e_j})$.*

Lemma 5.3. *Let $w = \sum_{i=1}^{m} e_i$. If for all $i \in [m]$, $e_i > 1$, then $t(X)$, the quotient in the factorization of $f(X)$ modulo p, is invertible modulo the ideal $(p^{w-1}, p^{w-2} h_m(X))$.*

[8] The ring of integers $\mathcal{O}_K$ is potentially an extension of the ring $\mathbb{Z}[X]/(f(X))$, as it contains all elements of $\mathbb{Q}[X]/(f(X))$ that satisfy a polynomial relation with integer coefficients.

[9] Similarly, any integer that is a product of powers of Dedekind-special primes will also be referred to as Dedekind-special for $f(X)$.

Remark. In the ring of integers $\mathcal{O}_{\mathbf{K}}$ of the number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$, another theorem of Dedekind gives a similar factorization of the ideal (p) as in the lemma below, when the Dedekind-special property holds for p w.r.t. $f(X)$.

Lemma 5.4. *In the ring $\mathcal{R}$, the ideal (p) is same as $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_m^{e_m}$.*

Proof. $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_m^{e_m}$ is subset of (p); this is easy to see since all but one generators in $\prod_{i=1}^m (h_i(X)^{e_i}, p)$ are trivially in (p). The last generator $\prod_{i=1}^m h_i(X)^{e_i}$ is also in (p), because it is same as $f(X)$ modulo p, which is zero in $\mathcal{R}$ modulo p.

For the other direction, first consider the case where for all $i \in [m]$, $e_i > 1$. We show that the three terms in $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_m^{e_m}$, namely p^w, $p^{w-1}\mathfrak{p}_m$, and $\prod_{i=1}^m h_i(X)^{e_i}$ generate p. The last term is same as $p \cdot t(X)$ (by the factorization of $f(X)$ mod p). Thus, taking p as a common factor, the three terms generate $p \cdot 1$ by lemma 5.3.

Now, consider the case that there is some i such that $e_i = 1$, w.l.o.g. $e_m = 1$. If $m = 1$ and hence $e_1 = 1$, we have that (p) itself is maximal as every element in $\mathcal{R}$ not in (p) is invertible modulo p. For $m \geq 2$, we show that p is generated by $\prod_{i=1}^m (h_i(X), p)^{e_i}$ in $\mathcal{R}$. Let $w = \sum_{i=1}^m e_i$. Pick the generators $p^{w-1} * h_m(X)$, $p * \prod_{j=1}^{m-1} h_j(X)^{e_j}(X)$ and p^w from $\prod_{i=1}^m (h_i(X), p)^{e_i}$. Taking a common factor p out, we focus on the generators $p^{w-2} * h_m(X)$, $\prod_{j=1}^{m-1} h_j(X)^{e_j}$ and p^{w-1}. An easy application of the lemma 5.2 shows these three generators generate 1.

Theorem 5.5. *For any positive integer r,*

$$\mathbb{Z}_{p^r}[X]/(f(X)) \;\cong\; \mathcal{R}/p^r\mathcal{R} \;\cong\; \mathcal{R}/\prod_{i=1}^m \mathfrak{p}_i^{r \cdot e_i} \;\cong\; \prod_{i=1}^m \mathcal{R}/\mathfrak{p}_i^{r \cdot e_i}$$

Proof. We focus on the second and third congruence, as the first is straight forward. The second congruence follows directly from lemma 5.4. Since the powers of co-prime ideals are also co-prime, we apply CRT (of general rings and co-prime ideals) to conclude the proof.

The rest of the section is devoted to proving that $\mathcal{R}/\mathfrak{p}_i^r$ is a principal ideal ring (PIR) (Theorem 5.6 below), and any ideal $\mathfrak{a}$ is principal modulo $p^r\mathfrak{a}$ (Theorem 5.9). If $\mathcal{R}$ was a Dedekind domain, the usual proof goes as follows: One first shows that $\mathcal{R}/\mathfrak{p}_i^r$ is isomorphic to $\mathcal{R}_{\mathfrak{p}_i}/\mathfrak{p}_i^r\mathcal{R}_{\mathfrak{p}_i}$, where $\mathcal{R}_{\mathfrak{p}_i}$ is the *localization* of $\mathcal{R}$ at the ideal $\mathfrak{p}_i^r$. If the reader is not familiar with localization, he/she can skip this discussion, as the direct proof we give *does not* use localization. Next, it is shown that the local ring $\mathcal{R}_{\mathfrak{p}_i}$ is a principal ideal domain (PID) by showing that it is a discrete valuation ring (DVR). This step requires the prime ideal decomposition theorem for Dedekind domains. Since the quotient ring of a PID is a PID, the claim follows.

While our ring $\mathcal{R}$ may not be a Dedekind domain, most of the above steps would still go through for our special p, except for proving that $\mathcal{R}_{\mathfrak{p}_i}$ is a DVR, which is usually proved using the prime ideal decomposition theorem for Dedekind domains. Luckily, in our special case, we can still prove $\mathcal{R}_{\mathfrak{p}_i}$ is a DVR without the decomposition theorem for Dedekind Domains. As promised, we give a direct proof of Theorem 5.6. The proof of Theorem 5.9 is slightly more involved and uses the Krull intersection theorem for Noetherian rings.

Theorem 5.6. *For all $i \in [m]$, for all positive integers $r > 0$, $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$ is a principal ideal ring.*

In the proof of this theorem, there are two main cases, where either $e_i = 1$, or $e_i > 1$. In the first case p is always a generator of ideals (modulo $\mathfrak{p}_i^{r\cdot e_i}$) that are sub-ideals of $\mathfrak{p}_i$, and in the second case, using the Dedekind-special property of p (w.r.t. $f(X)$), the polynomial $h_i(X)$ is always a generator of ideals that are sub-ideals of $\mathfrak{p}_i$. Details follow.

Proof. Let $\mathfrak{q}$ be any ideal of $\mathcal{R}/\mathfrak{p}_i^r$. We first show that every ideal $\mathfrak{q}$ of $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$ that is not a sub-ideal of $(h_i(X), p)$ (as an ideal of $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$) is same as ideal (1) of $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$, and hence trivially principal. By lemma 5.1, $\mathfrak{p}_i$ is maximal in $\mathcal{R}$. Thus, by lemma 3.2 any $a(X) \in \mathcal{R}$ that is not in the maximal ideal $\mathfrak{p}_i = (h_i(X), p)$ is invertible modulo $\mathfrak{p}_i$, and also invertible modulo $\mathfrak{p}_i^{r\cdot e_i}$. If $\mathfrak{q}$ is not a sub-ideal of $(h_i(X), p)\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$, then there is an element $a(X)$ in $\mathfrak{q}$ that is not in $(h_i(X), p)\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$. Thus $a(X)$ is not in $(h_i(X), p)\mathcal{R}$ and hence is a unit of $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$, making $\mathfrak{q}$ same as (1).

So, now we focus on ideals $\mathfrak{q}$ that are sub-ideals of $(h_i(X), p)$. We first show that the ideal $(h_i(X), p)$ is principal in $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$. There are two cases:

1. $e_i = 1$:
   In this case, we show that $(h_i(X), p)$ is same as ideal (p) in $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$. For this, we show that $h_i(X)$ is generated by p modulo $\mathfrak{p}_i^{r\cdot e_i}$. From the factorization of $f(X)$ modulo p, we know that
   $$h_i(X) * \prod_{j\in[m], j\neq i} h_j(X)^{e_j} = p * t(X),$$
   in $\mathcal{R}$, for some polynomial $t(X)$. Moreover, each of the irreducible polynomials $h_j(X)$, $j \in [m], j \neq i$ is not in $(h_i(X), p)$ because $Z_p[X]$ is a UFD, and hence is invertible modulo $\mathfrak{p}_i^{r\cdot e_i}$ by lemma 3.2. Thus $h_i(X)$ is generated by p modulo $\mathfrak{p}_i^{r\cdot e_i}$.
2. $e_i > 1$: In this case, we show that $(h_i(X), p)$ is same as ideal $(h_i(X))$ in $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$. For this, we show that p is generated by $h_i(X)$ modulo $\mathfrak{p}_i^{r\cdot e_i}$. From the factorization of $f(X)$ modulo p, we know that
   $$h_i(X)^{e_i} * \prod_{j\in[m], j\neq i} h_j(X)^{e_j} = p * t(X),$$
   in $\mathcal{R}$, for some polynomial $t(X)$. Moreover, because p is a Dedekind-special w.r.t. $f(X)$, $t(X)$ is invertible modulo $\mathfrak{p}_i = (h_i(X), p)$. But, since $\mathfrak{p}_i$ is maximal, $t(X)$ is also invertible modulo $\mathfrak{p}_i = (h_i(X), p)^{r\cdot e_i}$. Thus, p is generated by $h_i(X)^{e_i}$ modulo $\mathfrak{p}_i^{r\cdot e_i}$, and hence also generated by $h_i(X)$ modulo $\mathfrak{p}_i^{r\cdot e_i}$.

Thus, $(h_i(X), p)$ is a principal ideal of $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$. Let g stand for this single generator of $(h_i(X), p)$, i.e. $g = p$ when $e_i = 1$ and $g = h_i(X)$ when $e_i > 1$. Hence, every ideal $\mathfrak{q}$ that is a sub-ideal of $(h_i(X), p)$, is a sub-ideal of (g). For any non-zero element a in $\mathfrak{q}$, let t_a be the largest integer greater than zero such that $a \in (g)^{t_a}$. Note $t_a < r \cdot e_i$, for otherwise a is zero in $\mathcal{R}/\mathfrak{p}_i^{r \cdot e_i}$. Thus, all elements of $\mathfrak{q}$ are in some ideal $(g)^t$, with $0 < t < r \cdot e_i$. Let t_q be the minimum of these t. Note $1 \leq t_q < r \cdot e_i$. We now show that $\mathfrak{q} = (g)^{t_q}$. Consider an element of a of $\mathfrak{q}$ that is in $(g)^{t_q}$. Then, a can be written as $g^{t_q} * a'$, where a' is not in the maximal ideal $(h(X), p)$ of $\mathcal{R}$. Hence, as before, a' is invertible in $\mathcal{R}/\mathfrak{p}_i^{r \cdot e_i}$, and thus g^{t_q} is in $\mathfrak{q}$. This shows that $\mathfrak{q} = (g)^{t_q}$, which makes it a principal ideal.

Corollary 5.7. *$\mathbb{Z}_{p^r}[X]/(f(X))$ is a principal ideal ring.*

Proof. Follows by theorems 5.5 and 5.6 as product of principal ideal rings is a principal ideal ring.

Lemma 5.8. *If $f(X)$ is irreducible as a polynomial in $\mathbb{Z}[X]$, then any ideal $\mathfrak{a}$ of $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ can be written as $\hat{\mathfrak{a}} \prod_{i \in [m]} \mathfrak{p}_i^{t_i}$, where t_i are non-negative integers, and $\hat{\mathfrak{a}}$ is an ideal of $\mathcal{R}$ co-prime to every $\mathfrak{p}_i$ $(i \in [m])$.*

Proof. If $\mathfrak{a}$ is co-prime to every $\mathfrak{p}_i$ $(i \in [m])$, then t_i can be taken to be zero, and we are done. Otherwise, let $I \subseteq [m]$ be the non-empty and maximal set of indices i, $i \in [m]$, such that $\mathfrak{a}$ is not co-prime to $\mathfrak{p}_i$. Since each $\mathfrak{p}_i$ is maximal (by lemma 5.1), this implies that $\mathfrak{a}$ is a subset of each of $\mathfrak{p}_i$ $(i \in I)$. For each $i \in I$, let $t(i) > 0$ be the largest integer such that $\mathfrak{a}$ is a subset of $\mathfrak{p}_i^{t(i)}$. Such a $t(i)$ is well-defined by corollary to Krull intersection theorem (Corollary 3.6), noting that $\mathcal{R}$ is also an integral domain.

We show that there exists an ideal $\hat{\mathfrak{a}}$ such that $\mathfrak{a} = \hat{\mathfrak{a}} * \prod_{i \in I} \mathfrak{p}_i^{t(i)}$.

Let $T = \sum_{i \in I} t(i)$. Define $\hat{\mathfrak{a}}$ to be the *fractional* ideal

$$p^{-T} * \mathfrak{a} * \left(\prod_{i \in I} \prod_{j \in [m], j \neq i} \mathfrak{p}_j^{t(i)} \right).$$

Using lemma 5.4, it is straightforward to check that $\hat{\mathfrak{a}} * (\prod_{i \in I} \mathfrak{p}_i^{t(i)}) = \mathfrak{a}$.

We now show that $\hat{\mathfrak{a}}$ is actually an integral ideal, i.e. an ideal of $\mathcal{R}$. We will show that $\mathfrak{a} * \left(\prod_{i \in I} \prod_{j \in [m], j \neq i} \mathfrak{p}_j^{t(i)} \right)$ is in $(p)^T$. Since, for all $i \in I$, $\mathfrak{a}$ is in $\mathfrak{p}_i^{t(i)}$, $\mathfrak{a} \subseteq \cap_{i \in I} \mathfrak{p}_i^{t(i)}$. But, these ideals $\mathfrak{p}_i^{t(i)}$ are all co-prime, and hence $\mathfrak{a} \subseteq \prod_{i \in I} \mathfrak{p}_i^{t(i)}$. We next show that for all $i \in I$, $\mathfrak{p}_i^{t(i)} * \prod_{j \in [m], j \neq i} \mathfrak{p}_j^{t(i)}$ is in $(p)^{t(i)}$. But, this is clear from the factorization of (p) given by lemma 5.4.
Claim: Ideal $\hat{\mathfrak{a}}$ is co-prime to every $\mathfrak{p}_i$, $i \in [m]$.
Proof of Claim: If there exists an $i \in [m]$, say i^*, such that $\hat{\mathfrak{a}}$ is not co-prime to $\mathfrak{p}_{i^*}$, then since the latter is maximal, $\hat{\mathfrak{a}}$ is contained in $\mathfrak{p}_{i^*}$. But, since $\mathfrak{a} = \hat{\mathfrak{a}} * \prod_{i \in I} \mathfrak{p}_i^{t(i)}$, this implies that $\mathfrak{a}$ is contained in $\mathfrak{p}_{i^*}^{t(i^*)+1}$, contradicting the maximality of $t(i^*)$. This proves the claim and the lemma.

Theorem 5.9. *If $f(X)$ is irreducible as a polynomial in $\mathbb{Z}[X]$, then for any ideal $\mathfrak{a}$ of $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, $\mathfrak{a}$ is principal modulo $p^r \mathfrak{a}$, i.e. as an ideal of $\mathcal{R}/p^r \mathfrak{a}$.*

This theorem follows by applying lemmas 5.8 and 5.4. Details follow.

Proof. First consider the case that $\mathfrak{a}$ is co-prime to all $\mathfrak{p}_i$. Then, by lemma 5.4 and lemma 3.2 and lemma 3.1 (*iii*), we have

$$p^r\mathfrak{a} \;=\; \mathfrak{a} \prod_{i\in[m]} \mathfrak{p}_i^{r\cdot e_i}.$$

Then, by CRT,

$$\mathcal{R}/(p^r\mathfrak{a}) \;\cong\; \mathcal{R}/\mathfrak{a} * \prod_{i=1}^{m} \mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}.$$

So $\mathfrak{a}$ will be principal in $\mathcal{R}/(p^r\mathfrak{a})$, if it is principal in each of the component rings. Theorem 5.6, shows that $\mathfrak{a}$ is principal in $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i}$, and $\mathfrak{a}$ is trivially principal modulo $\mathfrak{a}$, and hence the lemma is proved in this case.

Otherwise, by lemmas 5.8 and 5.4, for any integer $r \geq 0$, we have, $\mathfrak{a} * (p)^r = \hat{\mathfrak{a}} * \prod_{i\in[m]} \mathfrak{p}_i^{r\cdot e_i + t_i}$, for some non-negative integers t_i. Also, $\hat{\mathfrak{a}}$ is co-prime to each $\mathfrak{p}_i$ and hence to each $\mathfrak{p}_i^{r\cdot e_i}$ (by lemma 3.2) . Also, by CRT,

$$\mathcal{R}/(p^r\mathfrak{a}) \;\cong\; \mathcal{R}/\hat{\mathfrak{a}} * \prod_{i=1}^{m} \mathcal{R}/\mathfrak{p}_i^{r\cdot e_i + t_i}.$$

Then, using theorem 5.6, $\hat{\mathfrak{a}}$ is principal modulo $\mathfrak{a} * (p)^r$ by employing CRT, just as in the simple case above where $\mathfrak{a}$ was co-prime to all $\mathfrak{p}_i$. By Theorem 5.6, each $\mathfrak{p}_i$ is also principal modulo $\mathfrak{p}_j^s$, for any s. So, we just need to show that $\mathfrak{p}_i$ is principal modulo $\hat{\mathfrak{a}}$. Since $\hat{\mathfrak{a}}$ is co-prime to $\mathfrak{p}_i$, there exists elements in $\alpha \in \mathfrak{p}_i$ and $\beta \in \hat{\mathfrak{a}}$, such that $\alpha + \beta = 1$. Thus, $\alpha = 1$ modulo $\hat{\mathfrak{a}}$, and hence $\mathfrak{p}_i$ is same as (1) modulo $\hat{\mathfrak{a}}$. Ideal $\hat{\mathfrak{a}}$ is also co-prime to $\mathfrak{p}_i$, and hence by the same argument as above, $\mathfrak{p}_i$ is same as (1) modulo $\hat{\mathfrak{a}}$.

We now prove the above lemma 5.8 (and hence theorem 5.9) without requiring that $\mathcal{R}$ be an integral domain; the requirement of being an integral domain was required to employ the corollary to Krull intersection theorem (corollary 3.6). The proof we give below (lemma 5.10) does not use this corollary, and is specific to the maximal ideals $\mathfrak{p}_i$ of the Noetherian ring $\mathcal{R}$.

For each $i \in [m]$, define an ideal $\bar{\mathfrak{p}}_i$ of $\mathcal{R}$ by

$$\bar{\mathfrak{p}}_i = \bigcap_{t=0}^{\infty} \mathfrak{p}_i^t.$$

It is a well-defined ideal of $\mathcal{R}$, because for every element α of $\mathcal{R}$, and every element β of $\bar{\mathfrak{p}}_i \subseteq \mathfrak{p}_i^0 = \mathcal{R}$, $\alpha\beta$ is in every $\mathfrak{p}_i^t$ $(t \geq 0)$, as all $\mathfrak{p}_i^t$ are ideals of $\mathcal{R}$.

Lemma 5.10. *For all $i \in [m]$, the ideal $\bar{\mathfrak{p}}_i \;=\; 0$*

A proof of this lemma can be found in Appendix A.

Extension to Product of Powers of Primes.

Theorem 5.11. *Let $q = \prod_j p_j^{r_j}$ be a product of powers of primes such that for every j, the p_j is Dedekind-special w.r.t. $f(X)$. If $f(X)$ is irreducible as a polynomial in $\mathbb{Z}[X]$, then for any ideal $\mathfrak{a}$ of $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, $\mathfrak{a}$ is principal modulo $q\mathfrak{a}$, i.e. as an ideal of $\mathcal{R}/q\mathfrak{a}$.*

The proof of this theorem is similar to the proof of above theorem 5.9, by iteratively computing $\hat{\mathfrak{a}}$ (using lemma 5.8) that is co-prime to all (p_j) and additionally observing that ideals (p) and (p') are co-prime for distinct primes p and p'.

6 Example Polynomial Rings and non-Bigenic Ideals

An ideal will be called *bigenic* if it can be genereated by two or less elements of the ring. In this section, we give natural examples of modular polynomials $(f(X), p)$ such that $f(X)$ modulo p is Dedekind-special, yet the ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ is a strict sub-ring of the ring of integers $\mathcal{O}_{\mathbf{K}}$ of the number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$. It is well known that in such a case $\mathcal{R}$ is not a Dedekind domain, and indeed all prime ideals of $\mathcal{R}$ that are not co-prime to the so-called *conductor ideal* of $\mathcal{R}$ are not invertible (see e.g. Theorem 6.1 in [Cona]). Another well-known property of Dedekind domains is that all its ideals are bigenic. However, it is not an easy task to show that some ideal of non-Dedekind-domain $\mathcal{R}$ is not bigenic. Although, examples exist of non-bigenic ideals in strict subrings (of rank n) of $\mathcal{O}_{\mathbf{K}}$ [Cona], these subrings are not the polynomial ring $\mathcal{R}$, and moreover these non-bigenic ideals have a diagonal Hermite normal form $\mathbb{Z}$-basis. We will show below a non-trivial ideal of $\mathcal{R}$ that requires a minimum of three generators.

Consider $f(X) = X^4 + 7$. By Eisenstein criterion, $f(X)$ is irreducible over $\mathbb{Q}$. Next, modulo 2, $f(X) = (X+1)^4 \pmod 2$, and in particular $f(X) = (X+1)^4 - 2 * t(X)$, where $t(X) = 2X^3 + 3X^2 + 2X - 3$. However, $(X+1) \mid t(X)$ modulo 2, and hence by Dedekind index theorem $2 \mid [\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$, and consequently $\mathcal{R}$ is a strict sub-ring of $\mathcal{O}_{\mathbf{K}}$ and hence not a Dedekind domain. We next check that for every prime p different from 2, $(f(X), p)$ is Dedekind-special. First, modulo $p = 7$, $f(X) = X^4 \pmod 7$, and $f(X) - X^4 = 7 * 1$. Since, X does not divide 1 modulo 7, $(f(X), 7)$ is Dedekind-special. Since, it is also known[10] that $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]^2$ divides Δ_f, the prime p can divide $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$ only if Δ_f has p^2 as a factor. In our example, using corollary 4.9, $\Delta_f = 4^4 7^3$, and hence only primes 2 and 7 can divide $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$, and hence for all other primes p, by Dedekind index theorem, $(f(Y), p)$ is also Dedekind-special. Thus, using CRT, we can base hardness of RLWE$_q$ for any integer q that is not even, on hard problems in lattices corresponding to ideals of non-Dedekind-domain $\mathcal{R}$. It is not difficult to see that the above argument can be generalized to arbitrary power-of-two degree $f(X)$.

Proposition 6.1. *The ideal $\mathcal{I} = (8, 4(X+1), 2(X+1)^2)$ of $\mathcal{R} = \mathbb{Z}[X]/(X^4+7)$ is not bigenic.*

[10] $\Delta_f = [\mathcal{O}_{\mathbf{K}} : \mathcal{R}]^2 \cdot \mathrm{disc}(\mathcal{O}_{\mathbf{K}})$, and $\mathrm{disc}(\mathcal{O}_{\mathbf{K}})$ is an integer.

Proof. Note that $\mathcal{I}$ as an ideal of $\mathcal{R}$ requires at least three generators if $\mathcal{I}_0 = (8, 4(X+1), 2(X+1)^2, X^4+7)$ as an ideal of $\mathbb{Z}[X]$ requires at least four generators. By a change of variable, i.e. setting $X+1 = Y$, and noting that $\mathbb{Z}[Y-1]$ is same as $\mathbb{Z}[Y]$, we are left with proving that $(8, 4Y, 2Y^2, Y^4-4Y^3+6Y^2-4Y+8)$ as an ideal of $\mathbb{Z}[Y]$ requires at least four generators. This ideal simplifies to $(8, 4Y, 2Y^2, Y^4)$, from which it is clear that the ideal needs at least four generators.

The above example has the issue that $1/2 \cdot \mathcal{I}$ which is also an ideal of $\mathcal{R}$ may or may not be bigenic, as the above simple proof does not extend to $1/2 \cdot \mathcal{I}$. A bigger issue is that $\mathcal{I}$, considered as a subset of $\mathbf{K} = \mathbb{Q}[X]/(X^4+7)$, is also as it is an ideal of the ring of integers $\mathcal{O}_{\mathbf{K}}$, and hence the corresponding lattice inherits all the algebraic properties of a Dedekind domain. In fact, we conjecture that for all ideals $\mathcal{R}$ of this particular $\mathbf{K}$, either the ideal is bigenic or it is as it an ideal of $\mathcal{O}_{\mathbf{K}}$. So, to have a more fruitful example we must look to a different number field, which we show next.

This example is inspired by [Conc, Example 4.16]. Consider the irreducible (over $\mathbb{Q}$) polynomial $f(X) = X^5 - 2^4 \cdot 3$, and the corresponding number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$. Consider $\beta = X^4/8$ as an element of $\mathbf{K}$. Its easy to check that $\beta^5 - 2 \cdot 3^4 = 0$, and hence $\beta \in \mathcal{O}_{\mathbf{K}}$. This also shows that $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ is not same as $\mathcal{O}_{\mathbf{K}}$, and hence is not integrally closed and consequently not a Dedekind domain. We now have an easy example of a non-bigenic ideal of $\mathcal{R}$.

Proposition 6.2. *The ideal $\mathcal{I} = (16, 4X, 2X^2)$ of $\mathcal{R} = \mathbb{Z}[X]/(X^5 - 2^4 \cdot 3)$ is not bigenic. Further this ideal of $\mathcal{R}$ is not as it is an ideal of ring of integers of $\mathbf{K} = \mathbb{Q}[X]/(X^5 - 2^4 \cdot 3)$.*

Proof. The proof is similar to the previous proposition, noting that $\mathcal{I}$ as an ideal of $\mathcal{R}$ requires three generators if $\mathcal{I}_0 = (16,\ 4X,\ 2X^2,\ X^5 - 48)$ as an ideal of $\mathbb{Z}[X]$ requires at least four generators. But, $\mathcal{I}_0$ is same as $(16,\ 4X,\ 2X^2,\ X^5)$, which is easily seen to require four generators as an ideal of $\mathbb{Z}[X]$.

To check that $\mathcal{I}$ is not an ideal of $\mathcal{O}_{\mathbf{K}}$. Recall, $\beta = x^4/8$ is in $\mathcal{O}_{\mathbf{K}}$. We just show that $4X \cdot \beta$ is not in $\mathcal{I}$, and hence $\mathcal{I}$ is not closed under multiplication by $\mathcal{O}_b K$. indeed, we have $4X \cdot \beta = X^5/2 = 24$ which is same as 8 modulo 16. Since 8 is not in the ideal $\mathcal{I}$, this completes the proof.

This example is still not satisfying for two reasons. First, we should really show that $1/2 \cdot \mathcal{I}$ is not bigenic, for if this latter ideal was bigenic, a rational scaling of $\mathcal{I}$ becomes bigenic. Second, the HNF $\mathbb{Z}$-basis of this ideal is diagonal. Fortunately, the ideal in the following proposition has strong properties, although the proof is more involved now.

Proposition 6.3. *The ideal $\mathcal{I} = (8, 2(X+2), X(X+2)$ of $\mathcal{R} = \mathbb{Z}[X]/(X^5 - 48)$ has the following properties*

(i) *$\mathcal{I}$ is not bigenic,*
(ii) *no rational scaling of $\mathcal{I}$ that is an ideal of $\mathcal{R}$ is bigenic,*
(iii) *no rational scaling of $\mathcal{I}$ is a fractional ideal of $\mathcal{O}_{\mathbf{K}}$,*
(iv) *the HNF $\mathbb{Z}$-basis of $\mathcal{I}$ is not diagonal.*

Proof. We focus on proving (i), as the rest will follow easily.

Now, assume to the contrary that this ideal is bigenic and generated by $L0 = (\ell_1, \ell_2)$, and as ideals of $\mathbb{Z}[X]/(X^5 - 48)$, $L0 = \mathcal{I}$. Both ℓ_1 and ℓ_2 must be in the $\mathbb{Z}$-span of $\mathbb{Z}$-basis of the ideal $\mathcal{I}$, which is depicted below by concatenating the circulant matrices of $8, 2X + 4$ and $X^2 + 4$. We also compute its reduced Hermite normal form (HNF).

$$\text{HNF}\begin{pmatrix} 4 & 0 & 0 & 48 & 0 & 4 & 0 & 0 & 0 & 96 & 8 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 48 & 2 & 4 & 0 & 0 & 0 & 0 & 8 & 0 & 0 & 0 \\ 1 & 0 & 4 & 0 & 0 & 0 & 2 & 4 & 0 & 0 & 0 & 0 & 8 & 0 & 0 \\ 0 & 1 & 0 & 4 & 0 & 0 & 0 & 2 & 4 & 0 & 0 & 0 & 0 & 8 & 0 \\ 0 & 0 & 1 & 0 & 4 & 0 & 0 & 0 & 2 & 4 & 0 & 0 & 0 & 0 & 8 \end{pmatrix} = \begin{pmatrix} 8 & 4 & 4 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

From the HNF it is clear that ℓ_1 can be written as $a_1X^4 + b_1X^3 + c_1(X^2 + 4) + d_1(2X + 4) + e_1 \cdot 8$ and similarly, ℓ_2 can be written as $a_2X^4 + b_2X^3 + c_2(X^2 + 4) + d_2(2X + 4) + e_2 \cdot 8$, where all of $a_1, ...e_1, a_2, ..., e_2$ are in $\mathbb{Z}$.

Next, note that it suffices to prove that $L1 = (\ell_1, \ell_2, X^5, 48)$ as ideal of $\mathbb{Z}[X]$ does not contain all three of $8, 2X + 4$, and $X^2 + 4$. We will instead prove something stronger that $L2 = (\ell_1, \ell_2, X^4, 16)$ as ideal of $\mathbb{Z}[X]$ does not contain all three of $8, 2X + 4$, and $X^2 + 4$.

Further, since we have included X^4 in $L2$, we can now assume w.l.o.g. that a_1 and a_2 are zero. Further, using Euclidean algorithm, w.l.o.g. assume that c_2 is zero. Thus, $\ell_1 = b_1X^3 + c_1(X^2 + 4) + d_1(2X + 4) + e_1 \cdot 8$, and $\ell_2 = b_2X^3 + d_2(2X + 4) + e_2 \cdot 8$. Further, since 16 is included in $L2$, e_1 and e_2 can just be restricted to $\{0, 1\}$.

Now, since $L2$ must generate $x^2 + 4$, and given that $b_1, ...e_1, b_2, ..., e_2$ are just integers, it is clear that $c_1 = 1 \bmod 16$. Also, it is clear that both e_1 and e_2 cannot be zero, for otherwise 8 cannot be generated. Since c_1 is non-zero, to generate $2x + 4$, modulo 16, one can only use ℓ_2 (and not use ℓ_1), and hence $d_2 = 1 \bmod 16$, and $b_2, e_2 = 0 \bmod 16$, which as argued above just means that $e_2 = 0$, and hence $e_1 = 1$. But, this means $X^2 + 4$ cannot be generated from $L2$. That completes the proof of (i)

We now go on to prove (ii)-(iv). We have already shown above that the HNF of the ideal $\mathcal{I}$ is not diagonal, so that proves (iv). Since, the ideal $\mathcal{I}$ contains $X^2 + 4$, any rational scaling of $\mathcal{I}$ that keeps it as a subset of $\mathcal{R}$ must be an integer scaling. However, the above proof of non-bigenic nature of $\mathcal{I}$ easily extends to any integer scaling of $\mathcal{I}$.

For (iii), we first show that $\mathcal{I}$ by itself (i.e. without any scaling) is not an ideal of $\mathcal{O}_{\mathbf{K}}$. Recall, $\beta = x^4/8$ is in $\mathcal{O}_{\mathbf{K}}$. We just show that $(2X + 4) \cdot \beta$ is not in $\mathcal{I}$, and hence $\mathcal{I}$ is not closed under multiplication by $\mathcal{O}_bK$. To begin with, note that $(X^2 + 4)(X^2 - 4) = (X^4 - 16)$ is in the ideal $\mathcal{I}$. Using this, we have $(2X + 4) \cdot \beta = X^5/4 + X^4/2 = 12 + X^4/2 = 12 + 8$ (modulo $\mathcal{I}$) which is same as 4 modulo 16. Since 4 is not in the ideal $\mathcal{I}$ (of $\mathcal{R}$), this completes the proof.

Next, consider the set $\frac{p}{q} \cdot \mathcal{I}$, for co-prime integers p, q. Again, we just show that $\frac{p}{q}(2X + 4) \cdot \beta$ is not in $\frac{p}{q} \cdot \mathcal{I}$. But this is same as checking that $(2X + 4) \cdot \beta$ is not in $\cdot\mathcal{I}$.

7 Randomized Algorithm to Compute a Generator of Ideal $\mathfrak{a}$ modulo $p^r\mathfrak{a}$

In this section we restrict ourselves to the setting of Section 5. Given an ideal $\mathfrak{a}$ described by a set of generators $\{\gamma_i\}_{i\in[n]}$ in $\mathcal{R}$ or a $\mathbb{Z}$-basis $\boldsymbol{B}(\mathfrak{a})$, we wish to compute a generator of the principal ideal $\mathfrak{a}$ modulo $p^r\mathfrak{a}$, which is principal by theorem 5.9.

We show that the following simple and efficient randomized algorithm computes such a generator with non-negligible probability[11].

Algorithm 1 FindGen

```
Input: A $\mathbb{Z}$-basis $\boldsymbol{B}$ for an ideal $\mathfrak{a}$ of $\mathcal{R}$.
Output: A single generator $a(X)$ for ideal $\mathfrak{a}$ mod $p^r\mathfrak{a}$.
Pick a random $n$-vector $\boldsymbol{\rho}$ with component polynomials $\rho_k$ ($k \in [n]$) chosen uniformly and independently from $\mathbb{Z}_p[X]/(f(X)) = \mathcal{R}/(p)$.
View the $n$ columns of $\boldsymbol{B}$ as $n$ polynomials $\gamma_k \in \mathcal{R}$ ($k \in [n]$).
Compute $a(X) = \sum_{k=1}^{m} \rho_k * \gamma_k$ in $\mathcal{R}$.
Output $a(X)$
```

7.1 Correctness

Lemma 7.1. *The algorithm* **FindGen** *outputs a generator $a(X)$ of $\mathfrak{a}$ modulo $p^r\mathfrak{a}$ with probability at least $\prod_{i\in[m]}(1 - 2/p^{d_i})$, where d_i is the degree of the irreducible (modulo p) polynomials $h_i(X)$ such that $f(X) = \prod_{i\in[m]} h_i(X)^{e_i}$ in $\mathbb{Z}_p[X]$.*

Proof. By lemma 5.8 and lemma 5.4, we have for any integer $r \geq 0$, $\mathfrak{a} * (p)^r = \hat{\mathfrak{a}} * \prod_{i\in[m]} \mathfrak{p}_i^{r\cdot e_i+t_i}$, where $\hat{\mathfrak{a}}$ is co-prime to every $\mathfrak{p}_i$ ($i \in [m]$). Thus, noting that all the $\mathfrak{p}_i$ are prime (lemma 5.1), and by employing CRT, we have that the ring $\mathcal{R}/p^r\mathfrak{a}$ is isomorphic to $\mathcal{R}/\hat{\mathfrak{a}} * \prod_{i\in[m]} \mathcal{R}/\mathfrak{p}_i^{r\cdot e_i+t_i}$. Since $\mathfrak{a}$ is zero modulo $\hat{\mathfrak{a}}$, we can focus on $\mathfrak{a}$ modulo $\mathfrak{p}_i^{r\cdot e_i+t_i}$, for each $i \in [m]$.

First, note that each of the n columns of $\boldsymbol{B}$ can be viewed as n polynomials $\gamma_k \in \mathcal{R}$ ($k \in [n]$), such that the γ_k collectively form a set of generators (over $\mathcal{R}$) of $\mathfrak{a}$. Recall, $a(X)$ computed in the algorithm is just $\sum_k \rho_k\gamma_k$.

Fix an $i \in [m]$. View each of the elements γ_k ($k \in [n]$) also as elements of the quotient ring $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i+t_i}$, and the randomly chosen elements ρ_k as also elements in $\mathcal{R}/\mathfrak{p}_i^{r\cdot e_i+t_i}$. Denote $\mathfrak{a}$ reduced modulo $\mathfrak{p}_i^{r\cdot e_i+t_i}$ by $\mathfrak{a}_i$. By Theorem 5.6, $\mathfrak{a}_i$ is principal and is generated by a finite power of g (including $1 = g^0$), where g is either p or $h_i(X)$ (depending on whether e_i is one or greater than one resp.). Similarly, each γ_k (the generators of $\mathfrak{a}$) is itself generated by a finite power of

[11] This is similar to the known randomized algorithms that find a second generator for an ideal of a Dedekind domain, given a basis and a first generator (see e.g. [Coh93]).

g modulo $\mathfrak{p}_i^{t_i}\mathfrak{s}^r$, say the power is $v_{k,i} \geq 0$. Hence, $\mathfrak{a}_i$ is generated by $g^{v_i^*}$, where $v_i^* = \min\{v_{k,i} \ : \ k \in [n]\}$.

Note, γ_k can be written as $\alpha_{k,i} g^{v_{k,i}}$ modulo $\mathfrak{p}_i^{r \cdot e_i + t_i}$, where $\alpha_{k,i}$ is not in $\mathfrak{p}_i = (h_i(X), p)$. Then, $\sum_k \rho_k \gamma_k$ modulo $\mathfrak{p}_i^{r \cdot e_i + t_i}$ can be written as $g^{v_i^*} * \sum_k \rho_k \alpha_{k,i} g^{v_{k,i} - v_i^*}$. Note, at least for one $k \in [n]$, $v_{k,i} - v_i^*$ is zero. So, let I_i be the non-empty set of indices, subset of $[n]$, such that $v_{k,i} - v_i^*$ is zero.

Since by lemma 5.1, $\mathfrak{p}_i$ is a maximal ideal of $\mathcal{R}$ and hence every element of $\mathcal{R}$ not in $\mathfrak{p}_i$ is invertible modulo $\mathfrak{p}_i$, we need to show that with high probability, over the random choices of $\{\rho_k\}_k$, *for all* $i \in [m]$, $\sum_{k \in I_i} \rho_k \alpha_{k,i}$ is not zero modulo $\mathfrak{p}_i$. Note that for $k \notin I_i$, the quantities $\rho_k \alpha_{k,i} g^{v_{k,i} - v_i^*}$ are in $(g) \subseteq (h_i(X), p)$, so the full sum (over all $k \in [n]$) will be non-zero modulo $(h_i(X), p) = \mathfrak{p}_i$ and hence invertible.

To calculate this probability, we first note that $\mathbb{Z}[X]/(h_i(X), p)$ is a finite field, more precisely $\mathrm{GF}(p^{d_i})$, as $h_i(X)$ is irreducible modulo p, with d_i being the degree of $h_i(X)$. Thus, we can view each of ρ_k and $\alpha_{k,i}$ as element of this field (by reducing mod p). We have already seen that $\alpha_{k,i}$ is non-zero in this field, as it is not in $(h_i(X), p)$. However, a random choice of ρ_k in $\mathbb{Z}_p[X]/(f(X))$ may lead ρ_k it to be zero modulo $(h_i(X), p)$, although this probability is small, as we next show.

First, note that $\mathbb{Z}_p[X]/(f(X)) = \mathcal{R}/(p)$. Then, by employing CRT and theorem 5.5, ρ_k is uniformly and *independently* distributed in the rings $\mathcal{R}/\mathfrak{p}_i^{e_i}$. Further, by lemma 5.1($i$), $\mathfrak{p}_i^{e_i} = \mathfrak{s}_i = (p, h_i(X)^{e_i})$. Thus, $\mathcal{R}/\mathfrak{p}_i^{e_i} = \mathbb{Z}[X]/\ (f(X),\ p,\ h_i(X)^{e_i})$, which is same as $\mathbb{Z}[X]/(p, h_i(X)^{e_i})$.

Hence ρ_k is zero modulo $\mathfrak{p}_i$ only if it is a multiple of $h_i(X)$. Since all (canonically represented) polynomials in $\mathfrak{s}_i$ have degree at most $d_i * e_i - 1$, there are at most $p^{d_i * e_i}$ polynomials. Similarly, all canonical polynomials in $\mathfrak{s}_i$ that are a multiple of $h_i(X)$ are at most $p^{d_i * (e_i - 1)}$. This proves that the probability that ρ_k is zero in $\mathrm{GF}(p^{d_j})$ is at most $1/p^{d_i}$. Moreover, conditioned on ρ_k being non-zero, the probability that it is c for some non-zero c in $\mathrm{GF}(p^{d_i})$ is same regardless of c, as number of elements in the coset of c in $\mathfrak{s}_i$ is same for all c. Thus, conditioned on ρ_k being non-zero, ρ_k is uniformly distributed in $\mathrm{GF}(p^{d_i})$.

Thus, probability that $\beta_i = (\sum_{k \in I_i} \rho_k \alpha_{k,i} \bmod \ (h_i(X), p))$ is zero, i.e. zero in $\mathrm{GF}(p^{d_i})$, is at most $1/p^{d_i * |I_i|}$ plus $1/p^{d_i}$, which is at most $2/p^{d_i}$. Since, ρ_k are independently distributed in the various rings $\mathbb{Z}[X]/\mathfrak{s}_i$, the probability that all of these m quantities β_i are non-zero is at least $\prod_{i \in [m]}(1 - 2/p^{d_i})$, which is also a lower bound on the probability that $a(X)$ is a generator of $\mathfrak{a}$ modulo $p^r\mathfrak{a}$.

Extension to Product of Powers of Primes. Let $q = \prod_j p_j^{r_j}$ be a product of powers of primes such that for every j, the modular polynomial $(f(X), p_j)$ is Dedekind-special. The above algorithm can be correctly extended by choosing ρ_i randomly and independently from $Z_{q'}[X]/(f(X))$ where $q' = \prod_j p_j$. The probability of success in this case is at least $\prod_j \prod_{i \in [m_j]}(1 - 2/p_j^{d_{j,i}})$, where $d_{j,i}$ is the degree of the m_j irreducible polynomials $h_{j,i}(X)$ (modulo p_j) such that $f(X) = \prod_{i \in [m]} h_{j,i}(X)^{e_{j,i}}$ in $\mathbb{Z}_p[X]$.

Extension to Arbitrary q without known-factorization. If the factorization of q is not known, and say $q = \prod_j p_j^{r_j}$ as above, we can still use the above algorithm, but this time by choosing ρ_i randomly and independently modulo $\mathbb{Z}_q[X]/(f(X))$. In the proof of lemma 7.1, again using CRT and focusing on individual primes, say p_j, ρ_k is now uniformly and independently distributed in $\mathbb{Z}[X]/\mathfrak{p}_i^{e_i r_j}$. By a similar argument as in the proof of lemma 5.1(i), this ring is isomorphic to $\mathbb{Z}[X]/(p, h_i(X)^{e_i r_j})$. By the probability analysis in the lemma 7.1 above, the probability of success remains the same as in the known factorization case above.

Boosting the Probability of Success. One can boost the probability of finding a generator of $\mathfrak{a}$ modulo $q\mathfrak{a}$ by repeating the above algorithm, but to stop the repetition we need an efficient test that $a(X)$ as computed is indeed a generator. But, this is same as checking $(\mathfrak{a}, q\mathfrak{a}) = (a(X), q\mathfrak{a})$, which can be efficiently tested by computing the Hermite normal form of $\boldsymbol{B}$ (the given $\mathbb{Z}$-basis of $\mathfrak{a}$) and the Hermite normal form of $[\boldsymbol{C}_a \mid q\boldsymbol{B}]$, and checking for equality. Here, $\boldsymbol{C}_a$ is the circulant matrix of $a(X)$ in $\mathbb{Z}[X]/(f(X))$.

8 Hardness of Decisional RLWE

In this section, by default, we focus on a degree-n monic polynomial $f(X)$ and an integer $q \geq 2$ where $(f(X), q)$ is *Dedekind-special*. Let $\mathcal{R}_\mathbb{R} = \mathbb{R}[X]/(f(X))$.

First we give out the same distribution of error distributions as in [PRS17], which we will use in the following reduction.

Definition 8.1 (Error Distribution). *Fix arbitrary $s(n) = \omega(\sqrt{\log(n)})$. For $\alpha > 0$, a distribution sampled from Υ_α is an elliptical Gaussian distribution $D_\mathbf{r}$, where $\mathbf{r} \in G$ is sampled as follow: for $i = 0, \ldots, s_1 - 1$, sample $x_i \in D_1$ and set $r_i^2 = \alpha^2(x_i^2 + s^2(n))/2$, for $i = s_1, \ldots, s_1 + s_2 - 1$, sample x_i, y_i from $D_{1/\sqrt{2}}$ and set $r_i^2 = r_{i+s_2}^2 = \alpha^2(x_i^2 + y_i^2 + s^2(n))/2$.*

Definition 8.2 (RLWE Distribution). *Let $\boldsymbol{V}$ be the Vandermonde matrix of the modulo polynomial $f(x)$. For $\mathbf{s} \in \mathcal{R}_q^\vee$ and an error distribution ψ over $\mathcal{R}_\mathbb{R}$, we define the RLWE distribution $\mathcal{A}_{\mathbf{s},\psi}$ over $\mathcal{R}_q \times \mathcal{R}_\mathbb{R}/\mathcal{R}^\vee$ as $\left(\mathbf{a}, \mathbf{b} = \mathbf{a} * \mathbf{s}/q + \boldsymbol{V}^{-1}\mathbf{e} \bmod \mathcal{R}^\vee\right)$ where $\mathbf{e}$ is sampled from ψ, $\mathbf{a}$ is uniform over $\mathcal{R}_q$.*

Definition 8.3 ((Average-case) Decisional RLWE Problem). *Let Υ_α be a distribution over family of error distributions, each over $\mathbb{R}[X]/(f(X))$. The* average-case decisional RLWE problem*, $\mathit{RLWE}_{q,\Upsilon_\alpha}$ is to distinguish (with non-negligible advantage) between independent samples from $A_{\mathbf{s},\psi}$ for a random choice of uniform $s \in \mathcal{R}_q^\vee$ and $\psi \in \Upsilon_\alpha$ and the same number of uniformly random and independent samples from $\mathcal{R}_q \times \mathcal{R}_\mathbb{R}/\mathcal{R}^\vee$.*

Let $\mathcal{R}$-DGS_γ be the discrete Gaussian sampling problem DGS_γ when restricted to the ideal lattices on the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(f(X))$.

Theorem 8.1. *Let $\alpha = \alpha(n) \in (0,1)$, $q = q(n) \geq 2$ be an integer and $f(x)$ be any degree-n monic polynomial where $(f(X), q)$ is Dedekind-special. Let $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ be a polynomial ring. If $\alpha q \geq 2 \cdot \omega(1)$, for some negligible $\epsilon = \epsilon(n)$, there is a probabilistic polynomial-time quantum reduction from $\mathcal{R}$-DGS_γ to (average case, decisional) $\mathsf{RLWE}_{q,\Upsilon_\alpha}$, where*

$$\gamma = \max\left\{\eta_\epsilon(\mathcal{L}(\mathcal{I})) \cdot (\sqrt{2}/\alpha) \cdot \omega(1), \sqrt{2n}/\lambda_1(\mathcal{L}(\mathcal{I})^\vee)\right\}$$

Note that $\eta_\epsilon(\mathcal{L}) > \omega(\sqrt{\log(n)})/\lambda_1(\mathcal{L}^\vee)$. Using known reduction [Reg06], this immediately implies a polynomial-time quantum reduction from SIVP_γ to (average-case, decision) $\mathsf{RLWE}_{q,\Upsilon_\alpha}$ for any $\gamma \leq \max\left\{\omega(\sqrt{n\log(n)}/\alpha, \sqrt{2}n\right\}$.

In case of spherical error, same as [PRS17, Section 7] we have

Corollary 8.2. *With the same notation as Theorem 8.1, there's a polynomial time quantum reduction from $\mathcal{R}$-DGS_γ to (average-case, decisional) RLWE_{q,D_ξ} using ℓ samples, where*

$$\gamma = \max\left\{\eta_\epsilon(\mathcal{L}(\mathcal{I})) \cdot (\sqrt{2}/\xi) \cdot \left(\frac{n\ell}{\log(n\ell)}\right)^{\frac{1}{4}} \cdot \omega(\sqrt{\log(n)}), \sqrt{2n}/\lambda_1(\mathcal{L}(\mathcal{I})^\vee)\right\},$$

as long as $\xi q \geq \left(\frac{n\ell}{\log(n\ell)}\right)^{\frac{1}{4}} \cdot \omega(\sqrt{\log(n)})$.

Our proof to theorem 8.1 will be exactly the same as [PRS17, Theorem 6.2], that starts with a discrete Gaussian sampler with very large radius, and iteratively applys the following lemma 8.3.

Definition 8.4. *For $r > 0$, $\zeta > 0$ and $T \geq 1$, define $W_{r,\zeta,T}$ as the set of cardinality $(s_1 + s_2) \cdot (T + 1)$ containing for each $i = 0, \ldots, s1 + s2 - 1$ and $j = 0, \ldots, T$ the vector $\mathbf{r}_{i,j}$ which is equal to r in all coordinates except in the i-th, and the $(i + s2)$-th if $i \geq s_1$, where it is equal to $r \cdot (1 + \zeta)^j$.*

Lemma 8.3. *There's an efficient quantum algorithm that, given an oracle that solves $\mathsf{RLWE}_{q,\Upsilon_\alpha}$, an ideal $\mathcal{I} \subseteq \mathcal{R}$, a number $r \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{L}(\mathcal{I}))$ and $r' = r \cdot \omega(1)/(\alpha q) \geq \sqrt{2n}/\lambda_1(\mathcal{L}(\mathcal{I})^\vee)$, polynomially many samples from discrete Gaussian distribution $D_{\mathcal{L}(\mathcal{I}),\mathbf{r}}$ for each $\mathbf{r} \in W_{r,\zeta,T}$ (for some $\zeta = 1/poly(n)$ and $T = poly(n)$), and a vector $\mathbf{r'} \geq r'$, outputs an independent sample from $D_{\mathcal{L}(\mathcal{I}),\mathbf{r'}}$.*

As in [PRS17, Lemma 6.5], This iterative step is given by combining the following two parts: a classical one in lemma 8.4 that use a discrete Gaussian sampler and a RLWE oracle to solve the Gaussian Decoding Problem (GDP), and a quantum one in lemma 8.5 that use this GDP solver to provide discrete Gaussian samples with smaller radius.

Lemma 8.4. *There's a probabilistic (classical) polynomial time algorithm that, taking an oracle that solves $\mathsf{RLWE}_{q,\Upsilon_\alpha}$ for $\alpha \in (0,1)$ and integer $q > 2$, an ideal $\mathcal{I} \in \mathcal{R}$, a parameter $r \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{L}(\mathcal{I}))$, and polynomially many samples from discrete Gaussian $D_{\mathcal{L}(\mathcal{I}),\mathbf{r}}$ for each $\mathbf{r} \in W_{r,\zeta,T}$ for some $\zeta = 1/poly(n)$ and $T = poly(n)$, solves $\mathsf{GDP}_{\mathcal{L}(\mathcal{I})^\vee,g}$ for any $g = o(1) \cdot \alpha q/(2r)$.*

Lemma 8.5 ([PRS17, Lemma 6.7]). *There is an efficient quantum algorithm that, given any n-dimensional lattice $\mathcal{L}$, a number $g < \frac{\lambda_1(\mathcal{L}^\vee)}{2\sqrt{2n}}$, a vector $\mathbf{r} \geq 1$, and an oracle that solves $\mathsf{GDP}_{\mathcal{L}^\vee,g}$ with all but negligible probability, outputs a sample from $D_{\mathcal{L},\frac{\mathbf{r}}{2g}}$.*

The proof of lemma 8.4 follows exactly from [PRS17, Lemma 6.6], except for two problems:

1. The core reduction from Gaussian Decoding Problem to RLWE in [PRS17, Lemma 6.8] requires the underlying ring to be a dedekind domain, which is not true in our case (see section 6). We provide such counterpart in lemma 8.6.
2. We need a similar lemma as in [PRS17, Lemma 6.9] for non-maximal orders (i.e. orders that are not the ring of integers) of number fields, which says that any elliptical Gaussian whose parameters' product is sufficiently large is "smooth" modulo an ideal. We provide a proof in lemma 8.9.

Lemma 8.6. *There's an efficient algorithm that, takes as input an integer $q \geq 2$, a dual ideal lattice $\mathcal{L}(\mathcal{I})^\vee$ where $\mathcal{I}$ is an ideal in $\mathcal{R}$, a coset $\mathbf{e} + \mathcal{L}(\mathcal{I})^\vee$ with a bound $d \geq ||\mathbf{e}||_\infty$, a parameter $r \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{L}(\mathcal{I}))$ and samples from $D_{\mathcal{L}(\mathcal{I}),\mathbf{r}}$ for some $\mathbf{r} \geq r$. It outputs samples that are within negligible statistical distance from the RLWE distribution $A_{\mathbf{s},\mathbf{r}'}$ for a uniformly random $\mathbf{s} \in \mathcal{R}_q^\vee$, where $(\mathbf{r}_i')^2 = (\mathbf{r}_i|\mathbf{e}_i|/q)^2 + (rd/q)^2$.*

To prove this lemma 8.6, we follow the standard techniques as in [PRS17, Lemma 6.8] which is a slight generalization over [LPR10, Lemma 4.7], elaborated as below.

Proof Sketch. First sample a random $\hat{\mathbf{z}} = \boldsymbol{V}\mathbf{z}$ from the discrete Gaussian $D_{\mathcal{L}(\mathcal{I}),\mathbf{r}}$ where $\mathbf{z} \in \mathcal{I}$. Because $\mathbf{r} \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{L}(\mathcal{I}))$, by smoothing lemma 2.1, the distribution of ($\mathbf{z} \bmod q\mathcal{I}$) is within a negligible distance from uniform distribution over $\mathcal{I}/q\mathcal{I}$. Also let $\mathbf{e}'$ be an independent sample from the continuous Gaussian $D_{\alpha/\sqrt{2}}$.

Now, for any element $\boldsymbol{V}\mathbf{y} = \hat{\mathbf{y}} = \mathbf{e} + \hat{\mathbf{x}} \in \mathbf{e} + \mathcal{L}(\mathcal{I})^\vee$, where $\hat{\mathbf{x}} = \boldsymbol{V}\mathbf{x} \in \mathcal{L}(\mathcal{I})^\vee$, we could directly provide a "RLWE sample" from $\mathcal{I}/q\mathcal{I} \times \mathcal{R}_\mathbb{R}/\mathcal{R}^\vee$ as

$$\left(\mathbf{z} \bmod q\mathcal{I}, \mathbf{z} * \mathbf{y}/q + \mathbf{e}' \bmod \mathcal{R}^\vee = \frac{\mathbf{z} * \mathbf{x}}{q} + \frac{1}{q}\boldsymbol{C}_z\boldsymbol{V}^{-1}\mathbf{e} + \mathbf{e}' \bmod \mathcal{R}^\vee\right).$$

for some secret $\mathbf{x} \in \mathcal{I}^\vee/q\mathcal{I}^\vee$. To jump out of the ideal, we use lemma 8.7, a counterpart of clearing lemma of [LPR10, Lemma 2.15] for non dedekind domains, that gives (i) an invertible and efficiently computable bijection $\psi : \mathcal{I}/q\mathcal{I} \to \mathcal{R}/q\mathcal{R}$, and (ii) an efficiently invertible and computable bijection $\phi : \mathcal{I}^\vee/q\mathcal{I}^\vee \to \mathcal{R}^\vee/q\mathcal{R}^\vee$, with the additional property that $\mathbf{z} * \mathbf{x} = \psi(\mathbf{z}) * \phi(\mathbf{x})$. Therefore the final RLWE distribution would be over $\mathcal{R}_q \times \mathcal{R}_\mathbb{R}/\mathcal{R}^\vee$ as

$$\left(\psi(\mathbf{z} \bmod q\mathcal{I}), \mathbf{z} * \mathbf{y}/q + \mathbf{e}' \bmod \mathcal{R}^\vee = \frac{\psi(\mathbf{z}) * \phi(\mathbf{x})}{q} + \frac{1}{q}\boldsymbol{C}_z\boldsymbol{V}^{-1}\mathbf{e} + \mathbf{e}' \bmod \mathcal{R}^\vee\right)$$

for some secret $\phi(\mathbf{x}) \in \mathcal{R}^\vee/q\mathcal{R}^\vee$. Note that since ψ is invertible, $\psi(\mathbf{z} \bmod q\mathcal{I})$ is almost uniform over $\mathcal{R}/q\mathcal{R} = \mathcal{R}_q$.

Moreover, if we sample $\mathbf{e}$ as in $\mathsf{GDP}_{\mathcal{L}(\mathcal{I})^\vee,g}$ where $g = \alpha q/(\sqrt{2}r)$, the distribution of $\left(\frac{1}{q}\boldsymbol{C}_z\boldsymbol{V}^{-1}\mathbf{e} + \mathbf{e}'\right)$ will be exactly Υ_α, as in [PRS17, Lemma 6.8]. Then we complete the proof by applying the standard technique to randomize the secret as in [Reg10, Lemma 3.2]

The following lemma is an extension of an important technical lemma from [LPR10, Lemma 2.15], which is informally referred to as the *ideal clearing lemma*, and is the key to extending Regev's LWE-hardness [Reg10] to the Ring-LWE setting. Our proof of the lemma is quite different from the proof in [LPR10] as it extends to some non dedekind domains, and hence cannot use the standard prime ideal factorization and ideal invertibility guaranteed for dedekind domains. The mapping ϕ we obtain below is actually more (computationally) efficiently invertible than the corresponding mapping in [LPR10]. Since, for cyclotomic number fields, the ring of integers is same as the polynomial ring $\mathcal{R}$, this more efficient mapping can be employed.

Lemma 8.7. (**Ideal Clearing Lemma**) *For any integer q that is Dedekind-special for $f(X)$, given a $\mathbb{Z}$-basis $\boldsymbol{B}(\mathcal{I})$ for ideal $\mathcal{I} \subseteq \mathcal{R}$,*

(i) *there is an efficiently computable $\mathcal{R}$-module isomorphism $\psi : \mathcal{I}/q\mathcal{I} \to \mathcal{R}/q\mathcal{R}$,*

(ii) *there is an efficiently invertible $\mathcal{R}$-module isomorphism $\phi : \mathcal{I}^\vee/q\mathcal{I}^\vee \to \mathcal{R}^\vee/q\mathcal{R}^\vee$, such that*

(iii) *for any $\mathbf{z} \in \mathcal{I}/q\mathcal{I}$ and $\mathbf{x} \in \mathcal{I}^\vee/q\mathcal{I}^\vee$, their polynomial product satisfies*

$$\mathbf{z} * \mathbf{x} \equiv \psi(\mathbf{z}) * \phi(\mathbf{x}) \pmod{q\mathcal{R}^\vee}$$

Proof. By Algorithm FindGen (lemma 7.1), we can efficiently find a $\mathbf{g}$ that is a generator of $\mathcal{I}$ modulo $q\mathcal{I}$. In other words, as ideals, $\mathcal{I} = (\mathbf{g}) + q\mathcal{I}$. Thus, $\mathbf{g} \in \mathcal{I}$. This implies that $\mathbf{g} = \boldsymbol{B}(\mathcal{I})\mathbf{d}^{(0)}$ for some integer-vector $\mathbf{d}^{(0)}$. Similarly, the coefficient representation of $g(X) * X^i$, is $\boldsymbol{B}(\mathcal{I})\mathbf{d}^{(i)}$ for some integer vector $\mathbf{d}^{(i)}$. Thus,

$$\boldsymbol{C}_g = \boldsymbol{B}(\mathcal{I}) \cdot \boldsymbol{D}, \tag{2}$$

where $\boldsymbol{D}$ is an integer matrix (with columns $\mathbf{d}^{(i)}$).

Also, we have that every column of $\boldsymbol{B}(\mathcal{I})$ is generated by $\boldsymbol{C}_g$ mod $q\mathcal{I}$, or mod $q\boldsymbol{B}(\mathcal{I})$. Thus,

$$\boldsymbol{B}(\mathcal{I}) = \boldsymbol{C}_g\boldsymbol{U} + q \cdot \boldsymbol{B}(\mathcal{I})\boldsymbol{T} \tag{3}$$

for some integer, matrices $\boldsymbol{U}$ and $\boldsymbol{T}$. Equivalently,

$$\boldsymbol{B}(\mathcal{I}) \cdot (I - q\boldsymbol{T}) = \boldsymbol{C}_g\boldsymbol{U}, \tag{4}$$

or, since $\boldsymbol{C}_g$ is full-ranked, we have

$$\boldsymbol{C}_g^{-1}\boldsymbol{B}(\mathcal{I}) \cdot (I - q\boldsymbol{T}) = \boldsymbol{U}. \tag{5}$$

We next show that $\boldsymbol{D} \cdot \boldsymbol{U} = I \pmod{q}$. Note, from (2) and observing that $\boldsymbol{B}(\mathcal{I})$ is full-ranked, $\boldsymbol{D} = \boldsymbol{B}(\mathcal{I})^{-1}\boldsymbol{C}_g$. Left multiplying both sides of (5) by $\boldsymbol{D}$, we get $(I - q\boldsymbol{T}) = \boldsymbol{D} * \boldsymbol{U}$, and hence

$$\boldsymbol{D} \cdot \boldsymbol{U} = I \pmod{q}. \tag{6}$$

Now, consider the following two mappings for claims (i)-(iii). For any $\mathbf{z} \in \mathcal{I}$ and $\mathbf{x} \in \mathcal{I}^\vee$, define

$$\psi(\mathbf{z}) = \mathbf{a} = \boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} \pmod{q\mathcal{R}} \tag{7}$$

$$\phi(\mathbf{x}) = \mathbf{g} * \mathbf{x} \pmod{q\mathcal{R}^\vee} \tag{8}$$

For any $\mathbf{z}$ in $\mathcal{I}$, and $\mathbf{a} = \psi(\mathbf{z})$ we have $\boldsymbol{C}_g\mathbf{a} \equiv \boldsymbol{C}_g\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$, which by (4) is same as $\boldsymbol{B}(\mathcal{I})(I - q\boldsymbol{T})\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} = \mathbf{z} \pmod{q\mathcal{I}}$, So, ψ is invertible, i.e. $\psi^{-1}(\mathbf{a}) = \mathbf{g} * \mathbf{a} = \mathbf{z} \pmod{q\mathcal{I}}$. It is also surjective since $\boldsymbol{C}_g\mathbf{a}$ is in $\mathcal{I}$ for any $\mathbf{a} \in \mathcal{R}$. Since, ψ^{-1} is easily seen, by commutativity, to be a $\mathcal{R}$-module homomorphism, ψ is an $\mathcal{R}$-module isomorphism. Further, $\boldsymbol{U}$ can be efficiently computed using (6), and this proves (i).

For (ii), we first note that by corollary 4.11 and using (2),

$$\begin{aligned} \mathbf{g} * \mathbf{x} &= (\boldsymbol{V}^\top\boldsymbol{V})^{-1} \cdot (\boldsymbol{V}^\top\boldsymbol{V}) \cdot \boldsymbol{C}_g \cdot \mathbf{x} \\ &= (\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{C}_g^\top \cdot (\boldsymbol{V}^\top\boldsymbol{V}) \cdot \mathbf{x} \\ &= (\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{D}^\top\boldsymbol{B}(\mathcal{I})^\top(\boldsymbol{V}^\top\boldsymbol{V}) \cdot \mathbf{x} \end{aligned} \tag{9}$$

Recall by lemma 4.5, $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}$ is a $\mathbb{Z}$-basis of $\mathcal{I}^\vee$, and $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}$ is a $\mathbb{Z}$-basis of $\mathcal{R}^\vee$. Thus using (9), we can invert $\phi(\mathbf{x})$ by left multiplcation by $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}\boldsymbol{U}^\top(\boldsymbol{V}^\top\boldsymbol{V})$ to $\mathbf{x} \bmod q\mathcal{I}^\vee$. Further, for any $\mathbf{s} \in \mathcal{R}^\vee$, $(\boldsymbol{V}^\top\boldsymbol{V})^{-1} \cdot \boldsymbol{B}(\mathcal{I})^{-\top}\boldsymbol{U}^\top(\boldsymbol{V}^\top\boldsymbol{V}) \cdot \mathbf{s}$ lies in $\mathcal{I}^\vee$ by the aforementioned basis. Thus, ϕ is an invertible and surjective $\mathcal{R}$-module homomorphism, that is also efficiently invertible, thus proving (ii).

Now, we move on to prove (iii). For some $\mathbf{t_0} \in \mathcal{R}$ and $\mathbf{t_1} \in \mathcal{R}^\vee$, we have

$$\begin{aligned} &\psi(\mathbf{z}) * \phi(\mathbf{x}) \\ &= \big(\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} - q \cdot \mathbf{t_0}\big) * (\boldsymbol{C}_g\mathbf{x} - q \cdot \mathbf{t_1}) \\ &= \boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \boldsymbol{C}_g\mathbf{x} - q \cdot \mathbf{t_0} * \mathbf{g} * \mathbf{x} - q \cdot \boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \mathbf{t_1} + q^2 \cdot \mathbf{t_0} * \mathbf{t_1} \\ &\equiv \boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \boldsymbol{C}_g\mathbf{x} \pmod{q\mathcal{R}^\vee} \qquad (10) \\ &\equiv \boldsymbol{C}_g^{-1}\boldsymbol{B}(\mathcal{I})(I - q \cdot \boldsymbol{T})\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \boldsymbol{C}_g\mathbf{x} \pmod{q\mathcal{R}^\vee} \\ &\equiv \mathbf{z} * \mathbf{x} - q \cdot \boldsymbol{C}_g^{-1}\boldsymbol{B}(\mathcal{I})\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \boldsymbol{C}_g\mathbf{x} \pmod{q\mathcal{R}^\vee} \\ &\equiv \mathbf{z} * \mathbf{x} - q \cdot \boldsymbol{C}_g\boldsymbol{C}_x\boldsymbol{C}_g^{-1}\boldsymbol{B}(\mathcal{I})\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} \pmod{q\mathcal{R}^\vee} \\ &\equiv \mathbf{z} * \mathbf{x} - q \cdot \mathbf{x} * \boldsymbol{B}(\mathcal{I})\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} \pmod{q\mathcal{R}^\vee} \\ &\equiv \mathbf{z} * \mathbf{x} \pmod{q\mathcal{R}^\vee} \qquad (11) \end{aligned}$$

where (10) follows by noting that $\mathbf{t_0} * g \in \mathcal{I}$ and $\mathbf{x} \in \mathcal{I}^\vee$ and then employing lemma 4.6. Similarly, $\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$ is in $\mathcal{I} \subseteq \mathcal{R}$, and we can mod out its multiplication by $\mathbf{t_1} \in \mathcal{R}^\vee$. Also, for the last equation (11), we use lemma 4.6, noting that $\boldsymbol{B}(\mathcal{I})\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$ is in $\mathcal{I}$.

Remark. When comparing with [LPR10], note that they obtain a $t \in \mathcal{I}$ such that $t \cdot \mathcal{I}^{-1}$ is co-prime to ideal (q). In other words, $t \cdot \mathcal{I}^{-1} + (q) = (1)$. Multiplying both sides by the ideal $\mathcal{I}$, we get, $(t) + q\mathcal{I} = \mathcal{I}$, which is same as saying that t is the generator of $\mathcal{I}$ mod $q\mathcal{I}$. In other words [LPR10] implicitly shows that $\mathcal{I}$ is principal mod $q\mathcal{I}$, but this is well-known for Dedekind domains. As mentioned earlier, our case is more difficult, yet we manage to prove it.

The above clearing lemma also generalizes to ring of integers of a number field, which is known to be a Dedekind domain. Also, for Dedekind domains $\mathfrak{D}$ it is known that for any ideal $\mathfrak{a}$, $\mathfrak{D}/\mathfrak{a}$ is a principal ideal ring (see wikipedia entry for "Principal Ideal Rings" for a proof). The lemma stated and proved below is easier to use than the original lemma in [LPR10] because as mentioned in the remark above it just needs an arbitrary generator of the principal ideal $\mathcal{I}/(q\mathcal{I})$.

Lemma 8.8. (**Ideal Clearing Lemma for Ring of Integers [LPR10]**) *For any positive integer q, given a $\mathbb{Z}$-basis $\boldsymbol{B}(\mathcal{I})$ for ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbf{K}}$, and a generator $\mathbf{g} \in \mathcal{I}$ for the principal ideal $\mathcal{I}/(q\mathcal{I})$,*

(i) *there is an efficiently computable $\mathcal{O}_{\mathbf{K}}$-module isomorphism $\psi : \mathcal{I}/(q\mathcal{I}) \to \mathcal{O}_{\mathbf{K}}/(q\mathcal{O}_{\mathbf{K}})$,*
(ii) *there is an efficiently invertible $\mathcal{O}_{\mathbf{K}}$-module isomorphism $\phi : \mathcal{I}^\vee/(q\mathcal{I}^\vee) \to \mathcal{O}_{\mathbf{K}}^\vee/(q\mathcal{O}_{\mathbf{K}}^\vee)$,*
(iii) *such that, for any $\mathbf{z} \in \mathcal{I}/(q\mathcal{I})$ and $\mathbf{x} \in \mathcal{I}^\vee/(q\mathcal{I}^\vee)$, their polynomial product satisfies*

$$\mathbf{z} * \mathbf{x} \equiv \psi(\mathbf{z}) * \phi(\mathbf{x}) \pmod{q\mathcal{O}_{\mathbf{K}}^\vee}$$

For a proof of the lemma, see Appendix B.

We now give a counterpart of [PRS17, Lemma 6.9].

Lemma 8.9. *For any ideal $\mathcal{I}$ of $\mathcal{R}$, and $\mathbf{r} \in G$, where*

$$c \ := \ \left(\prod_{i=1}^{n} r_i\right)^{1/n} \cdot (\det(\mathcal{I}) \cdot \varDelta_f)^{-1/n} \ \geq 1,$$

where we have $\mathbf{r} \geq \eta_\epsilon(\mathcal{L}(\mathcal{I}))$ for $\epsilon = \exp(-c^2 n)$.

Proof. Let $\mathbf{R}$ be diag($\mathbf{r}$), and $\mathcal{L}_r = \mathbf{R}^{-1} \cdot \boldsymbol{V} \cdot \mathcal{L}(\mathcal{I})$, so that $\mathcal{L}_r^\vee = \mathbf{R} \cdot \mathcal{L}(\mathcal{I})^\vee$. Since, the dual ideal $\mathcal{I}^\vee$ is the pre-image (under embedding $\boldsymbol{V}$) of the conjugate of $\mathcal{L}(\mathcal{I})^\vee$, any non-zero $\mathbf{w}$ in $\mathcal{L}_r^\vee$ has the form $\mathbf{R} \cdot \mathrm{conj}(\boldsymbol{V}\mathbf{w})$, for $\mathbf{w} \in \mathcal{I}^\vee$.
Claim: for $\mathbf{w} \in \mathcal{I}^\vee$, $\prod_i (\boldsymbol{V}\mathbf{w})_i \ \geq \ \varDelta_f^{-1} \cdot \det(\mathcal{I})^{-1}$.
Proof of Claim: We proved in lemma 4.5 that $\mathcal{I}^\vee$ is a fractional ideal of $\mathcal{R}$. that is $\mathbb{Z}$-spanned by $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}\mathcal{I}^{-T}$. Thus, any $\mathbf{w} \in \mathcal{I}^\vee$ can be viewed as a polynomial $w(X)$ (over $\mathbb{Q}$) with circulant matrix $\boldsymbol{C}_w$. Moreover, every column of $\boldsymbol{C}_w$ can be viewed as a polynomial that is in the ideal $\mathcal{I}^\vee$. Thus, $\boldsymbol{C}_w$ can be generated from the $\mathbb{Z}$-basis of $\mathcal{I}^\vee$ as $\boldsymbol{C}_w = (\boldsymbol{V}^\top \boldsymbol{V})^{-1}\mathcal{I}^{-T}\mathbf{M}$, where $\mathbf{M}$ is an integer $n \times n$ matrix. Now, $\det(\boldsymbol{C}_w)$ is same as $\det(\boldsymbol{D}_w)$ where $\boldsymbol{D}_w$ is the diagonal matrix formed from vector $\boldsymbol{V}\mathbf{w}$ (see equation (1)). Since, by above, $\det(\boldsymbol{C}_w) \ \geq$

$\det(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot \det(\mathcal{I})^{-1}$, we have that $\prod_i (\boldsymbol{V}\mathbf{w})_i \;\geq\; \det(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot \det(\mathcal{I})^{-1}$. Since $\det(\boldsymbol{V}^\top \boldsymbol{V})$ is exactly Δ_f, the claim follows,

Thus, for any $\mathbf{w}$ in $\mathcal{L}_r$, $\|\mathbf{w}\|$ is same as $\sum_i r_i^2 \cdot |(\boldsymbol{V}\mathbf{w})_i|^2$, which by arithmetic mean being no less than the geometric mean implies that

$$\|\mathbf{w}\|^2 \;\geq\; n \left(\prod_i r_i^2 \cdot |(\boldsymbol{V}\mathbf{w})_i|^2 \right)^{1/n},$$

which from the above claim and the hypothesis of the lemma implies that $\|\mathbf{w}\|^2 \geq c^2 n$, so that $\lambda_1(\mathcal{L}_r^\vee) \geq c\sqrt{n}$. The smoothing lemma 2.1 then implies that $1 \geq \eta_\epsilon(\mathcal{L}_r)$, or equivalently $\mathbf{r} \geq \eta_\epsilon(\mathcal{L}(\mathcal{I}))$.

Remark. Note that $\det(\boldsymbol{V}^\top \boldsymbol{V})$ is exactly Δ_f, and for special case $\mathcal{I} = \mathcal{R}^\vee$, we know that it is generated by $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}$ and hence $\det(\mathcal{I}) = \det(\boldsymbol{V}^\top \boldsymbol{V})^{-1}$. Consequently, $\det(\mathcal{R}^\vee) \cdot \Delta_f = 1$, and $c = \left(\prod_{i=1}^n r_i\right)^{1/n}$. Since, the above lemma is used in proof of lemma 8.4, applied to arbitrary ideals in $\mathcal{R}$, the determinant of (any basis) of these ideals is an integer and hence larger than $\det(\mathcal{I})$. Thus, c will only be smaller than the c for the case of $\mathcal{R}^\vee$, and hence a smaller ϵ is obtained.

References

AM69. Michael Francis Atiyah and I. G. MacDonald. *Introduction to commutative algebra.* Addison-Wesley-Longman, 1969. 3

BBPS19. Madalina Bolboceanu, Zvika Brakerski, Renen Perlman, and Devika Sharma. Order-LWE and the hardness of ring-LWE with entropic secrets. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology – ASIACRYPT 2019, Part II*, volume 11922 of *Lecture Notes in Computer Science*, pages 91–120, Kobe, Japan, December 8–12, 2019. Springer, Heidelberg, Germany. 1

BGV12. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS 2012: 3rd Innovations in Theoretical Computer Science*, pages 309–325, Cambridge, MA, USA, January 8–10, 2012. Association for Computing Machinery. 1

Bra12. Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *Lecture Notes in Computer Science*, pages 868–886, Santa Barbara, CA, USA, August 19–23, 2012. Springer, Heidelberg, Germany. 1

CGGI16. Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology – ASIACRYPT 2016, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 3–33, Hanoi, Vietnam, December 4–8, 2016. Springer, Heidelberg, Germany. 1

CKKS17. Jung Hee Cheon, Andrey Kim, Miran Kim, and Yong Soo Song. Homomorphic encryption for arithmetic of approximate numbers. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017, Part I*, volume 10624 of *Lecture Notes in Computer Science*, pages 409–437, Hong Kong, China, December 3–7, 2017. Springer, Heidelberg, Germany. 1

Cla84. A. Clark. *Elements of Abstract Algebra*. Dover Books on Mathematics Series. Dover Publications, 1984. 3

Coh93. Henri Cohen. *A course in computational algebraic number theory*, volume 8. Springer-Verlag Berlin, 1993. 3, 11

Cona. Keith Conrad. The conductor ideal of an order. 1, 6

Conb. Keith Conrad. Dedekind's index theorem. 3

Conc. Keith Conrad. The different ideal. 7, 4.2, 6

Cond. Keith Conrad. Noetherian rings. 3.4

DD12. Léo Ducas and Alain Durmus. Ring-LWE in polynomial rings. In Marc Fischlin, Johannes Buchmann, and Mark Manulis, editors, *PKC 2012: 15th International Conference on Theory and Practice of Public Key Cryptography*, volume 7293 of *Lecture Notes in Computer Science*, pages 34–51, Darmstadt, Germany, May 21–23, 2012. Springer, Heidelberg, Germany. 5

DM15. Léo Ducas and Daniele Micciancio. FHEW: Bootstrapping homomorphic encryption in less than a second. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 617–640, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany. 1

Eis13. David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013. 3.6, 3

FT91. A. Fröhlich and M. J. Taylor. *Algebraic Number Theory*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1991. C

FV12. Junfeng Fan and Frederik Vercauteren. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Report 2012/144, 2012. `https://eprint.iacr.org/2012/144`. 1

Gen09. Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, *41st Annual ACM Symposium on Theory of Computing*, pages 169–178, Bethesda, MD, USA, May 31 – June 2, 2009. ACM Press. 1

GSW13. Craig Gentry, Amit Sahai, and Brent Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 75–92, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany. 1

Kap73. Irving Kaplansky. Commutative rings. In *Conference on Commutative Algebra*, pages 153–166. Springer, 1973. 3

LLL82. Arjen Lenstra, Hendrik Lenstra, and Laszlo Lovasz. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982. A

LPR10. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany. 1, 1, 1, 8, 8, 8, 8.8, B

MR07. Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007. 2.1, 2.2, 2.3

PRS17. Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. In Hamed Hatami, Pierre McKenzie, and Valerie King, editors, *49th Annual ACM Symposium on Theory of Computing*, pages 461–473, Montreal, QC, Canada, June 19–23, 2017. ACM Press. 1, 2.1, 8, 8, 8, 8, 8.5, 8, 1, 2, 8, 8, 8

Reg05. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th Annual ACM Symposium on Theory of Computing*, pages 84–93, Baltimore, MA, USA, May 22–24, 2005. ACM Press. 1

Reg06. Oded Regev. Lattice-based cryptography (invited talk). In Cynthia Dwork, editor, *Advances in Cryptology – CRYPTO 2006*, volume 4117 of *Lecture Notes in Computer Science*, pages 131–141, Santa Barbara, CA, USA, August 20–24, 2006. Springer, Heidelberg, Germany. 8

Reg10. Oded Regev. The learning with errors problem (invited survey). In *2010 IEEE 25th Annual Conference on Computational Complexity*, pages 191–204, June 2010. 8

RSW18. Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the ring-LWE and polynomial-LWE problems. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 146–173, Tel Aviv, Israel, April 29 – May 3, 2018. Springer, Heidelberg, Germany. 1

SSTX09. Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 617–635, Tokyo, Japan, December 6–10, 2009. Springer, Heidelberg, Germany. 1

A Appendix

Lemma 3.1 (repeated).

(i) Every non-trivial ring has at least one maximal ideal.
(ii) A maximal ideal is always a prime ideal.
(iii) The quotient ring $R/\mathfrak{a}$ is a field iff $\mathfrak{a}$ is a maximal ideal.
(iv) For ideals $\mathfrak{a}$ and $\mathfrak{b}$, their sum $\mathfrak{a}+\mathfrak{b}$ is the set of all $x+y$ where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. It is the smallest ideal containing $\mathfrak{a}$ and $\mathfrak{b}$.
(v) Thus, a maximal ideal $\mathfrak{m}$ is co-prime to every ideal that is not a subset of $\mathfrak{m}$.
(vi) If $\mathfrak{a}$ and $\mathfrak{b}$ are *not* co-prime, then there exists a maximal ideal $\mathfrak{m}$ such that $\mathfrak{a}+\mathfrak{b} \subseteq \mathfrak{m}$.
(vii) If $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime, then $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.
($viii$) If a prime ideal $\mathfrak{p}$ contains product of two ideal $\mathfrak{a}\mathfrak{b}$, then at least one of $\mathfrak{a}$ or $\mathfrak{b}$ is in $\mathfrak{p}$.
(ix) If an ideal $\mathfrak{a}$ is co-prime to two ideals, say $\mathfrak{b}$ and $\mathfrak{c}$, then $\mathfrak{a}$ is co-prime to $\mathfrak{b}\mathfrak{c}$.
(x) If for some positive integer r, and $a \in R$, a^r is contained in a prime ideal $\mathfrak{p}$, then a is contained in $\mathfrak{p}$ (by definition of prime ideal).
(xi) This easily generalizes to the fact that if for some positive integer r, and ideal $\mathfrak{a}$, $\mathfrak{a}^r$ is contained in a prime ideal $\mathfrak{p}$, then $\mathfrak{a}$ is contained in $\mathfrak{p}$.
(xii) If ideals $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime, then for any positive integers r, s, their powers $\mathfrak{a}^r$ and $\mathfrak{b}^s$ are also co-prime.
($xiii$) If a maximal ideal $\mathfrak{m}$ contains product of powers of distinct maximal ideals $\mathfrak{n}_1, ..., \mathfrak{n}_k$, then $\mathfrak{m}$ must be one of $\mathfrak{n}_1, ..., \mathfrak{n}_k$.

Proof. Proof of ((i)). If a prime ideal $\mathfrak{p}$ contains product of two ideal $\mathfrak{a}\mathfrak{b}$, then at least one of $\mathfrak{a}$ or $\mathfrak{b}$ is in $\mathfrak{p}$. If neither of $\mathfrak{a}$ and $\mathfrak{b}$ is contained in $\mathfrak{p}$, then there are elements $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$, that are not in $\mathfrak{p}$. Yet, $a * b$, being in $\mathfrak{a}\mathfrak{b}$ is in $\mathfrak{p}$, contradicting the fact that $\mathfrak{p}$ is prime.

Proof of ((ii)). If an ideal $\mathfrak{a}$ is co-prime to two ideals, say $\mathfrak{b}$ and $\mathfrak{c}$, then $\mathfrak{a}$ is co-prime to $\mathfrak{b}\mathfrak{c}$. For if not, then $\mathfrak{a}+\mathfrak{b}\mathfrak{c}$ is contained in a maximal ideal $\mathfrak{m}$, and hence $\mathfrak{b}\mathfrak{c}$ is also contained in $\mathfrak{m}$. By previous item, one of $\mathfrak{b}$ or $\mathfrak{c}$, w.l.o.g. $\mathfrak{b}$, is contained in $\mathfrak{m}$. Since $\mathfrak{a}$ is also contained in $\mathfrak{m}$, this implies that $\mathfrak{a}+\mathfrak{b}$ is contained in $\mathfrak{m}$, contradicting the fact that $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime.

Proof of ((iii)). If ideals $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime, then for any positive integers r, s, their powers $\mathfrak{a}^r$ and $\mathfrak{b}^s$ are also co-prime: if $\mathfrak{a}^r$ and $\mathfrak{b}^s$ are not co-prime then there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}^r + \mathfrak{b}^s$, and hence also $\mathfrak{a}^r$ and $\mathfrak{b}^s$ individually. Since $\mathfrak{m}$ is also prime, $\mathfrak{m}$ contains both $\mathfrak{a}$ and $\mathfrak{b}$ and hence also their sum, contradicting the fact that $\mathfrak{a}$ and $\mathfrak{b}$ are co-prime.

Proof of ((iv)). If a maximal ideal $\mathfrak{m}$ contains product of powers of distinct maximal ideals $\mathfrak{n}_1, ..., \mathfrak{n}_k$, then $\mathfrak{m}$ must be one of $\mathfrak{n}_1, ..., \mathfrak{n}_k$. Say, $\prod_i \mathfrak{n}_i^{r_i}$ is contained in $\mathfrak{m}$. Suppose $\mathfrak{m}$ is not the same as one of $\mathfrak{n}_1, ..., \mathfrak{n}_k$. Then, $\mathfrak{m}$ is co-prime to each of $\mathfrak{n}_i$, and hence also to their powers $\mathfrak{n}_i^{r_i}$, which are also pair-wise co-prime. Thus, one of $\mathfrak{n}_i^{r_i}$ is in $\mathfrak{m}$ (by item (i)), and hence maximal ideal $\mathfrak{n}_i$ is itself in maximal ideal $\mathfrak{m}$, an absurdity.

Lemma 3.2 (repeated) For any ring R, and any maximal ideal $\mathfrak{a} = (a_1, a_2)$ of R, let $x \in R$ be such that x is not in $\mathfrak{a}$. Then for any positive integers r, s, x is invertible modulo (a_1^r, a_2^s).

The lemma can be proved easily in multiple ways, but we prefer an argument used in Prop. 2.5 in [LLL82].

Proof. Clearly, for $r = 1$ and $s = 1$, the claim holds, i.e. x is invertible modulo the maximal ideal $\mathfrak{a}$, as $R/\mathfrak{a}$ is a field. Thus,

$$\mu x = 1 - (\nu_1 a_1 + \nu_2 a_2),$$

for some μ, ν_1, ν_2. If ν_2 is zero, then x is invertible modulo (a_1) and hence also modulo any power of (a_1), and we are done. Similarly, for ν_1 being zero. Else,

$$\mu x + \nu_1 a_1 = 1 - \nu_2 a_2,$$

Multiplying both sides by $1 + \nu_2 a_2 + ... + (\nu_2 a_2)^{s-1}$, we get

$$\mu' x + \nu_1' a_1 = 1 - \nu_2^s a_2^s,$$

for some μ' and ν_1'. Rewriting this as

$$\mu' x + \nu_2^s a_2^s = 1 - \nu_1' a_1,$$

and multiplying both sides by $1 + \nu_1' a_1 + ... + (\nu_1' a_1)^{r-1}$, the claim follows.

Lemma 5.2 (repeated) In the ring $\mathcal{R}$, let $w = \sum_{i=1}^m e_i$. If $w \geq 2$, and some $e_i = 1$ (w.l.o.g. $e_m = 1$), then $p^{w-2} * h_m(X)$ is invertible modulo the ideal $(p^{w-1}, \prod_{j=1}^{m-1} h_j(X)^{e_j})$.

Proof. The case $w = 2$ is implied by the above lemma 5.1 and lemma 3.2. So, we focus on $w > 2$. Since all $h_i(X)$ are irreducible and distinct, by using the extended Euclidean algorithm in $\mathbb{Z}[X]$, we have

$$\mu(X) p^{w-2} h_m(X) + \lambda(X) \prod_{j=1}^{m-1} h_j(X)^{e_j} = c,$$

for some non-trivial polynomials $\mu(X)$ and $\lambda(X)$ and an integer c. If c is a multiple of the prime p, then $\lambda(X) \prod_{j=1}^{m-1} h_j(X)^{e_j}$ is zero modulo p. Since $\lambda(X)$ is non-trivial this implies that one of $h_j(X)$ is zero modulo p, which is impossible. Thus, $(c, p) = 1$, and hence

$$\mu'(X) p^{w-2} h_m(X) + \lambda'(X) \prod_{j=1}^{m-1} h_j(X)^{e_j} = 1 - \nu p,$$

for some non-trivial polynomials $\mu'(X)$ and $\lambda'(X)$ and an integer ν. Multiplying both sides by $1 + \nu p + ... + (\nu p)^{w-2}$, we have

$$\mu''(X) p^{w-2} h_m(X) + \lambda''(X) \prod_{j=1}^{m-1} h_j(X)^{e_j} = 1 - \nu^{w-1} p^{w-1},$$

for some non-trivial polynomials $\mu''(X)$ and $\lambda''(X)$, and that concludes the proof.

Lemma 5.3 (repeated) Let $w = \sum_{i=1}^{m} e_i$. If for all $i \in [m]$, $e_i > 1$, then $t(X)$, the quotient in the factorization of $f(X)$ modulo p, is invertible modulo the ideal $(p^{w-1}, p^{w-2}h_m(X))$.

Proof. Since p is Dedekind-special, $t(X)$ is not in any $\mathfrak{p}_i$, and hence not in $\mathfrak{p}_m$. Since all $h_1(X)$ is irreducible, an $t(X)$ is not in $(p, h_m(X))$, by using the extended Euclidean algorithm in $\mathbb{Z}[X]$, we have

$$\mu(X)p^{w-2}h_m(X) + \lambda(X)t(X) = c,$$

for some non-trivial polynomials $\mu(X)$ and $\lambda(X)$ and an integer c. If c is a multiple of the prime p, then $\lambda(X)t(X)$ is zero modulo p. Since $\lambda(X)$ is non-trivial this implies that one of $t(X)$ is zero modulo p, which is impossible by the Dedekind-special property. Thus, $(c, p) = 1$, and we conclude using the same argument as in the previous lemma.

Lemma 5.10 (repeated) For all $i \in [m]$, the ideal $\bar{\mathfrak{p}}_i \ = \ 0$

Proof. Since $\mathcal{R}$ is Noetherian, and $\bar{\mathfrak{p}}_i$ is an ideal of $\mathcal{R}$, it is finitely generated, and hence a finite set of k generators, for some $k > 0$, say $g_1, ..., g_k$. Moreover, since $\bar{\mathfrak{p}}_i \subseteq \mathfrak{p}_i$, these generators are also in $\mathfrak{p}_i = (h_i(X), p)$. Let, $\mu_1, ..., \mu_k$ and $\lambda_1, ..., \lambda_k$ be elements of $\mathcal{R}$ such that for each $k \in [k]$, $g_j = \mu_j p + \lambda_j h_i(X)$, where w.l.o.g. μ_j is not a multiple of $h_i(X)$, and otherwise μ_j and λ_j are polynomials of degree less than the degree of monic $f(X)$. This also implies that $g_j = \lambda_j h_i(X) \bmod p$. Let J^* be the maximal subset of $[k]$, such that λ_j is non-zero for $j \in J^*$.
Claim 1: The set J^* is empty.
Proof of Claim 1: In the ring $\mathcal{R}$, since $f(X)$ is monic, we can assume that g_j is reduced to degree less than degree of $f(X)$. For $j \in J^*$, g_j is a multiple of $h_(X)$ mod p. Since $Z_p[X]$ is a UFD, consider the unique factorization of g_j in $Z_p[X]$, and let the largest power of $h_i(X)$ in this factorization be $h_i(X)^{t_j}$, where $t_j > 0$. Let $g_j(X) = \lambda'_j h_i(X)^{t_j} \bmod p$, where λ'_j is non-zero, and is not a multiple of $h_i(X) \bmod p$.

Let $t^* = \min \{t_j \mid j \in J^*\}$. Let j^* be an arbitrary index in J^* such that $t_j = t^*$. Since by Krull intersection theorem (theorem 3.5), $\bar{\mathfrak{p}}_i \subseteq \mathfrak{p}_i\bar{\mathfrak{p}}_i$, each generator g_j is in $\mathfrak{p}_i\bar{\mathfrak{p}}_i$, which is same as $(h_i(X), p)(g_1, ...g_k)$. Thus,

$$g_{j^*} = h_i(X) * \sum_{j \in J^*} \alpha_j \lambda'_j h_i(X)^{t_j} \bmod \ (p, f(X)),$$

where α_j is in $\mathcal{R}$, and at least one α_j is non-zero. Substituting, $\lambda'_{j^*} h_i(X)^{t_{j^*}}$ on the left hand side we get

$$\lambda'_{j^*} h_i(X)^{t_{j^*}} = h_i(X) * \sum_{j \in J^*} \alpha_j \lambda'_j h_i(X)^{t_j} \bmod \ (p, f(X)).$$

This can equivalently be written as

$$\lambda'_{j^*} h_i(X)^{t_{j^*} - t_{j^*}} = h_i(X) * \sum_{j \in J^*} \alpha_j \lambda'_j h_i(X)^{t_j - t_{j^*}} \bmod \ (p, f(X)),$$

as all $t_j > t_{j^*} > 0$ for $j \in J^*$. But, this is a contradiction of λ'_{j^*} being not a multiple of $h_i(X)$ mod p.

End of Proof of Claim 1

Thus, for all $k \in [k]$, $g_j = \mu_j p$. Again, since by theorem 3.5, $\bar{\mathfrak{p}}_i \subseteq \mathfrak{p}_i\bar{\mathfrak{p}}_i$, each generator g_j is in $\mathfrak{p}_i\bar{\mathfrak{p}}_i$, which is same as $(h_i(X), p)(g_1, ...g_k)$. Thus, for any particular $j' \in [k]$,

$$\mu_{j'}p = \sum_{j \in [k]} (\alpha_j p + \beta_j h_i(X))\mu_j p \bmod \ (f(X)),$$

where α_j, β_j are in $\mathcal{R}$, and at least one is non-trivial. Since $Z[X]$ is a UFD and $f(X)$ is monic, we can factor[12] out p. And thus,

$$\mu_{j'} = \sum_{j \in [k]} \beta_j h_i(X)\mu_j \bmod \ (p, f(X)).$$

But, this implies that either $\mu_{j'}$ is zero or $\mu_{j'}$ is a multiple of $h_i(X)$, the latter being a contradiction. Hence, all μ_j are zero for $j \in [k]$. This implies that that $\hat{\mathfrak{p}_i} = 0$.

B Proof of Ideal Clearing Lemma for Ring of Integers

Lemma 8.8 (repeated) (**Ideal Clearing Lemma for Ring of Integers** [LPR10]) For any positive integer q, given a $\mathbb{Z}$-basis $\boldsymbol{B}(\mathcal{I})$ for ideal $\mathcal{I}$ of $\mathcal{O}_{\mathbf{K}}$, and a generator $\mathbf{g} \in \mathcal{I}$ for the principal ideal $\mathcal{I}/(q\mathcal{I})$,

(*i*) There's an efficiently computable $\mathcal{O}_{\mathbf{K}}$-module isomorphism $\psi : \mathcal{I}/(q\mathcal{I}) \to \mathcal{O}_{\mathbf{K}}/(q\mathcal{O}_{\mathbf{K}})$,

(*ii*) There's an efficiently invertible $\mathcal{O}_{\mathbf{K}}$-module isomorphism $\phi : \mathcal{I}^\vee/(q\mathcal{I}^\vee) \to \mathcal{O}_{\mathbf{K}}^\vee/(q\mathcal{O}_{\mathbf{K}}^\vee)$,

(*iii*) such that, for any $\mathbf{z} \in \mathcal{I}/(q\mathcal{I})$ and $\mathbf{x} \in \mathcal{I}^\vee/(q\mathcal{I}^\vee)$, their polynomial product satisfies

$$\mathbf{z} * \mathbf{x} \equiv \psi(\mathbf{z}) * \phi(\mathbf{x}) \pmod{q\mathcal{O}_{\mathbf{K}}^\vee}$$

Proof. We will write $\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})$ for a basis of $\mathcal{O}_{\mathbf{K}}$.

We have that $\mathbf{g}$ is a generator of $\mathcal{I}$ modulo $q\mathcal{I}$. In other words, as ideals, $\mathcal{I} = (\mathbf{g}) + q\mathcal{I}$. Thus, $\mathbf{g} \in \mathcal{I}$. Thus,

$$\boldsymbol{C}_g\boldsymbol{B}(\mathcal{O}_{\mathbf{K}}) = \boldsymbol{B}(\mathcal{I}) \cdot \boldsymbol{D}, \tag{12}$$

where $\boldsymbol{D}$ is an integer matrix.

We also have that every column of $\boldsymbol{B}(\mathcal{I})$ is generated by $\boldsymbol{C}_g$ mod $q\mathcal{I}$, or mod $q\boldsymbol{B}(\mathcal{I})$. Thus,

$$\boldsymbol{B}(\mathcal{I}) = \boldsymbol{C}_g\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U} + q \cdot \boldsymbol{B}(\mathcal{I})\boldsymbol{T} \tag{13}$$

[12] This is where one would usually require that $\mathcal{R}$ is an integer domain.

for some integer, matrices $\boldsymbol{U}$ and $\boldsymbol{T}$. Equivalently,

$$\boldsymbol{B}(\mathcal{I}) \cdot (I - q\boldsymbol{T}) = \boldsymbol{C}_g \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U}, \tag{14}$$

or, since $\boldsymbol{C}_g$ is full-ranked, we have

$$(\boldsymbol{C}_g \boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))^{-1}\boldsymbol{B}(\mathcal{I}) \cdot (I - q\boldsymbol{T}) = \boldsymbol{U} \tag{15}$$

We next show that $\boldsymbol{D} \cdot \boldsymbol{U} = I \pmod{q}$. Note, from (12) and observing that $\boldsymbol{B}(\mathcal{I})$ is full-ranked, $\boldsymbol{D} = \boldsymbol{B}(\mathcal{I})^{-1}\boldsymbol{C}_g\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})$. Multiplying the above equation on the left by $\boldsymbol{D}$, we get $(I - q\boldsymbol{T}) = \boldsymbol{D} \cdot \boldsymbol{U}$, and hence

$$\boldsymbol{D} \cdot \boldsymbol{U} = I \pmod{q}. \tag{16}$$

Now, consider the following two mappings for claims (i)-(iii). For any $\mathbf{z} \in \mathcal{I}$ and $\mathbf{x} \in \mathcal{I}^\vee$, define

$$\psi(\mathbf{z}) = \mathbf{a} = \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} \pmod{q\mathcal{O}_{\mathbf{K}}} \tag{17}$$

$$\phi(\mathbf{x}) = \mathbf{g} * \mathbf{x} \pmod{q\mathcal{O}_{\mathbf{K}}^\vee} \tag{18}$$

For any $\mathbf{z}$ in $\mathcal{I}$, and $\mathbf{a} = \psi(\mathbf{z})$ we have $\boldsymbol{C}_g\mathbf{a} \equiv \boldsymbol{C}_g\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$, which by (13) is same as $\boldsymbol{B}(\mathcal{I})(I - q\boldsymbol{T})\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} = \mathbf{z} \pmod{q\mathcal{I}}$, So, ψ is an invertible map. It is also surjective since $\boldsymbol{C}_g\mathbf{a}$ is in $\mathcal{I}$ for any $\mathbf{a} \in \mathcal{O}_{\mathbf{K}}$. Since, ψ^{-1} is easily seen to be a $\mathcal{O}_{\mathbf{K}}$-module homomorphism, ψ is an $\mathcal{O}_{\mathbf{K}}$-module isomorphism. Further, we already showed how to compute $\boldsymbol{U}$ efficiently, this proves (i).

For (ii), we first note that by corollary 4.11 and using (12),

$$\mathbf{g} * \mathbf{x} = (\boldsymbol{V}^\top\boldsymbol{V})^{-1} \cdot (\boldsymbol{V}^\top\boldsymbol{V}) \cdot \boldsymbol{C}_g \cdot \mathbf{x} \tag{19}$$

$$= (\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{C}_g^\top \cdot (\boldsymbol{V}^\top\boldsymbol{V}) \cdot \mathbf{x} \tag{20}$$

$$= (\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})^{-\top}\boldsymbol{D}^\top\boldsymbol{B}(\mathcal{I})^\top(\boldsymbol{V}^\top\boldsymbol{V}) \cdot \mathbf{x} \bmod q\mathcal{O}_{\mathbf{K}}^\vee, \tag{21}$$

where the last equality follows by noting that $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})^{-\top}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_{\mathbf{K}}^\vee$ (see footnote to lemma 4.5).

Thus, by lemma 4.5, $\phi(\mathbf{x})$ is inverted by $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}\boldsymbol{U}^\top\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})^\top(\boldsymbol{V}^\top\boldsymbol{V})$ to $\mathbf{x} \bmod q\mathcal{I}^\vee$. Further, for any $\mathbf{s} \in \mathcal{O}_{\mathbf{K}}^\vee$, $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}\boldsymbol{U}^\top\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})^\top(\boldsymbol{V}^\top\boldsymbol{V})\mathbf{s}$ lies in $\mathcal{I}^\vee$ by the aforementioned basis. Thus, ϕ is an invertible and surjective $\mathcal{O}_{\mathbf{K}}$-module homomorphism, that is also efficiently invertible, thus proving (ii).

Now, we move on to prove (iii). For some $\mathbf{t_0} \in \mathcal{O}_{\mathbf{K}}$ and $\mathbf{t_1} \in \mathcal{O}_{\mathbf{K}}^\vee$, we have

$$\begin{aligned}
&\psi(\mathbf{z}) * \phi(\mathbf{x}) \\
&= \left(\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} - q \cdot \mathbf{t_0}\right) * (\boldsymbol{C}_g\mathbf{x} - q \cdot \mathbf{t_1}) \\
&= \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \boldsymbol{C}_g\mathbf{x} - q \cdot \mathbf{t_0} * \mathbf{g} * \mathbf{x} - q \cdot \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \mathbf{t_1} + q^2 \cdot \mathbf{t_0} * \mathbf{t_1} \\
&\equiv \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \boldsymbol{C}_g\mathbf{x} \pmod{q\mathcal{O}_{\mathbf{K}}^\vee} && (22) \\
&\equiv \boldsymbol{C}_g^{-1}\boldsymbol{B}(\mathcal{I})(I - q \cdot \boldsymbol{T})\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \boldsymbol{C}_g\mathbf{x} \pmod{q\mathcal{O}_{\mathbf{K}}^\vee} \\
&\equiv \mathbf{z} * \mathbf{x} - q \cdot \boldsymbol{C}_g^{-1}\boldsymbol{B}(\mathcal{I})\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} * \boldsymbol{C}_g\mathbf{x} \pmod{q\mathcal{O}_{\mathbf{K}}^\vee} \\
&\equiv \mathbf{z} * \mathbf{x} - q \cdot \boldsymbol{C}_g\boldsymbol{C}_x\boldsymbol{C}_g^{-1}\boldsymbol{B}(\mathcal{I})\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} \pmod{q\mathcal{O}_{\mathbf{K}}^\vee} \\
&\equiv \mathbf{z} * \mathbf{x} - q \cdot \mathbf{x} * \boldsymbol{B}(\mathcal{I})\boldsymbol{T}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z} \pmod{q\mathcal{O}_{\mathbf{K}}^\vee} \\
&\equiv \mathbf{z} * \mathbf{x} \pmod{q\mathcal{O}_{\mathbf{K}}^\vee} && (23)
\end{aligned}$$

where (22) follows by noting that $\mathbf{t_0} * g \in \mathcal{I}$ and $\mathbf{x} \in \mathcal{I}^\vee$ and then employing lemma 4.6. Similarly, $\boldsymbol{B}(\mathcal{O}_\mathbf{K})\boldsymbol{U}\boldsymbol{B}(\mathcal{I})^{-1}\mathbf{z}$ is in $\mathcal{I}$. Also, for the last equation (23), we use lemma 4.6.

C Ring of Integers of Cyclotomic Fields

In this section, we restrict ourselves to cyclotomic fields, i.e. where $f(X)$ is a cyclotomic polynomial. Recall, a complex number ζ is a primitive m-th root of unity, if its order is exactly m. The m-th **cyclotomic polynomial** is defined by

$$\Phi_m(X) \;=\; \prod(X-\zeta)$$

where the product runs over the different primitive m-th roots of unity ζ. Since, such primitive roots lie in a splitting extension field E (over $\mathbb{Q}$) of $X^m - 1$, the primitive roots are exactly the generators of the cyclic group of order m; thus degree of $\Phi_m(X)$ is exactly the Euler totient function $\phi(m)$. It is well-known that cyclotomic polynomials are irreducible in $\mathbb{Q}[X]$. The cyclotomic field $\mathbb{Q}[X]/(\Phi_m(X))$ will be denoted by $\mathbb{Q}[m]$.

We have the following well-known identities.

$$\begin{aligned} X^m - 1 \;&=\; \prod_{d|m}\Phi_d(X) \\ \Phi_m(X) \;&=\; \prod_{d|m}(X^d-1)^{\mu(m/d)} \\ \Phi_{p^r}(X) &= \frac{X^{p^r}-1}{X^{p^{r-1}}-1} = \sum_{i=0}^{p-1} X^{ip^{r-1}} \end{aligned}$$

where $\mu(\cdot)$ is the mobius function, p is a prime, and $r \geq 1$. It follows that $\Phi_m(X)$ is always a polynomial over the base field $\mathbb{Q}$.

We also have the following lemma, whose proof can be found in any text in algebraic number theory, for instance (VI. 1.14) of [FT91].

Lemma C.1. *If $m = m_1m_2$ with $(m_1, m_2) = 1$, then $\mathbb{Q}[m]$ is the compositum of arithmetically disjoint fields, i.e.*

$$\begin{aligned} \mathbb{Q}[m] &\cong \mathbb{Q}[m_1] \otimes_\mathbb{Q} \mathbb{Q}[m_2] \\ \mathcal{O}_{\mathbb{Q}[m]} &\cong \mathcal{O}_{\mathbb{Q}[m_1]} \otimes_\mathbb{Z} \mathcal{O}_{\mathbb{Q}[m_2]} \end{aligned}$$

It is well-known that the ring of integers $\mathcal{O}_\mathbf{K} = \mathbb{Q}[X]/(\Phi_m(X))$ of a cyclotomic field is same as the polynomial ring $\mathbb{Z}[X]/(\Phi_m(X))$. Below, we give an easy proof of this fact using Dedekind index theorem. This polynomial ring will also be referred to as the m-th **cyclotomic ring**. Recall, in section 2, we defined the discriminant of a separable polynomial $f(X)$ to be the square of the determinant of the vandermonde matrix of $f(X)$. When $f(X)$ is a cyclotomic polynomial, the discriminant of the polynomial is also called the **discriminant** of the cyclotomic field and denoted $\varDelta_\mathbf{K}$ (as also the discriminant of the ring of integers, or the cyclotomic ring).

Theorem C.2. *For any m, the ring of integers $\mathcal{O}_{\mathbf{K}}$ of the cyclotomic field $\mathbf{K} = \mathbb{Q}[X]/(\Phi_m(X))$ is same as the polynomial ring $\mathcal{R} = \mathbb{Z}[X]/(\Phi_m(X))$. Thus, $\mathcal{R}$ is a Dedekind domain.*

Proof. By lemma C.1, we are reduced to proving the theorem for m that are prime powers, i.e. $m = q^r$, for some prime q and positive integer r. It is well known[13] that a prime p divides $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$ only if p^2 is a factor of $\varDelta_{\Phi_m(X)}$. By corollary 4.9 , the discriminant of a monic separable $f(X)$ is same as the determinant of the circulant matrix of $f'(X)$. Further, since the similarity transform given by the vandermonde matrix of $f(X)$, transforms the circulant matrix of any $g(X)$ to a diagonal matrix with entries $g(\zeta_i)$, where ζ_i are the roots of $f(X)$, one can show that $\varDelta_{f_1}\varDelta_{f_2}$ divides the discriminant of $f_1(X)f_2(X)$. Thus, discriminant of $\Phi_m(X)$ divides the discriminant of $X^m - 1$. For $m = p^r$, the discriminant of $X^m - 1$ is easily seen to be (upto sign) a power of p. Thus, $\varDelta_{\Phi_m(X)}$ can only be divisible by prime p. This further implies that only prime p, if any, can divide $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$.

By Dedekind index theorem 3.8, for any prime p, p does not divide $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$ iff p is Dedekind-special for $\Phi_m(X)$. Thus, we just need to check that prime p coming from $m = p^r$ is Dedekind-special for $\Phi_m(X)$. Since modulo p, the power-p map is a Frobenius map, we have that $\Phi_{p^r}(X) = \Phi_p(X)^{p^{r-1}}$ mod p. Next, note that $\Phi_p(X) = (X-1)^{p-1}$ mod p, by first noting that $X^p - 1 = (x-1)^p$ mod p. Thus, $\Phi_{p^r}(X) = (X-1)^{\phi(p^r)}$. To test the Dedekind-special property, write $\Phi_{p^r}(X) = (X-1)^{\phi(p^r)} + p * t(X)$. Evaluating both sides at $X = 1$, we note that $\Phi_{p^r}(X)_{|X=1} = p$, and hence $t(1) = 1$ mod p. Thus $t(X)$ is not divisible by $(X-1)$ modulo p, and hence p is Dedekind special for $\Phi_{p^r}(X)$.

[13] $\varDelta_f = [\mathcal{O}_{\mathbf{K}} : \mathcal{R}]^2 \cdot \mathrm{disc}(\mathcal{O}_{\mathbf{K}})$, and $\mathrm{disc}(\mathcal{O}_{\mathbf{K}})$ is an integer.