Ring-LWE Hardness Based on Non-invertible Ideals[⋆]

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

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

Abstract. We extend the known pseudorandomness of Ring-LWE to be based on lattices that do not correspond to any ideal of any order in the underlying number field. 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.

In this work we show that hardness of q-Ring-LWE can be based on worst-case hardness of ideal lattices in arbitrary orders $\mathcal{O}$, as long as the order $\mathcal{O}$ satisfies the property that $\frac{1}{m} \cdot \mathcal{O}$ contains the ring of integers, for some m co-prime to q. The reduction requires that the noise be a factor m more than the original Ring-LWE reduction. We also show that for the power-of-two cyclotomic number fields, there exist orders with $m = 4$ such that non-trivial ideals of the order, which are not contained in the conductor, are non-invertible. Since the conductor itself is non-invertible, this gives a non-trivial multiplicative set that lies outside the ideal class group.

Another reduction shows that hardness of q-Ring-LWE can be based on worst-case hardness of lattices that correspond to sum of ideal-lattices in arbitrary and different orders in the number field, as long as the (set of) orders $\{\mathcal{O}_i\}$ satisfy the property that $\frac{1}{m} \cdot \mathcal{O}_i$ contains the ring of integers, for some m co-prime to q. We also show that for the power-of-two cyclotomic number fields, there exist orders $\mathcal{O}_1, \mathcal{O}_2$ with $m = 8$ such that there are ideals $\mathcal{I}_1, \mathcal{I}_2$ of $\mathcal{O}_1, \mathcal{O}_2$ resp. with $\mathcal{I}_1 + \mathcal{I}_2$ not an ideal of any order in the number field.

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*

[⋆] An earlier unpublished version of this paper was titled "Enhancing Ring-LWE Hardness Using Dedekind Index Theorem" [JL22].

[⋆⋆] Part of this work was done while the author was a summer intern at IBM T. J. Watson Research Center.

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), shortest vector problem (SVP) 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.

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 $\mathbf{K} = \mathbb{Q}[X]/(f(X))$. The hardness of RLWE is then based on lattice problems restricted to ideal lattices in the ring $\mathcal{O}_{\mathbf{K}}$, 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 size 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 evaluation 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 $\mathcal{O}_{\mathbf{K}}$ of a number field enjoy remarkable algebraic properties, namely that such rings are Dedekind domains [3], 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. Further, since all ideals are invertible as fractional ideals, they form a multiplicative group. In light of this [4], it is natural to ask if the class of lattices can be expanded to a class having lesser algebraic properties. Ideally, one would like to base the hardness of RLWE on worst-case general integer lattices as is the case for LWE.

[3] In Appendix E we provide a brief introduction to Dedekind domains and ring of integers. For the purpose of present discussion, the ring $\mathcal{O}_{\mathbf{K}}$ can be viewed as an extension of the polynomial ring $\mathbb{Z}[X]/(f(X))$ that includes elements from $\mathbb{Q}[X]/(f(X))$ which satisfy any polynomial equation with integer coefficients. This *integral-closure* leads to $\mathcal{O}_{\mathbf{K}}$ satisfying unique prime-ideal factorization property (see e.g. [Cla84]).

[4] We will later discuss in more detail the currently best known attacks on ideal lattices.

To mitigate this issue, 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 $\mathcal{O}$ (i.e. any full-ranked sub-ring) such as the polynomial ring $\mathbb{Z}[X]/(f(X))$. In a followup work, the paper [BBS21] shows that the hardness of this q-Order-LWE (i.e. modulo q and in order $\mathcal{O}$) can be based on worst-case hard problems of ideal lattices of this order as long as the index of the order in the maximal order $\mathcal{O}_{\mathbf{K}}$, i.e. $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$, is co-prime to q. A similar, and in fact more general, result is also implied by [PP19], and we will discuss this in more detail in the related work section. As we will see later, most of these RLWE-like reductions employ a key lemma informally known as the "ideal-clearing lemma", which removes any mention of the (worst-case) ideal from the q-RLWE samples.

In this work we show that the hardness of the original Ring-LWE problem q-RLWE itself can be based on hardness of ideal lattices of arbitrary orders as long as $\frac{1}{m} \cdot \mathcal{O}$ contains the ring of integers $\mathcal{O}_{\mathbf{K}}$ for some m co-prime to q. We will show that this condition implies that $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$ is co-prime to q. There is a cost in the reduction, as the noise in the Ring-LWE samples is required to be factor m larger than in the original reduction from ideals of $\mathcal{O}_{\mathbf{K}}$ [LPR10], with all else equal. We also show that this is a reasonable cost to pay, since with really small m, such as $m = 4$, for the popular power-of-two cyclotomic fields $\mathbf{K}$, there are orders $\mathcal{O}$ with $\mathcal{O}_{\mathbf{K}} \subset \frac{1}{m} \cdot \mathcal{O}$, such that $\mathcal{O}$ have non-trivial ideals that require at least three generators and are non-invertible. We also show that these non-trivial ideals are not contained in the conductor ideal (well known to be non-invertible), and thus we get a rich multiplicative set of non-invertible ideals. By the very definition of ideal-class *group*, this set lies outside the ideal-class group, and hence the whole range of attacks using ideal-class group are not applicable; see "Known Attacks on Ideal Lattices" below. This gives a rigorous explanation of why such attacks never managed to break RLWE, in whatever sense the break was of the ideal lattice problem based on ideal class groups, the most general of these being [CDW17] that used the Stickelberger relation for ring of integers of cyclotomic fields.

In more detail, we show that for any ideal $\mathcal{I}$ of order $\mathcal{O}$, such that $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$ is co-prime to q, the ideal $\mathcal{I}$ modulo $q\mathcal{I}$ is principal. This fact is well-known for Dedekind domains and is usually proven using unique prime-ideal factorization of Dedekind domains[5]. With the above condition on arbitrary $\mathcal{O}$, that $\mathcal{I}$ modulo $q\mathcal{I}$ is principal for $\mathcal{O}$ and the generator efficiently computable is also shown in [PP19] but using conductor-ideal theory and ultimately using the unique prime-ideal factorization of Dedekind domains. However, we prove it for all such orders using elementary ideal theory, and consequently we give a rather simple (classical) randomized algorithm to find the generator of the principal ideal $\mathcal{I}/q\mathcal{I}$, given a $\mathbb{Z}$-basis of $\mathcal{I}$ and without access to a basis of $\mathcal{O}$ [6]. The algorithm essentially takes a random $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$-linear combination of the columns of a given

[5] This fact is also implicitly used in the original ideal clearing lemma of [LPR10].

[6] The general problem of finding a generator of a principal ideal is only known to have a sub-exponential time classical algorithm [BF14], and a quantum polynomial time algorithm [BS16].

$\mathbb{Z}$-basis of $\mathcal{I}$. Finally, we prove that given only a $\mathbb{Z}$-basis of the ideal $\mathcal{I}$ and a generator of principal ideal $\mathcal{I}/(q\mathcal{I})$, we can efficiently *clear the ideal and the order* in the hardness reduction. Later, in Section 1.1, we give a more detailed overview of our techniques.

Naturally, our technique and novel randomized algorithm are also applicable to the order being $\mathcal{O}_{\mathbf{K}}$ but now working for all q. This leads to an improved (time complexity) reduction for the usual q-RLWE hardness as compared to [LPR10]. In addition, our technique does not require q to have a known-factorization, whereas [LPR10] does.

It is worth remarking that for every number field $\mathbf{K}$, there is a finite number m, namely $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$, 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 $\mathcal{O}$. Thus, the ideals (and corresponding lattices) in $\mathcal{O}$ include all hard ideal lattices coming from $\mathcal{O}_{\mathbf{K}}$. However, we show later that the reverse is not true. Moreover, we will give non-trivial examples of ideals of sub-orders $\mathcal{O}$ that require at least three generators and are consequently non-invertible. A comparison of all the relevant algebraic properties of ideals of $\mathcal{O}_{\mathbf{K}}$ and non-Dedekind $\mathcal{O}$ can be found in Table 1.

We also give another reduction that shows that hardness of q-Ring-LWE can be based on worst-case hardness of lattices that correspond to sum of ideal-lattices in arbitrary and different orders in the number field, as long as the (set of) orders $\{\mathcal{O}_i\}$ satisfy the property that $\frac{1}{m} \cdot \mathcal{O}_i$ contains the ring of integers, for some m co-prime to q. The reduction requires that the noise be a factor m more than the original Ring-LWE reduction. We also show that for the power-of-two cyclotomic number fields, there exist orders $\mathcal{O}_1, \mathcal{O}_2$ with $m = 8$ such that there are ideals $\mathcal{I}_1, \mathcal{I}_2$ of $\mathcal{O}_1, \mathcal{O}_2$ resp. with $\mathcal{I}_1 + \mathcal{I}_2$ not an ideal of any order in the number field. However, it can also be shown that every integer lattice of rank 2^n corresponds to a *fractional ideal* of some order in the 2^n-cyclotomic number field. Thus, the value of this reduction is not as clear cut as the earlier described reduction from ideals of hidden order.

Known Attacks on Ideal Lattices There are no known efficient classical/quantum algorithms for polynomial-factor approximation of SVP, SIVP etc for ideal lattices of $\mathcal{O}_{\mathbf{K}}$ (or sub-rings such as $\mathcal{R}_{\mathbf{K}}$), even restricted to prime-power cyclotomic fields. However, after a flurry of heuristic claims [Ber14,CGS14], the work [CDPR16] has shown that when restricted to principal ideals, the sub-exponential-approximate SVP problem can be solved in quantum polynomial time. The attack has two parts. First, an arbitrary generator of the principal ideal is computed by index-calculus method by first computing the ideal class group [BF14,BS16]. Second, a short generator is computed by running bounded-distance-decoding on Dirichlet's logunit lattice (i.e. the logarithms of the unit group that form a small ranked lattice) [CDPR16]. For general ideals in $\mathcal{O}_{\mathbf{K}}$, we know that $\mathcal{O}_{\mathbf{K}}$ being a Dedekind domain has the property that every ideal has at most two generators and in fact it is relatively easy to compute some pair of generators for every ideal using prime ideal factorization (see e.g. [FT91,LPR10]). However, now the above second step does not work as logarithm of additive terms is non-linear. We should remark that of the two generators one can always be taken to be a number, e.g. the norm of the ideal, although even this does not help in searching through the logunit lattice. So, more advanced techniques are required.

For cyclotomic fields, remarkably, [CDW17] use the Stickelberger relation and module (see e.g. [IR90]) to convert a general ideal to a (not too large generator) principal sub-ideal, and under some plausible assumptions, obtain a quantum polynomial time algorithm for sub-exponential-approximate SVP for general ideals of cyclotomic fields. However, the Stickelberger relation works using the Galois group of a cyclotomic extension of Q, so it does not extend to non-Galois fields. But even for cyclotomic fields and Galois fields it will not work for general (non-Dedekind) orders as not all ideals are invertible. Recall, the principal ideals are broken using index calculus on the ideal class group, but for non-maximal orders, the class group is only defined for the ideals that are invertible and not for all ideals (see the asterisk in line one of Table 1). So, none of the above techniques are expected to work on ideals of non-maximal orders. One may wonder that since the number of bad primes p', i.e. the ones that divide the index of $\mathcal{R}_{\mathbf{K}}$ in $\mathcal{O}_{\mathbf{K}}$, 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 [Cond, Theorem 8.6], the number of non-prime ideals contained in these prime ideals is unlimited. 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 $\mathcal{O}_{\mathbf{K}}$.

Algebraic Property	$\mathcal{O}_{\mathbf{K}}$	$\mathcal{O} \subsetneq \mathcal{O}_{\mathbf{K}}$
Class Group and Unit Group Computation [FT91,BF14]	Yes	Yes*
Irredundant Primary Decomposition of Ideals [AM69, Ch. 4]	Yes	Yes
Jordan-Hölder Filtration of Ideals [Cond,BBS21]	Yes	Yes
Tight bound on Shortest Vector [PR07,LPR10] (Lemma **??**)	Yes	Yes
Every Fractional Ideal is Invertible [Cla84,FT91,Cona]	Yes	No
Every Ideal co-prime to Conductor is Invertible [Cona]	Yes	Yes
Unique Prime Ideal Factorization (PIF) [Cla84,FT91]	Yes	No
PIF of ideals co-prime to Conductor [Cona]	Yes	Yes
Every Ideal can be generated by two elements [FT91]	Yes	No
Compute (two or more) generators given $\mathbb{Z}$-basis (e.g. [LPR10])	Yes	?
Ideal $\mathcal{I}$ mod $q\mathcal{I}$ is Principal (for q co-prime to index) (Secs. 3,4)	Yes	Yes

Table 1. Comparison of algebraic properties that an ideal lattice satisfies in the worst case. If a property is indicated with an affirmative, then it is also known to be efficiently computable (for class group, the claim is only for heuristic sub-exponential complexity[BF14]; moreover (*), for $\mathcal{O}$ the class group is only defined limited to the subset of invertible ideals of $\mathcal{O}$ (modulo group of *all* principal ideals) [Cona]). The question mark above indicates that it is an open problem.

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 a trace-product, but rather a polynomial multiplication. Thus, it is not enough that a lattice $\mathcal{L}$ and its dual lattice $\mathcal{L}^*$ have the property that $\mathcal{L}^\top \mathcal{L}^* = \boldsymbol{I}$. 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[7] 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 $\mathcal{O}$ could be a non Dedekind domain, the ideal $\mathcal{I}$ may not be invertible. However, we prove a more general clearing lemma that suffices for the reduction, and only requires that $\mathcal{I}$ be a principal ideal modulo $q\mathcal{I}$.

Related Work.

While [PP19] focuses on unifying all known versions and generalizations of Ring-LWE, Order-LWE, Module-LWE and others and showing that all of these can be based on hardness of usual RLWE and hardness of ideals in the Dedekind domain $\mathcal{O}_{\mathbf{K}}$, they do prove some interesting technical lemmas which can be seen as ideal-clearing lemmas. In particular, Theorem 4.1 in that work implies that for q-Order-LWE (in any order $\mathcal{O}$ in a number field with $\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$ co-prime to q), one can base its hardness on hardness of SIVP of sub-class of ideal (-lattices) of $\mathcal{O}$, namely restricted to ideal (-lattices) $\mathcal{I}$ that are invertible modulo ideal $q\mathcal{O}$ (or more generally any ideal $\mathfrak{q}$). The work [BBS21] actually relies on this theorem. But, [PP19] in another lemma also show that if $\mathfrak{q}$ is co-prime to the conductor ideal $\mathfrak{c}_{\mathcal{O}}$ of $\mathcal{O}$ (w.r.t. $\mathcal{O}_{\mathbf{K}}$), then every ideal of $\mathcal{O}$ is invertible modulo $\mathfrak{q}$. Thus, [PP19] already proves that hardness of q-Order-LWE (defined over $\mathcal{O}$) can be based on hardness of SIVP of ideal lattices in $\mathcal{O}$, whenever $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$ is co-prime to q – note it is easy to show that $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$ being co-prime to q implies that $\mathfrak{q}$ is co-prime to the conductor ideal $\mathfrak{c}_{\mathcal{O}}$ (see e.g. lemma 2.5). In this work, we also make a novel technical contribution by showing that $\mathfrak{q}$ being co-prime to the conductor ideal $\mathfrak{c}_{\mathcal{O}}$ implies that $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$ is co-prime to q (again see lemma 2.5). Thus the two conditions are equivalent whenever $\mathfrak{q}$ is of the form $q\mathcal{O}$.

As mentioned earlier, [PP19] has a taxonomical treatment of LWE-like problems, although the main focus is on proving that all versions of these problems can be reduced to usual Ring-LWE. Nevertheless, we remark that with some additional work their result also implies that Ring-LWE hardness can be based

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

on hardness of ideals in orders $\mathcal{O}$ as long as $(1/m) \cdot \mathcal{O}$ contains $\mathcal{O}_{\mathbf{K}}$ with m co-prime to q, and with the same penalty of noise blowing up by a factor of m. However, since their approach requires finding prime ideals of $\mathcal{O}$ above $q\mathcal{O}$, it definitely needs access to a basis of $\mathcal{O}$, so their reduction cannot be based on hard problems with hidden order.

In [RSW18], a reduction from decision (resp. search) RLWE in $\mathcal{O}_{\mathbf{K}}$ to decision (resp. search) polynomial-LWE [SSTX09] (i.e. with the ring $\mathcal{R}_{\mathbf{K}}$) is obtained, Since, the hardness of RLWE in $\mathcal{O}_{\mathbf{K}}$ 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. In [PP19], a more general framework is considered which encompasses Module-LWE [BGV12,LS15] and Order-LWE [BBPS19] and shows reductions from Ring-LWE to these other variants, and with tight reductions, but with the same limitation.

In [AD17], the authors show a reduction from module-LWE in dimension d to RLWE with modulus q^d. This reduction continues to hold for module version of Order-LWE in dimension d to q^d-Order-LWE as the main theorem in [AD17], Theorem 1, continues to hold for any order of the number field, and not just the ring of integers. This is because the main property used in the proof of that theorem is that ideals of the ring of integers are full-ranked as Z-modules. But this holds for all orders of a number field (see lemma 2.2).

Outline. The rest of the paper is organized as follows. The remaining part of Introduction contains a technical overview. Section 2 covers preliminaries of lattices, smoothing lemma, and hard problems over lattices. Section 2.1 covers basics of ideals. Section 2.4 introduces the polynomial ring calculus including dual ideals. Section 3 proves that ideal $\mathcal{I}$ is principal modulo $q\mathcal{I}$. Section 4 gives a novel randomized algorithm to find a generator for above principal ideal. Section 5 proves the pseudo-randomness of q-Ring-LWE using earlier works and the novel formulation of the ideal and order clearing lemma and its proof using the theory and algorithms developed in earlier sections. Section 6 gives examples of non-bigenic ideals.

1.1 Technical Overview

The state-of-the-art decisional Ring-LWE hardness, extended to lattices of ideals (of ring of integers) of all number fields, is the culmination of three works: the original Regev LWE-reduction [Reg05], the decisional Ring-LWE hardness for cyclotomic fields [LPR10], and the extension to all number fields [PRS17].

First, we briefly describe the main components of Regev's hardness reduction from discrete Gaussian sampling (DGS) over worst-case integer lattices to learning-with-error (q-LWE) modulo integer q. The DGS problem for a lattice $\mathcal{L}$ can be classically solved if the variance σ for the Gaussian sampling is sufficiently large, for instance $\sigma > 2^{2n}\lambda_n(\mathcal{L})$, where n is the dimension of the lattice and λ_n, as usual, is the minimum length of a set of n linearly independent vectors from $\mathcal{L}$. This step is also called the bootstrapping step of DGS. To obtain finer sampling, i.e. for σ approaching a polynomial factor away from $\lambda_n(\mathcal{L})$, Regev employs a recursive strategy involving two reductions:

1. A quantum reduction that allows one to solve finer DGS for $\mathcal{L}$ given a worst-case promise closest-vector-problem (CVP) oracle for the dual lattice $\mathcal{L}^\vee$. A promise-CVP oracle $\mathrm{CVP}_{\mathcal{L}^\vee,d}$ solves the closest vector problem as long as the input instance is promised to be within distance d of the lattice $\mathcal{L}^\vee$. The larger the promise under which the CVP oracle works, the finer is the DGS sampler, upto a limit. It is worth remarking that the main quantum components of this algorithm is a quantum fourier transform, and a computation (over superpositions) that computes a representative of point x modulo a given basic parallelepiped of $\mathcal{L}^\vee$.
2. A classical reduction that uses a q-LWE oracle, along with a fine DGS sampler for $\mathcal{L}$ to solve promise-CVP over the dual lattice $\mathcal{L}^\vee$. The finer the DGS sampler, the larger the promise that the CVP solver can handle. One hard problem solved in this step is what maybe referred to as "clearing the lattice". Note that the CVP input instance describes a point x close to some lattice point y of some lattice $\mathcal{L}^\vee$, whereas the q-LWE oracle which is used to solve this problem does not explicitly refer to any lattice. Regev's clever idea is to use the DGS sampler to sample a lattice vector v from $\mathcal{L}$, and take the inner product of v with x to obtain the LWE sample. Since the dual lattice, by definition, is spanned by $\mathcal{L}^{-\top}$, this leads to clearing of the lattice from the LWE instance.

The work [LPR10] essentially extended step 2 above to use a q-RLWE oracle to solve the CVP problem for ideal lattices, more precisely, the ideal lattices of dual of the *ring of integers* of the underlying number field. The reduction to the decisional RLWE problem was only shown for cyclotomic fields. The biggest challenge that was solved in this work was that the usual dual of a lattice, and in this case a lattice defined by a $\mathbb{Z}$-basis of an ideal $\mathcal{I}$ of the ring, need not itself be an ideal. Fortunately, this problem is well studied in number theory, and it is well-known that the appropriate lattice to consider is not the lattice defined by the $\mathbb{Z}$-basis of the ideal, but by the lattice embedded in $\mathbb{C}^n$, the n-dimensional complex domain, by the "canonical embedding". This canonical embedding is similar to a Fourier transform and is essentially the linear transform defined by the Vandermonde matrix of $f(X)$, where $f(X)$ is the irreducible polynomial that defines the number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$.

Once we consider these embedded lattices, it turns out that the usual notion of a dual lattice leads to a lattice that does correspond to a (fractional) ideal of the same ring. This (fractional) ideal is referred to as the dual ideal $\mathcal{I}^\vee$ of the original ideal $\mathcal{I}$. This is crucial in solving the "clearing the lattice" problem in step 2 above, where the problem is more complicated now as the RLWE sample generation uses polynomial (or number field) multiplication, and hence clearing the lattice must also employ polynomial multiplication and not an inner product; the latter sufficed for LWE. This is one of the main reasons that working with the *dual ideal* is helpful, although it still doesn't immediately solve the problem.

To fully tackle the problem [LPR10] formulated and proved an "ideal clearing lemma", which informally showed the following:

(i) an efficient isomorphism ψ that maps the finely sampled v (from the ideal $\mathcal{I}$ or its corresponding lattice $\mathcal{L}$) to the ring modulo q,

(ii) an efficiently invertible isomorphism ϕ that maps y, a lattice point in lattice $\mathcal{L}^\vee$ of dual ideal $\mathcal{I}^\vee$ (or equivalently treating y as an element of ideal $\mathcal{I}^\vee$) to the dual of the ring (again, modulo q),

(iii) such that $\psi(v) * \phi(y) = v * y \pmod{q}$, where '*' is the polynomial multiplication in the number field (*ideal clearing property*).

Note that the image of ϕ and ψ lie in the ring and the dual of the ring respectively, and do not refer to the ideal or the lattice, and hence the name "ideal clearing lemma". More importantly, it is imperative to show that these isomorphisms are efficiently computable (invertible resp.) given only some basis of the ideal (or the corresponding lattice). This, however, is not an easy task and requires algorithms from computational number theory, and in particular the unique prime ideal factorization of ideals of Dedekind domains. [LPR10] show an invertible isomorphism ψ, as required above, by computing an element t in the ideal $\mathcal{I}^\vee$ such that $t \cdot \mathcal{I}^{-\vee}$ is co-prime to ideal (q). Intuitively, multiplication by t serves as the inverse of isomorphism ψ by noting the following: multiplication by any t in $\mathcal{I}^\vee$ would map the dual of the ring to the ideal $\mathcal{I}^\vee$. However, if the principal ideal (t) shares some prime ideals with factorization of (q), then this would not be a bijection. Thus, by requiring that $t \cdot \mathcal{I}^{-\vee}$ is coprime to (q), the map becomes bijective. But, note that this reasoning only holds in a ring where there is unique prime ideal factorization, and hence this technique only works for rings which have unique prime ideal factorization. It is well-known that the ring of integers $\mathcal{O}_\mathbf{K}$ of a number field $\mathbf{K}$ is a Dedekind domain which is also well-known to have unique prime ideal factorization. Further, all strict sub-rings of ring of integers of a number field are known to be non-Dedekind domain, and also *not* have unique prime ideal factorization.

1.2 Extension to Arbitrary Orders in the Number Field

In this work, we achieve the ideal clearing lemma by a slightly different strategy, which not just simplifies the claim for Dedekind domains, but is also applicable for $\mathcal{O}$, as long as q is co-prime to index of $\mathcal{O}$ in $\mathcal{O}_\mathbf{K}$ (denoted $[\mathcal{O}_\mathbf{K} : \mathcal{O}]$). The alternate strategy requires showing that for any ideal $\mathcal{I}$ of $\mathcal{O}$, and any such q, the ideal $\mathcal{I}/q\mathcal{I}$ is a principal ideal of the ring $\mathcal{O}/q\mathcal{I}$. We also give a simple and novel randomized algorithm to find a generator for this principal ideal. Finally, we show that with this generator in hand, we can give the requisite isomorphisms ϕ and ψ above, which are easily shown to be efficiently computable and invertible, and which satisfy the ideal clearing property.

Since the proof of ideal clearing lemma requires some key lemmas involving the dual ideal, which in turn is defined using the canonical embedding, we begin by giving in section 2.4 a basic introduction to dual ideals, especially tailored for the orders $\mathcal{O}$. The core of our work is in showing that $\mathcal{I}/q\mathcal{I}$ is a principal ideal of the ring $\mathcal{O}/q\mathcal{I}$, and we achieve this goal in a relatively elementary way, without invoking advanced techniques such as localization, Jordan-Holder decomposition, and of course neither the Dedekind domain prime ideal factorization.

We briefly describe how we prove that $\mathcal{I}/q\mathcal{I}$ is a principal ideal of the ring $\mathcal{O}/q\mathcal{I}$. We first prove that $\mathcal{O}/q\mathcal{O}$ is a principal ideal domain. For Dedekind domains, this is a well-known result, and holds for all q, in fact modulo all ideals. For general orders, it well-known that $q\mathcal{O}$ is a product of prime ideals (i.e. when q is co-prime to $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$), say $q\mathcal{O} = \mathfrak{p}_1^{e_1} \cdot \mathfrak{p}_r^{e_r}$. Next, any ideal $\mathfrak{a}$ is shown to be a product of an ideal $\hat{\mathfrak{a}}$ (co-prime to all the above ideals $\mathfrak{p}_i$) and product of some powers of above $\mathfrak{p}_i$. This is possible as ideals in orders are full-ranked sub-groups. With this factorization in hand, we first show that each of $\mathcal{O}/\mathfrak{p}_i^{e_i}$ is a principal ideal ring, which just requires showing that $\mathfrak{p}_i$ is principal modulo $\mathfrak{p}_i^{e_i}$ for $e_i > 1$. This is the trickiest part of the proof, and uses (recursive) factorization as above of each principal ideal (z) for $z \in \mathfrak{p}_i$, and shows that one of these must be the whole ideal $\mathfrak{p}_i$ (modulo $\mathfrak{p}_i^{e_i}$). The rest of the proof follows by Chinese remainder theorem.

The most interesting part of the proof is that it shows that every nonzero ideal $\mathfrak{a}$ modulo $\mathfrak{p}_i^{e_i}$ is generated by a power of a same $z \in \mathfrak{p}$ (see theorem 3.4). This allows us to give a simple randomized algorithm for the principal ideal $\mathcal{I}/q\mathcal{I}$, given any $\mathbb{Z}$-basis for the ideal $\mathcal{I}$. Indeed, the simple algorithm picks n random elements $\rho_k(X)$ ($k \in [n]$) from $\mathcal{O}/q\mathcal{O}$. Next, we view each of the n columns of the $\mathbb{Z}$-basis of $\mathcal{I}$ as polynomials, say $\gamma_k(X)$, which are all generated by power of a same z (modulo each $\mathfrak{p}_i$). The algorithm simply outputs $\sum_{k\in[n]} \gamma_k(X) * \rho_k(X)$. We prove that this is a generator of the principal ideal with a decent non-negligible probability.

2 Preliminaries

2.1 Ideal Basics

Let R be any commutative ring with unity. An (integral) *ideal* $\mathcal{I} \subseteq R$ is an additive subgroup that is closed under multiplication by the elements from R. A fractional ideal $\mathcal{I}$ is a subset of R, such that there exists an element $r \in R$ that makes $r \cdot \mathcal{I}$ an integral ideal of R. An ideal $\mathcal{I}$ of R is **invertible** if there exists a fractional ideal $\mathcal{J}$ such that $\mathcal{I}\mathcal{J} = R$. An ideal $\mathcal{I}$ 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 $\mathcal{P}$ such that $ab \in \mathcal{P}$ implies $a \in \mathcal{P}$ or $b \in \mathcal{P}$. A **primary ideal** of a ring R is an ideal $\mathcal{P}$ such that $ab \in \mathcal{P}$ implies $a \in \mathcal{P}$ or $b^n \in \mathcal{P}$ for some $n \geq 1$. 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 $\mathcal{I}$ and $\mathcal{J}$ are called **co-prime** if $\mathcal{I} + \mathcal{J} = (1)$. An element $c \in R$ will be called **invertible modulo an ideal** $\mathcal{I}$ if there exists a $\mu \in R$ and $\lambda \in \mathcal{I}$ such that $\mu c = 1 + \lambda$. In other words, c is a **unit** of quotient ring $R/\mathcal{I}$.

We enumerate a list of well-known facts about ideals, with elementary proofs, in appendix A.

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

Theorem 2.1 (Chinese Remainder Theorem (CRT)). *Let $\mathcal{I}_1, ..., \mathcal{I}_k$ be a set of pairwise co-prime ideals of a ring R. Then, $R/\mathcal{I}_1 \cdots \mathcal{I}_k \equiv \prod_i R/\mathcal{I}_i$.*

2.2 Basic Algebraic Number Theory

A number field is a finite extension of the field of rational numbers $\mathbb{Q}$. By the celebrated primitive element theorem, every number field $\mathbf{K}$ is isomorphic to $\mathbb{Q}[X]/(f(X))$ where $f(X) \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Q}$, and $[\mathbf{K} : \mathbb{Q}]$ is the degree of the polynomial $f(X)$. Let R be a subring of a ring R'. An element $x \in R'$ is said to be **integral** over R if it satisfies a monic polynomial equation, where the polynomial has coefficients in R. The **ring of integers** of a number field $\mathbf{K}$, denoted $\mathcal{O}_{\mathbf{K}}$, are the set of elements of $\mathbf{K}$ that are integral over $\mathbb{Z}$. Thus, $\mathcal{O}_{\mathbf{K}}$ is integrally closed. The ring of integers can in general be a strict super-ring of the polynomial ring $\mathcal{R}_{\mathbf{K}} = \mathbb{Z}[X]/(f(X))$. However, for cyclotomic fields, the ring of integers $\mathcal{O}_{\mathbf{K}}$ is same as $\mathcal{R}_{\mathbf{K}}$ (see Appendix F for a proof). It is well-known that the ring of integers $\mathcal{O}_{\mathbf{K}}$ of a number field is a Dedekind domain (see e.g. [FT91]). Even though our work does not employ Dedekind domains other than for comparison purposes, we give a brief introduction to Dedekind domains in Appendix E.

Generalizing the rings $\mathcal{O}_{\mathbf{K}}$ and $\mathcal{R}_{\mathbf{K}}$, an **order** $\mathcal{O}$ in the field $\mathbf{K}$ is a subring of $\mathbf{K}$ that is finitely generated as a $\mathbb{Z}$-module and contains a $\mathbb{Q}$-basis of $\mathbf{K}$. Orders in $\mathbf{K}$ are the subrings of $\mathcal{O}_{\mathbf{K}}$ with finite index, and hence $\mathcal{O}_{\mathbf{K}}$ is referred to as the maximal order. Since a Dedekind domain is integrally closed, the non-maximal orders are not Dedekind domains. However, orders share many features of the maximal order $\mathcal{O}_{\mathbf{K}}$ (see e.g. [Cond, Section 8]):

Lemma 2.2. (i) *An order in $\mathbf{K}$ is an integral domain and has fraction field $\mathbf{K}$.*
(ii) *All nonzero prime ideals in an order are maximal.*
(iii) *Every order has a $\mathbb{Z}$ basis that can be chosen to include* 1.
(iv) *All nonzero ideals in an order are finitely generated as a free $\mathbb{Z}$-module with rank $n = [\mathbf{K} : \mathbb{Q}]$.*
(v) *Given a rank n $\mathbb{Z}$-basis matrix of a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}$, $\boldsymbol{B}(\mathfrak{a})$, every sub-ideal $\mathfrak{m}$ of $\mathfrak{a}$ is the $\mathbb{Z}$-span of $\boldsymbol{B}(\mathfrak{a}) \cdot \boldsymbol{M}$, where $\boldsymbol{M}$ is an integer $n \times n$ matrix. Consequently, det($\boldsymbol{M}$) is same as $[\mathfrak{a} : \mathfrak{m}]$. Similar claim holds for orders $\mathcal{O}$ that are subset of (rationally scaled) orders $\mathcal{O}'$.*
(vi) *For every nonzero prime ideal $\mathfrak{p}$ of $\mathcal{O}$, and for every $r \geq 0$, $\mathfrak{p}^r \neq \mathfrak{p}^{r+1}$.*

The proof of (*iv*) follows by computing Hermite normal form. The proof of determinant in (*v*) follows by combining the structure theorem of finitely generated abelian groups [Lan02, Theorem 8.2] and the elementary divisors theorem of finitely generated submodules [Lan02, Theorem 7.8] (aka Smith Normal Form). The proof of (*vi*) follows from the generalized Cayley-Hamilton theorem (see e.g. [AM69, Corr. 2.5] or [Eis13], cf. Nakayama's lemma [AM69, Lemma 2.6]). For general orders, it is not necessary that $[\mathfrak{p}^r : \mathfrak{p}^{r+1}]$ is constant, whereas for the maximal order this is true.

Theorem 2.3. *([Cond, Theorem 8.6]) Let $m = [\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$. Every prime ideal $\mathfrak{p}$ of $\mathcal{O}$, such that $m\mathcal{O} \not\subset \mathfrak{p}$, is invertible.*

The proof of the following lemma is similar to proof of [Cona, Theorem 3.6] and can be found in Appendix A.

Lemma 2.4. *Let $m = [\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$. An ideal $\mathfrak{b}$ of $\mathcal{O}$ that is relatively prime to principal ideal $m\mathcal{O}$ is a product of prime ideals of $\mathcal{O}$.*

Note that in this work we will not require that this factorization of $\mathfrak{b}$ be unique, although it can be shown to be unique with considerable more work; in particular, by using the following lemma 2.5, the bijection between ideals of $\mathcal{O}$ and $\mathcal{O}_{\mathbf{K}}$ that are coprime to the conductor ideal [Cona, Theorem 3.8], and the famous unique factorization of ideals theorem for the Dedekind domain $\mathcal{O}_{\mathbf{K}}$ (see appendix E).

The **conductor** of an order $\mathcal{O}$ in the number field $\mathbf{K}$ is $\mathfrak{c} = \mathfrak{c}_{\mathcal{O}} = \{x \in \mathbf{K} : x\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}\}$. It is easy to check that $\mathfrak{c}_{\mathcal{O}}$ is an ideal of both $\mathcal{O}$ and $\mathcal{O}_{\mathbf{K}}$.

Lemma 2.5. *Let $m = [\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$. If an ideal $\mathfrak{b}$ of $\mathcal{O}$ is relatively prime to principal ideal $m\mathcal{O}$ then $\mathfrak{b}$ is relatively prime to the conductor ideal $\mathfrak{c}_{\mathcal{O}}$. The converse also holds when $\mathfrak{b}$ is restricted to ideals of the form $q\mathcal{O}$, where q is an integer.*

While the proof of the first statement of the lemma is well-known, we prove the converse using the primary-decomposition theorem of ideals of Noetherian rings; to the best of our knowledge this result was not known before [Cone].

Proof. – The first statement of the lemma is well-known and the following proof is due to [Cone]. We have $\mathfrak{b} + m\mathcal{O} = \mathcal{O}$. We just need to show that $m\mathcal{O} \subset \mathfrak{c}_{\mathcal{O}}$. Recall, by definition of the conductor, if $x \in \mathfrak{c}$ iff for every $y \in \mathcal{O}_{\mathbf{K}}$, $xy \subset \mathcal{O}$. But, for every $y \in \mathcal{O}_{\mathbf{K}}$, $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]y \in \mathcal{O}$. Thus, $m \in \mathfrak{c}$ and hence also $m\mathcal{O} \subset \mathfrak{c}$.

- For the converse, we show the contrapositive: if $q\mathcal{O}$ is not coprime to $m\mathcal{O}$ then $q\mathcal{O}$ is not coprime to $\mathfrak{c}$. Since, $q\mathcal{O}$ is not coprime to $m\mathcal{O}$, there is a prime p (factor of q) such that p divides $m = [\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$. We will show that $p\mathcal{O} + \mathfrak{c} \neq \mathcal{O}$, and the claim would follow as $q\mathcal{O} \subset p\mathcal{O}$.
  1. Since prime p divides $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$, there is a $b \in \mathcal{O}_{\mathbf{K}}$ such that $b \in (1/p)\mathcal{O}$–$\mathcal{O}$.
  2. Thus, pb is an element of $\mathcal{O}$ that is not in ideal $p\mathcal{O}$.
  3. Consider an irredundant primary decomposition of ideal $p\mathcal{O}$ of the Noetherian ring $\mathcal{O}$ ([AM69]), with primary ideals $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r$ with corresponding associated distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ (with $\mathfrak{p}_i$ being the radical ideal of $\mathfrak{q}_i$).
  4. Thus, $p\mathcal{O} = \cap_{i\in[r]}\mathfrak{q}_i$.
  5. Now, for any c in conductor $\mathfrak{c}$: $bc \in \mathcal{O}$, and hence $pbc \in p\mathcal{O}$, with $pb \notin p\mathcal{O}$ (by item 2).
  6. If $p\mathcal{O}$ were a prime ideal this would already imply $c \in p\mathcal{O}$, and hence $\mathfrak{c} \subset p\mathcal{O}$ and we would be done. If $p\mathcal{O}$ is not a prime ideal, we continue by noting that we have for all $i \in [r]$: $pbc \in \mathfrak{q}_i$ (by item 4).

7. Also, for all $i \in [r] \ : \ pbc \in \mathfrak{p}_i$ (by item 3). Let R be the subset of $[r]$ such that $pb \in \mathfrak{p}_i$. If R is a strict subset of $[r]$, then $c \in \prod_{j\in[r]\setminus R} \mathfrak{p}_j$. And hence $\mathfrak{c} \subseteq \prod_{j\in[r]\setminus R} \mathfrak{p}_j$. Since $p\mathcal{O}$ is subset of each $\mathfrak{p}_j$, this implies $p\mathcal{O} + \mathfrak{c} \subseteq \prod_{j\in[r]\setminus R} \mathfrak{p}_j$ which is strict subset of $\mathcal{O}$, and we are done.
8. The remaining case is that $R = [r]$. In other words, for all $j \in [r]$, $pb \in \mathfrak{p}_i$. Yet, since pb is not in $p\mathcal{O}$ (by item 2), there is some nontrivial subset T of $[r]$ such that for $i \in T \ : \ pb \notin \mathfrak{q}_i$. But, $pbc \in \mathfrak{q}_i$ for all i (by item 6).
9. Thus, since $\mathfrak{q}_i$ is a primary ideal, c is in radical of $\mathfrak{q}_i$, i.e. $\mathfrak{p}_i$ (for all $i \in T$). Thus, $\mathfrak{c} \subseteq \cap_{i\in T}\mathfrak{p}_i$. However, by item 4, $p\mathcal{O}$ is also subset of $\cap_{i\in T}\mathfrak{q}_i$ which in turn is subset of $\cap_{i\in T}\mathfrak{p}_i$, since each $\mathfrak{q}_i$ is contained in its radical ideal $\mathfrak{p}_i$. Thus, $p\mathcal{O} + \mathfrak{c} \subset \cap_{i\in T}\mathfrak{p}_i$, and since $\mathfrak{p}_i$ are maximal and hence proper ideals these are strict subsets of $\mathcal{O}$, and we are done.

The proof of the following well-known lemma [Cone] can be found in Appendix A.

Lemma 2.6. *Let $m = [\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$, and q be a positive integer relatively prime to m. Then, the quotient ring $\mathcal{O}/q\mathcal{O}$ is isomorphic to $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$ by the ring isomorphism $\phi \ : \ \mathcal{O}/q\mathcal{O} \to \mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}} \ :: \ \phi(\mathbf{x}) = \ell \cdot \mathbf{x} \bmod q\mathcal{O}_{\mathbf{K}}$, where ℓ is any integer such that $\ell{\cdot}m = 1 \bmod q$. The isomorphism ϕ is inverted by multiplication by m.*

2.3 The Canonical Space $\mathcal{H}$, Lattices, and Hard Lattice Problems

We'll be working with 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.

To start with, we will work with the ring $\mathcal{R}_{\mathbb{Q}} = \mathbb{Q}[X]/(f(X))$. When $f(X)$ is irreducible, $\mathbf{K} = \mathcal{R}_{\mathbb{Q}}$ is a number field. Later, we will develop the theory for many sub-rings such as $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, its modulo q version $\mathcal{R}_q = \mathbb{Z}_q[X]/(f(X))$ for some $q \in \mathbb{Z}$, and in general any order in $\mathbf{K}$.

For clarity, we use operator "$*$" for polynomial multiplication, operator "$\cdot$" for matrix multiplication, and operator "$\times$" for cartesian product.

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 general 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 $s_1 + 2s_2 = n$:

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

We now describe the canonical embedding from the polynomial ring $\mathcal{R}_{\mathbb{Q}}$ 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** $\varDelta_f$ of a polynomial is defined to be the square of the determinant of the Vandermonde matrix of $f(X)$. In corollary B.3 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 $g(X)$ and its vector representation $\mathbf{g}$, 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 $\mathcal{H}$:

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

It's dual is defined as $\mathcal{L}^\vee = \left\{ \mathbf{y} \in \mathcal{H} \mid \forall \mathbf{x} \in \mathcal{L} : \langle \mathbf{y}, \mathbf{x} \rangle = \mathbf{y}^H \mathbf{x} \in \mathbb{Z} \right\}$. 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 $G = \left\{ \mathbf{r} \in \mathbb{R}_+^n \mid \mathbf{r}_{s_1+i} = \mathbf{r}_{s_1+s_2+i}, 0 \le i < s_1 \right\}$. 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 $\rho_{1/\mathbf{r}}(\mathcal{L}^\vee \setminus \{0\}) \leq \epsilon$ where $1/\mathbf{r} = (1/r_0, 1/r_1, \ldots, 1/r_{n-1})$.*

Lemma 2.7 ([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 2.8 ([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 2.9 ([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 $\mathbf{x} \in \mathcal{L}$.

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 $D_{\mathcal{L},r}$.*

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 $\mathbf{e}$.*

More specifically, in this work, we consider the above problems restricted to the *ideal lattices*, when lattices are generated by ideals of orders in the field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$– see section 2.5.

2.4 Polynomial Ring Calculus

Circulant Matrices In polynomial ring modulo $f(X)$, the **circulant matrix** (modulo $f(X)$) or multiplication matrix 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 $i = 0, 1, \ldots, n-1$.

It's not difficult to see that circulant matrices are closed under addition and multiplication. Moreover, the multiplication commutes. For any two ring elements $g(X)$ and $h(X)$:

- $\boldsymbol{C}_g + \boldsymbol{C}_h = \boldsymbol{C}_{g+h}$.

– $\boldsymbol{C}_g \cdot \mathbf{h}$ corresponds to their product $g(X) * h(X)$.
– $\boldsymbol{C}_g \cdot \boldsymbol{C}_h = \boldsymbol{C}_{g*h} = \boldsymbol{C}_{h*g} = \boldsymbol{C}_h \cdot \boldsymbol{C}_g$.

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

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 $\boldsymbol{C}_g$. If $g(X)$ is from $\mathcal{R} = \mathbb{Z}[X]/(f(X))$, $\boldsymbol{C}_g$ is integer, and 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 $\mathcal{R}_{\mathbb{Q}}$ to its evaluation domain $\mathcal{H}$. We now demonstrate that, the Vandermonde matrix $\boldsymbol{V}$ diagonalizes the circulant matrices into its canonical embedding.

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 $(\boldsymbol{V} \cdot \boldsymbol{C}_g)_{i,j} = p_j(z_i)$ where $p_j(X) = g(X) * X^j \pmod{f(X)}$. In other words, $p_j(X) = g(X)X^j - t_j(X)f(X)$ for some polynomial $t_j(X)$, we have

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

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

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 **(field) norm** of $g(X)$ in the extension field $\mathcal{R}_{\mathbb{Q}}$ of $\mathbb{Q}$.

2.5 Ideal Lattices and Dual Ideals

Ideal Lattice. By lemma 2.2 (*iv*), an ideal $\mathcal{I}$ of any order $\mathcal{O}$ in $\mathbf{K}$ has a rank n $\mathbb{Z}$-basis, typically denoted by $\boldsymbol{B}(\mathcal{I})$, which defines a lattice in $\mathcal{O} \subseteq \mathcal{R}_{\mathbb{Q}}$. 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 $\boldsymbol{V} \cdot \boldsymbol{B}(\mathcal{I})$. Similarly, the order itself has a rank n $\mathbb{Z}$-basis, typically denoted by $\boldsymbol{B}(\mathcal{O})$, which leads to the following lemma.

Lemma 2.10. *The principal ideal $g\mathcal{O}$ of order $\mathcal{O}$ generated by a $g \in \mathcal{O}$ has a $\mathbb{Z}$-basis $\boldsymbol{C}_g \cdot \boldsymbol{B}(\mathcal{O})$.*

Ideal Lattice Dual. For an ideal $\mathcal{I}$ or any rank n lattice in $\mathcal{R}_{\mathbb{Q}}$, the dual of its lattice $\mathcal{L}(\mathcal{I})$ in $\mathcal{H}$ is defined to be $\mathcal{L}(\mathcal{I})^* = \left\{\mathbf{y} \in \mathcal{H} \mid \forall \mathbf{x} \in \mathcal{L}(\mathcal{I}),\, \mathbf{y}^H \cdot \mathbf{x} \in \mathbb{Z}\right\}$. 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 or any $\mathcal{R}_{\mathbb{Q}}$-lattice itself using *trace pairing*. Recall that, abusing notation, $\mathbf{a} * \mathbf{b}$ denotes the coefficients vector of polynomial $a(X) * b(X)$ modulo $f(X)$. The trace pairing of $a(X), b(X) \in \mathcal{R}_{\mathbb{Q}}$, $\operatorname{Tr}(a(X), b(X))$ is defined to be trace of $\boldsymbol{V} \cdot (\mathbf{a} * \mathbf{b})$ which is same as $(\boldsymbol{V}\mathbf{a})^\top \cdot (\boldsymbol{V}\mathbf{b})$. Thus, we can define the dual $\mathcal{I}^\vee$ of $\mathcal{I}$ to be the set

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

Note that this is the pre-image in $\mathcal{R}_{\mathbb{Q}}$ of the complex conjugate of $\mathcal{L}(\mathcal{I})^*$. We state below that when $\mathcal{I}$ is an ideal of an order $\mathcal{O}$, this is indeed a (fractional) ideal of $\mathcal{O}$ (see Appendix B for a proof). Hence, we will refer to $\mathcal{I}^\vee$ as the **dual ideal** of $\mathcal{I}$, whenever $\mathcal{I}$ itself is an ideal.

Lemma 2.11. *For an ideal $\mathcal{I}$ of $\mathcal{O}$ with $\mathbb{Z}$-basis $\boldsymbol{B}(\mathcal{I})$, the dual $\mathcal{I}^\vee$ is a fractional ideal of $\mathcal{O}$ with $\mathbb{Z}$-basis*[8] $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}$*, the latter with entries in $\mathbb{Q}$.*

The Dual (of the) Ring. When the entire ring $\mathcal{O}$ is considered as an ideal, its dual $\mathcal{O}^\vee$, by lemma 2.11, is a fractional ideal given by the $\mathbb{Z}$-basis matrix $(\boldsymbol{V}^\top\boldsymbol{V})^{-1} \cdot \boldsymbol{B}(\mathcal{O})^{-\top}$. See Appendix B for a full characterization of the dual ideal $\mathcal{O}^\vee$ and proofs of the following three lemmas (that will be used in proving the ideal clearing lemma).

Lemma 2.12. *For an ideal $\mathcal{I}$ of $\mathcal{O}$, for any $\mathbf{a} \in \mathcal{I}$ and any $\mathbf{b} \in \mathcal{I}^\vee$, $\mathbf{a} * \mathbf{b} \in \mathcal{O}^\vee$.*

Lemma 2.13. *For $g(X) \in \mathcal{R}_{\mathbb{Q}}$, we have $\boldsymbol{C}_g(\boldsymbol{V}^\top\boldsymbol{V})^{-1} = (\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{C}_g^\top$, and $(\boldsymbol{V}^\top\boldsymbol{V})\boldsymbol{C}_g = \boldsymbol{C}_g^\top(\boldsymbol{V}^\top\boldsymbol{V})$.*

Lemma 2.14. *Let $\mathcal{O}_1$ be a sub-order of $\mathcal{O}_2$, both orders of rank n. If for some integer m, $m\mathcal{O}_2 \subset \mathcal{O}_1$, then $[\mathcal{O}_2 : \mathcal{O}_1]$ divides m^n. Further, $m\mathcal{O}_1^\vee \subset \mathcal{O}_2^\vee$.*

We give a counterpart of [PRS17, Lemma 6.9]. The proof is similar and can be found in Appendix B. Define the discriminant of an order $\mathcal{O}$ (with a $\mathbb{Z}$-basis $\boldsymbol{B}(\mathcal{O})$) of a number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$ to be $\operatorname{disc}(\mathcal{O}) = \det(\boldsymbol{B}(\mathcal{O}))^2 \cdot \Delta_f$.

Lemma 2.15. *For any ideal $\mathcal{I}$ of order $\mathcal{O}$ in number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$, and $\mathbf{r} \in \mathcal{H}$, where*

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

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

[8] When $\mathcal{I}$ is not an ideal of an order, but just any $\mathcal{R}_{\mathbb{Q}}$-lattice, the basis of the dual is still given by $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}$, eben though it is not an ideal.

3 Principal Ideal Lemma for $\mathcal{I}/q\mathcal{I}$ for Ideals $\mathcal{I}$ in Orders $\mathcal{O}$ with index co-prime to q.

Let $\mathcal{O}$ be an order in number field $\mathbf{K}$. Let q be an integer that is co-prime to the index m of $\mathcal{O}$ in $\mathcal{O}_{\mathbf{K}}$, i.e. $m = [\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$. In this section we will show that for every such q, the ring $\mathcal{O}/q\mathcal{O}$ is a principal ideal ring (PIR). Moreover, for such q, we show that every ideal $\mathfrak{a}$ of $\mathcal{O}$, modulo the ideal $q\mathfrak{a}$, is principal. Normally, such a claim holds for Dedekind domains, and the usual proofs require the unique prime ideal decomposition theorem for Dedekind domains. We show that if the ring is an order in a number field, even though it may not be a Dedekind domain, it can directly be shown that the ring $\mathcal{O}/q\mathcal{O}$ is a PIR.

To start with, by lemma 2.4, $q\mathcal{O}$ is a product of prime ideals of $\mathcal{O}$, which we state as a lemma below.

Lemma 3.1. *In the order $\mathcal{O}$, for any q that is co-prime to m, the ideal (q) is same as $\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}...\mathfrak{p}_r^{e_r}$, for some distinct prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_r$ of $\mathcal{O}$, and positive integers $e_1, ..., e_r$.*

From now on, fix some (not necessarily unique) r, $\mathfrak{p}_1, ..., \mathfrak{p}_r$ and $e_1, ..., e_r$ that can be associated with q as guaranteed in the lemma above. The following theorem follows from above and CRT.

Theorem 3.2.

$$\mathcal{O}/q\mathcal{O} \cong \prod_{i=1}^{r} \mathcal{O}/\mathfrak{p}_i^{e_i}$$

The rest of the section is devoted to proving that $\mathcal{O}/q\mathcal{O}$ is a principal ideal ring (PIR) (Theorem 3.4 below), and any ideal $\mathfrak{a}$ is principal modulo $q\mathfrak{a}$ (Theorem 3.7). If $\mathcal{O}$ was a Dedekind domain, the usual proof goes as follows: One first shows that $\mathcal{O}/\mathfrak{p}_i$ is isomorphic to $\mathcal{O}_{\mathfrak{p}_i}/\mathfrak{p}_i\mathcal{O}_{\mathfrak{p}_i}$, where $\mathcal{O}_{\mathfrak{p}_i}$ is the *localization* of $\mathcal{O}$ at the ideal $\mathfrak{p}_i$. 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 $\mathcal{O}_{\mathfrak{p}_i}$ is a principal ideal ring 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 PIR is a PIR, the claim follows.

While our ring $\mathcal{O}$ may not be a Dedekind domain, most of the above steps would still go through for our special q, except for proving that $\mathcal{O}_{\mathfrak{p}_i}$ is a DVR, which is usually proved using the prime ideal decomposition theorem for Dedekind domains. Luckily, even for general orders, we can still prove $\mathcal{O}_{\mathfrak{p}_i}$ is a DVR without the decomposition theorem for Dedekind Domains. As promised, we give a direct proof of Theorem 3.4.

Lemma 3.3. *Any ideal $\mathfrak{a}$ of $\mathcal{O}$ can be written as $\hat{\mathfrak{a}} \cdot \prod_{i\in[r]} \mathfrak{p}_i^{t_i}$, where t_i are non-negative integers, and $\hat{\mathfrak{a}}$ is an ideal of $\mathcal{O}$ co-prime to every $\mathfrak{p}_i$ $(i \in [r])$.*

Proof. If $\mathfrak{a}$ is co-prime to every $\mathfrak{p}_i$ $(i \in [r])$, then t_i can be taken to be zero, and we are done. Otherwise, let $I \subseteq [r]$ be the non-empty and maximal set of indices i, $i \in [r]$, such that $\mathfrak{a}$ is not co-prime to $\mathfrak{p}_i$. Since each $\mathfrak{p}_i$ is prime and maximal, 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 as $[\mathcal{O} : \mathfrak{a}]$ is fixed, and $[\mathcal{O} : \mathfrak{p}_i^{t(i)}]$ becomes large with increasing $t(i)$ by lemma 2.2 (v)& (vi).

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

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

$$\frac{1}{q^T} \cdot \mathfrak{a} \cdot \prod_{i\in I} \left(\mathfrak{p}_i^{(e_i-1)t(i)} * \prod_{j\in[r], j\neq i} \mathfrak{p}_j^{e_j t(i)} \right).$$

Using lemma 3.1, it is straightforward to check that $\hat{\mathfrak{a}} \cdot \prod_{i\in I} \mathfrak{p}_i^{t(i)} = \mathfrak{a}$.

We now show that $\hat{\mathfrak{a}}$ is actually an integral ideal, i.e. an ideal of $\mathcal{O}$. We claim that $\mathfrak{a} \cdot \prod_{i\in I} \left(\mathfrak{p}_i^{(e_i-1)t(i)} * \prod_{j\in[r], j\neq i} \mathfrak{p}_j^{e_j t(i)} \right)$ is in $(q)^T$. 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 $\mathfrak{a} \subseteq \prod_{i\in I} \mathfrak{p}_i^{t(i)}$. Claim then follows from factorization of (q) given by lemma 3.1. We now prove the second claim of the lemma.

Claim: Ideal $\hat{\mathfrak{a}}$ is co-prime to every $\mathfrak{p}_i$, $i \in [r]$.

Proof of Claim: By maximality of I, we already have that for all $i \in [r] \setminus I$, $\hat{\mathfrak{a}}$ is co-prime to $\mathfrak{p}_i$. Now, if there exists an $i \in I$, say i^*, such that $\hat{\mathfrak{a}}$ is not co-prime to $\mathfrak{p}_{i^*}$, then since the latter is a maximal ideal, $\hat{\mathfrak{a}}$ is contained in $\mathfrak{p}_{i^*}$. But, since $\mathfrak{a} = \hat{\mathfrak{a}} \cdot \prod_{i\in I} \mathfrak{p}_i^{t(i)}$, 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 3.4. *For all $j \in [r]$, and all integers $e \geq 1$, $\mathcal{O}/\mathfrak{p}_j^e$ is a principal ideal ring. Further, for every $j \in [r]$, there is a fixed $z \in \mathcal{O}/\mathfrak{p}_j^e$ such that every non-zero ideal $\mathfrak{a}$ of $\mathcal{O}/\mathfrak{p}_j^e$ is generated by a non-negative integer power of z.*

Proof. If an ideal $\mathfrak{a}$ is co-prime to $\mathfrak{p}_j$, and hence also co-prime to $\mathfrak{p}_j^e$ then $\mathfrak{a}+\mathfrak{p}_j^e = (1)$, and hence $\mathfrak{a}$ modulo $\mathfrak{p}_j^e$ is generated by one, which is a zero-th power of the stipulated z. So, we are left with the case where ideal $\mathfrak{a}$ is not co-prime to $\mathfrak{p}_j$.

By lemma 3.3, any ideal $\mathfrak{a}$ can be written as $\hat{\mathfrak{a}} \cdot \prod_{i\in[r]} \mathfrak{p}_i^{t_i}$, where t_i are non-negative integers, and $\hat{\mathfrak{a}}$ is an ideal of $\mathcal{O}$ co-prime to every $\mathfrak{p}_i$ $(i \in [r])$. As before, $\hat{\mathfrak{a}}$ modulo $\mathfrak{p}_j^{e_j}$ is generated by one. Similarly, for all $i \neq j$, $\mathfrak{p}_i^{t_i}$ modulo $\mathfrak{p}_j^e$ is generated by one. If $t_j \geq e$, $\mathfrak{p}_j^{t_j}$ is zero modulo $\mathfrak{p}_j^e$ and is generated by zero, so the only interesting case we are left with is $0 < t_j < e$. We will just show that $\mathfrak{p}_j$ is principal modulo $\mathfrak{p}_j^e$ with $e > 1$, as this would imply that every power of $\mathfrak{p}_j$ is also principal, and if $\mathfrak{p}_j$ is generated by some z, then $\mathfrak{p}_j^{t_j}$ is generated by z^{t_j}.

For each $z \in \mathfrak{p}_j$, consider the principal ideal (z) in $\mathcal{O}$. Again, by lemma 3.3, it can be written as product of ideals co-prime to $\mathfrak{p}_j$ and some finite power t_z of $\mathfrak{p}_j$. Thus, ideal (z) modulo $\mathfrak{p}_j^e$, i.e. (z) viewed as an ideal of $\mathcal{O}/\mathfrak{p}_j^e$ is $\mathfrak{p}_j^{t_z}/\mathfrak{p}_j^e$. Let z^* be a $z \in \mathfrak{p}_j$ with minimal t_z. We claim that every $z \in \mathfrak{p}_j/\mathfrak{p}_j^e$ is in $\mathfrak{p}_j^{t_{z^*}}/\mathfrak{p}_j^e$, and hence $\mathfrak{p}_j/\mathfrak{p}_j^e$ is same as $\mathfrak{p}_j^{t_{z^*}}/\mathfrak{p}_j^e$. This will show that $\mathfrak{p}_j/\mathfrak{p}_j^e$ is principal, being generated by z^*. The claim is dispatched by noting that for every $z \in \mathfrak{p}_j/\mathfrak{p}_j^e$, by definition of t_z and the fact that t_{z^*} is minimal, $(z)/\mathfrak{p}_j^e$ is contained in $\mathfrak{p}_j^{t_{z^*}}/\mathfrak{p}_j^e$, and hence z itself is contained in $\mathfrak{p}_j^{t_{z^*}}/\mathfrak{p}_j^e$.

Corollary 3.5. *$\mathcal{O}/q\mathcal{O}$ is a principal ideal ring.*

Proof. Follows by theorems 3.2 and 3.4 as product of principal ideal rings is a principal ideal ring.

Corollary 3.6. *For all $i \in [r]$, the prime ideal $\mathfrak{p}_i$ of $\mathcal{O}$ is same as (p, h_i) for some $h_i \in \mathfrak{p}_i$, and some prime factor p of q.*

Proof. By corollary 3.5, the ideal $\mathfrak{p}_i$ mod $q\mathcal{O}$ is generated by some $h_i \in \mathfrak{p}_i/q\mathcal{O}$. W.l.o.g. pick any such $h_i \in \mathfrak{p}_i$ as the representative. Then, $\mathfrak{p}_i + (q) = (h_i) + (q)$. Since $(q) \subset \mathfrak{p}_i$, we have $\mathfrak{p}_i = (h_i, q)$. Since $\mathfrak{p}_i$ is prime, some prime factor of q must be in the ideal, say p. Then, $\mathfrak{p}_i = (h_i, p)$.

Theorem 3.7. *For any ideal $\mathfrak{a}$ of $\mathcal{O}$, $\mathfrak{a}$ is principal modulo $q\mathfrak{a}$, i.e. $\mathfrak{a}/q\mathfrak{a}$ (as an ideal of $\mathcal{O}/q\mathfrak{a}$) is principal.*

Proof. First consider the case that $\mathfrak{a}$ is co-prime to all $\mathfrak{p}_i$ ($i \in [1..r]$). Then, by lemma 3.1 and basic properties of ideals (see lemma A.1 (*xiv*) and (*xii*)), and CRT, we have $\mathcal{O}/q\mathfrak{a} \cong \mathcal{O}/\mathfrak{a} \cdot \prod_{i=1}^r \mathcal{O}/\mathfrak{p}_i^{e_i}$. So $\mathfrak{a}$ will be principal in $\mathcal{O}/q\mathfrak{a}$, if it is principal in each of the component rings. Theorem 3.4, shows that $\mathfrak{a}$ is principal in $\mathcal{O}/\mathfrak{p}_i^{e_i}$, and $\mathfrak{a}$ is trivially principal modulo $\mathfrak{a}$, and hence the lemma is proved in this case.

Otherwise, by lemmas 3.3 and 3.1, we have, $\mathfrak{a} \cdot (q) = \hat{\mathfrak{a}} \cdot \prod_{i\in[r]} \mathfrak{p}_i^{e_i+t_i}$, for some non-negative integers t_i. Also, $\hat{\mathfrak{a}}$ is co-prime to each $\mathfrak{p}_i$ and hence to each $\mathfrak{p}_i^{e_i+t_i}$. Thus, by CRT, $\mathcal{O}/q\mathfrak{a} \cong \mathcal{O}/\hat{\mathfrak{a}} \cdot \prod_{i=1}^r \mathcal{O}/\mathfrak{p}_i^{e_i+t_i}$. Then, using theorem 3.4, $\hat{\mathfrak{a}}$ is principal modulo $\mathfrak{a} \cdot (q)$ by employing CRT, just as in the simple case above where $\mathfrak{a}$ was co-prime to all $\mathfrak{p}_i$. By Theorem 3.4, for all $i, j \in [r]$, each $\mathfrak{p}_i$ is also principal modulo $\mathfrak{p}_j^s$, for any s. So, we just need to show that each $\mathfrak{p}_i$ 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 $\hat{\mathfrak{a}}$.

4 Generator Extractor for Principal Ideals of Hidden Orders

Let $\mathbf{K}$ be any number field, say $\mathbf{K} = \mathbb{Q}[X]/(f(X))$ for some irreducible polynomial $f(X)$ of degree n, with $n = [\mathbf{K} : \mathbb{Q}]$, and $\mathcal{O}$ be an order in the field. Let $m = [\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$ be the index of $\mathcal{O}$ in the maximal order $\mathcal{O}_{\mathbf{K}}$, i.e. the ring of integers of $\mathbf{K}$. Let q be relatively prime to m. We first focus on q being a prime power, say p^s. The case where q is a product of powers of different primes is handled subsequently. Given a $\mathbb{Z}$-basis $\boldsymbol{B}(\mathfrak{a})$ of an ideal $\mathfrak{a}$ of order $\mathcal{O}$, we wish to compute a generator of the principal ideal $\mathfrak{a}$ modulo $p^s\mathfrak{a}$ (which is principal by theorem 3.7), *without* access to a $\mathbb{Z}$-basis of the order $\mathcal{O}$.

We show that the following simple and efficient randomized algorithm computes such a generator with non-negligible probability for all p for number fields where $\mathcal{O}_{\mathbf{K}}$ is the polynomial ring $\mathbb{Z}[X]/(f(X))$, and for general number fields when $p > \Omega(n)$.

Algorithm 1 FindGen

```
Input: Rank $n$ $\mathbb{Z}$-bases $\boldsymbol{B}(\mathfrak{a})$ for an ideal $\mathfrak{a}$ of $\mathcal{O}$, and $\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})$ of $\mathcal{O}_{\mathbf{K}}$,
Output: A single generator $\mathbf{a}$ for ideal $\mathfrak{a}$ mod $p^s\mathfrak{a}$, i.e. ideal $\mathfrak{a}/p^s\mathfrak{a}$ of $\mathcal{O}/p^s\mathfrak{a}$.
Pick $n$ polynomials $\rho_k \in \mathcal{O}/p\mathcal{O}$ ($k \in [n]$), chosen uniformly and independently from finite ring $\mathcal{O}_{\mathbf{K}}/p\mathcal{O}_{\mathbf{K}}$ and mapped to $\mathcal{O}/p\mathcal{O}$ by the isomorphism in Lemma 2.6.
View the $n$ columns of $\boldsymbol{B}(\mathfrak{a})$ as $n$ polynomials $\gamma_k \in \mathbf{K}$ ($k \in [n]$).
Compute $\mathbf{a} = \sum_{k=1}^{n} \rho_k * \gamma_k$ in $\mathbf{K}$.
Output $\mathbf{a}$
```

Lemma 4.1. *For a prime p co-prime to m, let $p\mathcal{O}$ have a factorization in terms of prime ideals as $p\mathcal{O} = \prod_{i=1}^{r} \mathfrak{p}_i^{e_i}$. The algorithm* **FindGen** *outputs a generator* $\mathbf{a}$ *of $\mathfrak{a}$ modulo $p^s\mathfrak{a}$ with probability at least $\prod_{i\in[r]}(1 - 1/p^{d_i} - 1/p^{2d_i})$, where d_i is the degree of extension of the finite field (of characteristic p) $\mathcal{O}/\mathfrak{p}_i$ over $\mathbb{Z}_p$.*

Proof. First, by lemma 2.2(iii), $\mathbb{Z} \subset \mathcal{O}$, and hence the given $\mathbb{Z}$-basis $\boldsymbol{B}(\mathfrak{a})$ of ideal $\mathfrak{a}$ of $\mathcal{O}$ is also an $\mathcal{O}$-basis of $\mathfrak{a}$. Recall, $\mathbf{a}$ computed in the algorithm is just $\sum_k \rho_k\gamma_k$, and since ρ_k belong to $\mathcal{O}$ modulo $p\mathcal{O}$, we have $\mathbf{a} \in \mathfrak{a}$.

By lemma 3.3, we have $\mathfrak{a}\cdot(p)^s = \hat{\mathfrak{a}}\cdot\prod_{i\in[r]} \mathfrak{p}_i^{s\cdot e_i+t_i}$, where $\hat{\mathfrak{a}}$ is co-prime to every $\mathfrak{p}_i$ ($i \in [r]$). Thus, by employing CRT, we have that the ring $\mathcal{O}/p^s\mathfrak{a}$ is isomorphic to $\mathcal{O}/\hat{\mathfrak{a}}\cdot\prod_{i\in[r]} \mathcal{O}/\mathfrak{p}_i^{s\cdot e_i+t_i}$. Since, $\mathfrak{a}$ is zero mod $\hat{\mathfrak{a}}$, $\mathbf{a}$ is also zero mod $\hat{\mathfrak{a}}$, and hence trivially generates $\mathfrak{a}$ mod $\hat{\mathfrak{a}}$. Thus, we can focus on $\mathfrak{a}$ modulo $\mathfrak{p}_i^{s\cdot e_i+t_i}$, for each $i \in [r]$.

Fix an $i \in [r]$. Denote $\mathfrak{p}_i^{s\cdot e_i+t_i}$ by $\mathfrak{q}_i$. View each of the elements γ_k ($k \in [n]$) also as elements of the quotient ring $\mathcal{O}/\mathfrak{q}_i$, and the randomly chosen elements ρ_k as elements in the order $\mathcal{O}$. Denote $\mathfrak{a}$ reduced mod $\mathfrak{q}_i$ by $\mathfrak{a}_i$. By Theorem 3.4, $\mathfrak{a}_i$ is principal and is generated by finite power of some g_i. Similarly, each (γ_k) mod $\mathfrak{q}_i$ is itself generated by a finite power of the same g_i, say the power is $v_{k,i} \geq 0$. Hence, $\mathfrak{a}_i$ is generated by $g_i^{v_i^*}$, where $v_i^* = \min\{v_{k,i} \ : \ k \in [n]\}$. We need to show that $\sum_k \rho_k\gamma_k$ generates exactly $(g_i)^{v_i^*}$ mod $\mathfrak{q}_i$.

Note, γ_k can be written as $\alpha_{k,i}g_i^{v_{k,i}}$ mod $\mathfrak{q}_i$, for some $\alpha_{k,i} \in \mathcal{O}$ where $\alpha_{k,i}$ is not in $\mathfrak{p}_i$. Then, $\sum_k \rho_k\gamma_k$ mod $\mathfrak{q}_i$ can be written as $g_i^{v_i^*} * \sum_k \rho_k\alpha_{k,i}g_i^{v_{k,i}-v_i^*}$. 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 $\mathfrak{p}_i$ is a maximal ideal of $\mathcal{O}$, and every element of $\mathcal{O}$ not in $\mathfrak{p}_i$ is invertible mod $\mathfrak{p}_i$, we need to show that with decent probability, over the random choices of $\{\rho_k\}_k$, *for all* $i \in [r]$, $\sum_{k\in I_i} \rho_k\alpha_{k,i}$ is not zero modulo $\mathfrak{p}_i$. Note that for $k \notin I_i$, the quantities $\rho_k\alpha_{k,i}g_i^{v_{k,i}-v_i^*}$ are in $(g_i) \subseteq \mathfrak{p}_i$, so the full sum (over all $k \in [n]$) will be non-zero modulo $\mathfrak{p}_i$ and hence invertible.

To calculate this probability, we first note that $\mathcal{O}/\mathfrak{p}_i$ is a finite field as $\mathfrak{p}_i$ is a maximal ideal and is of finite rank in $\mathcal{O}$, as each ideal of an order has finite index in the order (lemma 2.2(v)). Further $\mathfrak{p}_i$ contains p and hence the field has characteristic p. Thus, by Galois theory of finite fields, $\mathcal{O}/\mathfrak{p}_i$ is isomorphic to $\mathrm{GF}(p^{d_i})$, for some positive integer d_i, i.e. the degree of extension. Thus, we can view each of ρ_k and $\alpha_{k,i}$ as elements of this field (by reducing modulo p, h_i as given by corollary 3.6). We have already seen that $\alpha_{k,i}$ is non-zero in this field, as it is not in $\mathfrak{p}_i$. However, a random choice of ρ_k in $\mathcal{O}/p\mathcal{O}$ may lead ρ_k to be zero modulo $\mathfrak{p}_i$, although this probability is small, as we next show.

First, by employing CRT and theorem 3.2, ρ_k is uniformly and *independently* distributed in the rings $\mathcal{O}/\mathfrak{p}_i^{e_i}$. Since, as additive groups, $\mathfrak{p}_i^{e_i}$ is an abelian sub-group of $\mathfrak{p}_i$ which is a sub-group of $\mathcal{O}$, every element of $\mathcal{O}/\mathfrak{p}_i^{e_i}$ can be uniquely expressed as $a + b$ where $a \in \mathfrak{p}_i/\mathfrak{p}_i^{e_i}$ and $b \in \mathcal{O}/\mathfrak{p}_i$, i.e. $\mathcal{O}/\mathfrak{p}_i^{e_i} \cong (\mathcal{O}/\mathfrak{p}_i)(\mathfrak{p}_i/\mathfrak{p}_i^{e_i})$. Thus, a randomly and uniformly chosen element of $\mathcal{O}/\mathfrak{p}_i^{e_i}$ is in ideal $\mathfrak{p}_i$, i.e. is zero in $(\mathcal{O}/\mathfrak{p}_i)$ with probability $1/|\mathcal{O}/\mathfrak{p}_i|$. This latter quantity is exactly $1/p^{d_i}$. In fact, this random element is uniformly distributed in each coset of sub-group $\mathfrak{p}_i/\mathfrak{p}_i^{e_i}$.

Thus, probability that $\beta_i = \sum_{k\in I_i} \rho_k\alpha_{k,i}$ is in ideal $\mathfrak{p}_i$ at most $1/p^{d_i}$ if $|I_i| = 1$, and otherwise at most $1/p^{d_i * |I_i|}$ plus $(1 - 1/p^{d_i*|I_i|}) \cdot 1/p^{d_i}$. In either case, it is at most $1/p^{d_i} + 1/p^{2d_i}$. Since, each ρ_k's projection is independently distributed in the various rings $\mathcal{O}/\mathfrak{p}_i^{e_i}$, the probability that all of these r quantities β_i are non-zero is at least $\prod_{i\in[r]}(1 - 1/p^{d_i} - 1/p^{2d_i})$, which is also a lower bound on the probability that $\mathbf{a}$ is a generator of $\mathfrak{a}$ modulo $p^s\mathfrak{a}$.

Extension to Product of Powers of Primes. Let $q = \prod_j p_j^{s_j}$ be a product of powers of primes such that q and hence each p_j is co-prime to m. For each j, let $p_j\mathcal{O}$ have a factorization in terms of prime ideals as $p_j\mathcal{O} = \prod_{i=1}^{r_j} \mathfrak{p}_{j,i}^{e_{j,i}}$. The above algorithm can be correctly extended by choosing ρ_k randomly and independently from $\mathcal{O}/q'\mathcal{O}$ where $q' = \prod_j p_j$ (by first sampling from $\mathcal{O}_{\mathbf{K}}/q'\mathcal{O}_{\mathbf{K}}$). The probability of success in this case is at least $\prod_j \prod_{i\in[r_j]}(1 - 1/p_j^{d_{j,i}} - 1/p_j^{2d_{j,i}})$, where $d_{j,i}$ is the degree of extension of the finite field (of characteristic p_j) $\mathcal{O}/\mathfrak{p}_{j,i}$ over $\mathbb{Z}_{p_j}$.

Extension to Arbitrary q without known-factorization. If the factorization of q is not known, and say $q = \prod_j p_j^{s_j}$ as above, we can still use the above algorithm, but this time by choosing ρ_k randomly and independently modulo $\mathcal{O}/q\mathcal{O}$ (by first sampling from $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$). In the proof of lemma 4.1, again using CRT and focusing on individual primes, say p_j, ρ_k is now uniformly and independently distributed in $\mathcal{O}/\mathfrak{p}_{j,i}^{e_{j,i}s_j}$. By the probability analysis in the lemma 4.1 above, the probability of success remains the same as in the known factorization case above, as it only depends on $d_{j,i}$ and not $e_{j,i}s_j$.

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 $\mathbf{a}$ as computed is indeed a generator. We show below in lemma 4.2 that $\mathbf{a} \in \mathfrak{a}$ is a generator of $\mathfrak{a}/q\mathfrak{a}$ iff

$\det(\boldsymbol{C}_a)\det(\boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))/\det(\boldsymbol{B}(\mathfrak{a}))$ is co-prime to q. Thus, this serves as an easy stopping criterion. The proof of the lemma can be found in Appendix A.

Lemma 4.2. *For any positive integer q, and for an ideal $\mathfrak{a}$ of $\mathcal{O}$ such that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}$ for m co-prime to q, a $\mathbf{g} \in \mathfrak{a}$ generates the ideal $\mathfrak{a}/q\mathfrak{a}$ iff $\det(\boldsymbol{C}_g) \cdot \det(\boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))/\det(\boldsymbol{B}(\mathfrak{a}))$ is co-prime to q.*

Probability Calculation from bound given by Lemma 4.1 While lemma 4.1 gives a lower bound on probability of success, i.e. $\prod_{i\in[r]}(1-1/p^{d_i}-1/p^{2d_i})$, we still need to show that this is non-negligible. If $p \geq n$, then for all $\mathcal{O}$ in all number fields K, $\prod_i(1-1/p_i^d) \geq (1-1/p)^n \geq e^{-1}$. This is usually the case in many applications, e.g. CRYSTALS-KYBER [BDK$^+$18]. and full-RNS-CKKS-HE [CHK$^+$18]. If $p < n$, then we focus on number fields such that $\mathcal{O}_{\mathbf{K}} = Z[X]/(f(X))$, so that all orders have elements (polynomials) with integer coefficients. Now, note that the bound $\prod_i(1-1/p_i^d)$ is worst when all e_i are one, as this makes r larger. Let's count how many different prime ideals $\mathfrak{p}$ can be above p. By corrollary 3.6, these ideals are of the form (p, h_i), where $h_i \in \mathcal{O} \subset \mathcal{O}_{\mathbf{K}}$, and hence h_i is an integer polynomial of degree d_i, irreducbile mod p. So the total number of distinct prime ideals with extension degree d can be at most p^d. So for each d, let r_d be this number, i.e. $r_d \leq p^d$. And $r = \sum_d r_d$. The bound is worst when d is smaller. So, the worst bound would be $\prod_d(1-1/p^d)^{r_d}$. A simple analysis shows that this is at least $n^{-1/\log p}$. And in the general case, q being product of prime powers, this is at least $n^{-1/\log q'}$.

5 Hardness of Decisional Ring-LWE based on Worst-case Ideals of Orders

In this section, we focus on a degree-n extension field of $\mathbb{Q}$, say $\mathbf{K} = \mathbb{Q}[X]/(f(X))$, an integer $q \geq 2$, and all orders $\mathcal{O}$ in $\mathbf{K}$ such that $m \cdot \mathcal{O}_{\mathbf{K}} \subset \mathcal{O}$ with m co-prime to q. Lemma 2.14 assures that index of $\mathcal{O}$ in the maximal order $\mathcal{O}_{\mathbf{K}}$ is also co-prime to q. Let $\mathbf{K}_{\mathbb{R}} = \mathbb{R}[X]/(f(X))$. As the heading of this section indicates, the results in this section extend the usual Ring-LWE hardness to be based on ideals of orders, and in fact without knowledge of the order. However, since one key component of this reduction uses the FindGen algorithm from Section 4, the result for hidden orders is *restricted* to q such that all prime factors p (of q) are $\Omega(n)$ (or, unrestricted p if $\mathcal{O}_{\mathbf{K}} = \mathcal{R}_{\mathbf{K}}$).

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

Definition 5.1 (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 $\mathbf{r} \in \mathcal{H}$ 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 $r_i^2 = r_{i+s_2}^2 = \alpha^2(x_i^2 + y_i^2 + s^2(n))/2$. Note the support is in $\mathcal{H}$ restricted to all real components.*

Definition 5.2 (Ring-LWE Distribution). *([LPR10]) Let $\boldsymbol{V}$ be the Vandermonde matrix of the polynomial $f(X)$. For $\mathbf{s} \in \mathcal{O}_{\mathbf{K}}^{\vee}/q\mathcal{O}_{\mathbf{K}}^{\vee}$ and an error distribution ψ over $\mathcal{H}$, we define the RLWE distribution $\mathcal{A}_{\mathbf{s},\psi}$ over $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}} \times \mathbf{K}_{\mathbb{R}}/\mathcal{O}_{\mathbf{K}}^{\vee}$ as $(\mathbf{a}, \mathbf{b} = \mathbf{a} * \mathbf{s}/q \ \ + \boldsymbol{V}^{-1}\mathbf{e} \bmod \mathcal{O}_{\mathbf{K}}^{\vee})$ where $\mathbf{e}$ is sampled from ψ, $\mathbf{a}$ is uniform over $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$.*

Definition 5.3 ((Average-case) Decisional Ring-LWE Problem (RLWE)). *Let Υ_α be a distribution over family of error distributions, each over $\mathcal{H}$. The* average-case decisional Ring-LWE problem*, 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 $s \in \mathcal{O}_{\mathbf{K}}^{\vee}/q\mathcal{O}_{\mathbf{K}}^{\vee}$ and $\psi \in \Upsilon_\alpha$ and the same number of uniformly random and independent samples from $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}} \times \mathbf{K}_{\mathbb{R}}/\mathcal{O}_{\mathbf{K}}^{\vee}$.*

Let m-$\mathcal{O}$-DGS$_\gamma$ be the discrete Gaussian sampling problem DGS$_\gamma$ when restricted to ideal lattices of orders $\mathcal{O}$ of $\mathbf{K}$ such that $m \cdot \mathcal{O}_{\mathbf{K}} \subset \mathcal{O}$. The problem only takes a $\mathbb{Z}$-basis of the ideal as input, apart from auxiliary information m and a basis of the maximal order $\mathcal{O}_{\mathbf{K}}$. In particular, the Z-basis of $\mathcal{O}$ is *not* provided. We now state the main theorem of this work.

Theorem 5.1. *Let $\alpha = \alpha(n) \in (0, 1)$ and $q = q(n) \geq 2$ be an integer, and m another positive integer co-prime to q. If $\alpha q/m \geq 2 \cdot \omega(1)$, for some negligible $\epsilon = \epsilon(n)$, there is a probabilistic polynomial-time quantum reduction from m-$\mathcal{O}$-DGS$_\gamma$ to (average case, decisional) RLWE$_{q,\Upsilon_\alpha}$, where*

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

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

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

Corollary 5.2. *With the same notation as Theorem 5.1, for m co-prime to q, there's a polynomial time quantum reduction from m-$\mathcal{O}$-DGS$_\gamma$ to (average-case, decisional) RLWE$_{q,D_\xi}$ using ℓ samples, where*

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

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

Our proof of theorem 5.1 will follow the blueprint of [PRS17, Theorem 6.2], that starts with a discrete Gaussian sampler with very large radius, and iteratively applies the following lemma 5.3.

Definition 5.4. *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 5.3. *There's an efficient quantum algorithm that, given an oracle that solves $\mathsf{RLWE}_{q,\Upsilon_\alpha}$, an ideal $\mathcal{I}$ of $\mathcal{O}$, with $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}$ for some integer m co-prime to q, a number $r \geq \sqrt{2}q \cdot \eta_\epsilon(\mathcal{L}(\mathcal{I}))$ and $r' = m \cdot r \cdot \omega(1)/(\alpha q) \geq \sqrt{2n}/\lambda_1(\mathcal{L}(\mathcal{I})^*)$, 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 with *one key difference*: a classical one in lemma 5.4 that use a discrete Gaussian sampler and an RLWE oracle to solve the Gaussian Decoding Problem (GDP) in $m\mathcal{L}(\mathcal{I})^*$ (instead of usual $\mathcal{L}(\mathcal{I})^*$), and a quantum one in lemma 5.5 that uses this GDP solver to provide discrete Gaussian samples with smaller radius. The above difference means that αq has to be m factor larger than usual because we can only employ lemma 5.5 on $m\mathcal{L}(\mathcal{I})^*$ which would then only give samples in $\frac{1}{m}\mathcal{L}$, and would need to be scaled by m to get lemma 5.3.

Lemma 5.4. *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 $\mathcal{I}$ of $\mathcal{O}$ such that $m \cdot \mathcal{O}_{\mathbf{K}} \subset\ cO$ for some integer m co-prime to q, 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 $\mathsf{GDP}_{m\mathcal{L}(\mathcal{I})^*,g}$ for any $g = o(1) \cdot \alpha q/(2r)$.*

Lemma 5.5 ([PRS17, Lemma 6.7]). *There is an efficient quantum algorithm that, given any n-dimensional lattice $\mathcal{L}$, a number $g < \frac{\lambda_1(\mathcal{L}^*)}{2\sqrt{2n}}$, a vector $\mathbf{r} \geq 1$, and an oracle that solves $\mathsf{GDP}_{\mathcal{L}^*,g}$ with all but negligible probability, outputs a sample from $D_{\mathcal{L},\frac{\mathbf{r}}{2g}}$.*

The proof of lemma 5.4 follows exactly from [PRS17, Lemma 6.6], except 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 the general case. We provide a counterpart in lemma 5.6 that works for all orders with the above condition.

Lemma 5.6. *Let $\mathcal{O}$ be an order such that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}$, for some integer m. There's an efficient algorithm that, takes as input an integer $q \geq 2$ co-prime to m, a dual ideal lattice $\mathcal{L}(\mathcal{I})^*$ where $\mathcal{I}$ is an ideal of $\mathcal{O}$, a coset $\mathbf{e} + m\mathcal{L}(\mathcal{I})^*$ 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 $\mathbf{s} \in \mathcal{O}_{\mathbf{K}}^\vee/q\mathcal{O}_{\mathbf{K}}^\vee$, where $(\mathbf{r}'_i)^2 = (\mathbf{r}_i|\mathbf{e}_i|/q)^2 + (rd/q)^2$.*

To prove this lemma 5.6, we mostly follow the technique of [LPR10, Lemma 4.7] which was slightly generalized in [PRS17, Lemma 6.8], but the main advance now being an ideal and order clearing lemma as elaborated 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 2.7, 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 $\hat{\mathbf{x}} \in m \cdot \mathcal{L}(\mathcal{I})^*$, and given a $\hat{\mathbf{y}}$ related to it by $\hat{\mathbf{y}} = \overline{\boldsymbol{V}\mathbf{y}} = \bar{\mathbf{e}} + \hat{\mathbf{x}} \in \bar{\mathbf{e}} + m \cdot \mathcal{L}(\mathcal{I})^*$, we have $\mathbf{y} = \boldsymbol{V}^{-1}\mathbf{e} + \mathbf{x}$, where $\mathrm{conj}(\hat{\mathbf{x}}) = \boldsymbol{V}\mathbf{x}$ for some $\mathbf{x} \in m \cdot \mathcal{I}^\vee$. Thus, we could directly provide a "Ring-LWE sample" from $\mathcal{I}/q\mathcal{I} \times \mathbf{K}_\mathbb{R}/\mathcal{O}^\vee_\mathbf{K}$ as

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

for some secret $\mathbf{x} \in m\mathcal{I}^\vee/qm\mathcal{I}^\vee$, noting that $m\mathcal{O}^\vee \subset \mathcal{O}^\vee_\mathbf{K}$. To jump out of the ideal, we use lemma 5.7, a counterpart of clearing lemma of [LPR10, Lemma 2.15] for non dedekind domains, that gives (i) an invertible and efficiently computable bijection $\psi : \mathcal{I}/q\mathcal{I} \to \mathcal{O}_\mathbf{K}/q\mathcal{O}_\mathbf{K}$, and (ii) an efficiently invertible and computable bijection $\phi : m\mathcal{I}^\vee/qm\mathcal{I}^\vee \to \mathcal{O}^\vee_\mathbf{K}/q\mathcal{O}^\vee_\mathbf{K}$, with the additional property that $\mathbf{z} * \mathbf{x} = \psi(\mathbf{z}) * \phi(\mathbf{x})$. Therefore the final Ring-LWE distribution would be over $\mathcal{O}_\mathbf{K}/q\mathcal{O}_\mathbf{K} \times \mathbf{K}_\mathbb{R}/\mathcal{O}^\vee_\mathbf{K}$ as

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

for some secret $\phi(\mathbf{x}) \in \mathcal{O}^\vee_\mathbf{K}/q\mathcal{O}^\vee_\mathbf{K}$. Note that since ψ is a bijection, $\psi(\mathbf{z} \bmod q\mathcal{I})$ is statistically (exponentially) close to uniform over $\mathcal{O}_\mathbf{K}/q\mathcal{O}_\mathbf{K}$.

Moreover, if we sample $\bar{\mathbf{e}} + m \cdot \mathcal{L}(\mathcal{I})^*$ as in $\mathsf{GDP}_{m\mathcal{L}(\mathcal{I})^*,g}$ where $g = \alpha q/(\sqrt{2}r)$, the distribution of $\left(\frac{1}{q}\boldsymbol{C}_z\boldsymbol{V}^{-1}\mathbf{e} + \mathbf{e}'\right)$ (conditioned on $\mathbf{z} \bmod q\mathcal{I}$) will be exactly Υ_α, as in [PRS17, Lemma 6.8]. Of course, we now require $\alpha q = m\omega(\log n)$ as opposed to the earlier $\alpha q = \omega(\log n)$. 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 non Dedekind-domains and even clears the order.

Lemma 5.7. Generalized Ideal and Order Clearing Lemma. *Fix a number field $\mathbf{K}$ with a known $\mathbb{Z}$-basis for its ring of integers $\mathcal{O}_\mathbf{K}$. For any relatively prime positive integers q and m, and any order $\mathcal{O}$ such that $m\mathcal{O}_\mathbf{K} \subset \mathcal{O}$, for any ideal $\mathcal{I}$ of $\mathcal{O}$, given a generator $\mathbf{g} \in \mathcal{I}$ for the principal ideal $\mathcal{I}/q\mathcal{I}$, and given* $\det(\mathcal{I})$,

(i) *there is an efficiently computable map $\psi : \mathcal{I} \to \mathcal{O}_\mathbf{K}$ that induces an efficiently computable $\mathcal{O}_\mathbf{K}/q\mathcal{O}_\mathbf{K}$-module isomorphism $\psi : \mathcal{I}/q\mathcal{I} \to \mathcal{O}_\mathbf{K}/q\mathcal{O}_\mathbf{K}$,*
(ii) *there is an efficiently computable map $\phi : m\mathcal{I}^\vee \to \mathcal{O}^\vee_\mathbf{K}$ that induces an efficiently invertible $\mathcal{O}_\mathbf{K}/q\mathcal{O}_\mathbf{K}$-module isomorphism $\phi : m\mathcal{I}^\vee/qm\mathcal{I}^\vee \to \mathcal{O}^\vee_\mathbf{K}/q\mathcal{O}^\vee_\mathbf{K}$,*

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

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

Proof. Let $\boldsymbol{B}(\mathcal{O})$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. Since $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}$, by lemma 2.2($v$), we have $m \cdot \boldsymbol{B}(\mathcal{O}_{\mathbf{K}}) = \boldsymbol{B}(\mathcal{O})\boldsymbol{L}$, and $\boldsymbol{B}(\mathcal{O}) = \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{M}$ for some integer matrices $\boldsymbol{L}$ and $\boldsymbol{M}$. Thus, $m \cdot I = \boldsymbol{M}\boldsymbol{L}$ and $m^n = \det \boldsymbol{L} \cdot \det \boldsymbol{M}$. Since m is co-prime to q, both $\det \boldsymbol{M}$ (index of $\mathcal{O}$ in $\mathcal{O}_{\mathbf{K}}$) and $\det \boldsymbol{L}$ are co-prime to q. Thus, by Theorem 3.7, $\mathcal{I}/q\mathcal{I}$ is guaranteed to be principal.

Let $\boldsymbol{B}(\mathcal{I})$ be a $\mathbb{Z}$-basis of $\mathcal{I}$. Since $\mathbf{g} \in \mathcal{I}$, by lemma 2.10 and lemma 2.2(v),

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

where $\boldsymbol{D}$ is an integer matrix. Since $\mathbf{g}$ generates $\mathcal{I}/q\mathcal{I}$, by lemma 4.2 and the fact that $\det \boldsymbol{M}$ is co-prime to q, the determinant of $\boldsymbol{D}$ is co-prime to q. Denote the determinant of $\boldsymbol{D} \cdot \boldsymbol{L}$ by d, and let u be an integer such that $u = d^{-1} \bmod q$. Note that d is easily computed as $\det(\boldsymbol{C}_g) * \det(m \cdot \boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))/\det(\boldsymbol{B}(\mathcal{I}))$.

Now to prove (i)-(iii), we first observe that $\mathcal{I}/q\mathcal{I}$ is an $\mathcal{O}/q\mathcal{O}$-module. Similarly, since by lemma 2.11, $m\mathcal{I}^\vee$ is a fractional $\mathcal{O}$-ideal and hence an $\mathcal{O}$-module, we have that $m\mathcal{I}^\vee/qm\mathcal{I}^\vee$ is an $\mathcal{O}/q\mathcal{O}$-module. Further, since q is co-prime to $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$, by lemma 2.6, the rings $\mathcal{O}/q\mathcal{O}$ and $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$ are isomorphic. Thus, both $\mathcal{I}/q\mathcal{I}$ and $m\mathcal{I}^\vee/qm\mathcal{I}^\vee$ are $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$-modules. Also, $\mathcal{O}_{\mathbf{K}}^\vee/q\mathcal{O}_{\mathbf{K}}^\vee$ is a $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$-module, since $\mathcal{O}_{\mathbf{K}}^\vee$ is an $\mathcal{O}_{\mathbf{K}}$ ideal. Note that, by lemma 2.14, $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}$ implies $m\mathcal{O}^\vee \subset \mathcal{O}_{\mathbf{K}}^\vee$.

Now, consider the following two mappings. For any $\mathbf{z} \in \mathcal{I}$ and $\mathbf{x} \in m\mathcal{I}^\vee$, define

$$\psi(\mathbf{z}) = d \cdot \mathbf{g}^{-1} * \mathbf{z} \tag{3}$$
$$\phi(\mathbf{x}) = u \cdot \mathbf{g} * \mathbf{x} \tag{4}$$

For (i), we first check that the ψ maps into $\mathcal{O}_{\mathbf{K}}$. Indeed, since $\mathbf{z} \in \mathcal{I}$, $\mathbf{z} = \boldsymbol{B}(\mathcal{I})\overrightarrow{z}$, for some integer vector $\overrightarrow{z}$. Thus, $\psi(\mathbf{z}) = d \cdot \boldsymbol{C}_g^{-1}\boldsymbol{B}(\mathcal{I})\overrightarrow{z}$. By (2), this is same as $\boldsymbol{B}(\mathcal{O}) \cdot d \cdot \boldsymbol{D}^{-1}\overrightarrow{z}$, which shows that $\psi(\mathbf{z}) \in \mathcal{O} \subseteq \mathcal{O}_{\mathbf{K}}$.

The induced map $\psi : \mathcal{I}/q\mathcal{I} \to \mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$ is easily inverted by (polynomial) multiplication with $m \cdot \ell \cdot u \cdot \mathbf{g}$, where ℓ is any integer such that $m \cdot \ell = 1 \bmod q$, by noting that $m \cdot \ell \cdot u \cdot d = 1 \bmod q$. Thus, the induced map ψ is an invertible map. It is also surjective since $m \cdot \ell \cdot u \cdot \mathbf{g} * \mathbf{a} = \ell \cdot u \cdot \boldsymbol{C}_g \cdot (m \cdot \mathbf{a})$ is in $\mathcal{I}$ for any $\mathbf{a} \in \mathcal{O}_{\mathbf{K}}$, as $m \cdot \mathbf{a}$ is in $\mathcal{O}$. Since, ψ is easily seen to be an $\mathcal{O}/q\mathcal{O}$-module homomorphism, and hence an $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$-module homomorphism, the induced map ψ is an $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$-module isomorphism, which is also efficiently computable. This proves (i).

For (ii), we first note that by lemma 2.13 and using (2), for $\mathbf{x} \in m\mathcal{I}^\vee$,

$$\begin{aligned} u \cdot \mathbf{g} * \mathbf{x} &= u \cdot (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \boldsymbol{C}_g \cdot \mathbf{x} \\ &= u \cdot (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{C}_g^\top \cdot (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \mathbf{x} \\ &= u \cdot (\boldsymbol{V}^\top \boldsymbol{V})^{-1} (\boldsymbol{B}(\mathcal{O}))^{-\top} \boldsymbol{D}^\top \boldsymbol{B}(\mathcal{I})^\top (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \mathbf{x} \\ &\in\ m \cdot \mathcal{O}^\vee \subset \mathcal{O}_{\mathbf{K}}^\vee \end{aligned}$$

where the last membership follows by noting that $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}(\boldsymbol{B}(\mathcal{O}))^{-\top}$ is a $\mathbb{Z}$-basis for $\mathcal{O}^\vee$ and $(\boldsymbol{V}^\top \boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-\top}$ is a $\mathbb{Z}$-basis for $\mathcal{I}^\vee$ (see lemma 2.11). Now, for the induced map $\phi : m\mathcal{I}^\vee / qm\mathcal{I}^\vee \rightarrow \mathcal{O}^\vee_{\mathbf{K}}/q\mathcal{O}^\vee_{\mathbf{K}}$, $\phi(\mathbf{x})$ is inverted by multiplication by $d \cdot \mathbf{g}^{-1}$ to $\mathbf{x}$ mod $qm\mathcal{I}^\vee$.

Further, for any $\mathbf{s} \in \mathcal{O}^\vee_{\mathbf{K}}$, $d \cdot \mathbf{g}^{-1}\mathbf{s}$ lies in $m\mathcal{I}^\vee$ which is seen as follows: using a basis for $\mathcal{O}^\vee_{\mathbf{K}}$, we have $\mathbf{s} = (\boldsymbol{V}^\top \boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})^{-\top}\overrightarrow{s}$ for some integer vector $\overrightarrow{s}$. Thus, $d \cdot \mathbf{g}^{-1}\mathbf{s}$ is same as $d \cdot \boldsymbol{C}_g^{-1}(\boldsymbol{V}^\top \boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{O}_{\mathbf{K}})^{-\top}\overrightarrow{s}$. By lemma 2.11, this is same as $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot d \cdot (\boldsymbol{C}_g \boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))^{-\top}\overrightarrow{s}$. By (2) and the fact that $m \cdot \boldsymbol{B}(\mathcal{O}_{\mathbf{K}}) = \boldsymbol{B}(\mathcal{O})\boldsymbol{L}$ this is same as $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot m \cdot \boldsymbol{B}(\mathcal{I})^{-\top} \cdot d \cdot (\boldsymbol{D}\boldsymbol{L})^{-\top}\overrightarrow{s}$, which by the above $\mathbb{Z}$-basis of $\mathcal{I}^\vee$ is in $m\mathcal{I}^\vee$. Thus, the induced map ϕ is an invertible and surjective $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$-module homomorphism, that is also efficiently invertible, thus proving (ii).

Now, we move on to prove (iii). By lemma 2.12, for $\mathbf{z} \in \mathcal{I}$ and $\mathbf{x} \in m\mathcal{I}^\vee$, $\mathbf{z} * \mathbf{x}$ is in $m\mathcal{O}^\vee \subset \mathcal{O}^\vee_{\mathbf{K}}$, and thus we have

$$\psi(\mathbf{z}) * \phi(\mathbf{x}) \;=\; u \cdot d \cdot \mathbf{z} * \mathbf{x} \;=\; \mathbf{z} * \mathbf{x} \bmod q\mathcal{O}^\vee_{\mathbf{K}}.$$

5.1 Ring-LWE hardness based on non-Ideal Lattices

In this section, we show an alternate hardness reduction for Ring-LWE. We show that hardness of Ring-LWE can be based on worst-case hardness of lattices in number fields which are of the form $\mathcal{I}_1 + \mathcal{I}_2$, where $\mathcal{I}_1$ is an ideal in an order $\mathcal{O}_1$, and $\mathcal{I}_2$ is an ideal in order $\mathcal{O}_2$. Let m be the smallest integer such that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_1$ and $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_2$, and q be any integer co-prime to q. Then the reduction is to q-Ring-LWE with noise a factor m larger than required in the usual Ring-LWE reduction from ideal lattices in the ring of integers. The key ingredient is of course a clearing lemma, this time for sum of ideals of two different orders. Since this need not be an ideal of any order (see 6), and similarly even $(\mathcal{I}_1 + \mathcal{I}_2)/q(\mathcal{I}_1 + \mathcal{I}_2)$ need not be an $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$-module, the isomorphisms we obtain are just group isomorphisms; but, that is really all that is required for the hardness reduction to Ring-LWE.

As opposed to the general clearing lemma in the previous section, where information about $\mathcal{O}$ was not required, here we will require that a $\mathbb{Z}$-basis of $(\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2$ is also given, In fact, the clearing lemma critically uses the fact that, although, $\mathcal{I}_1 + \mathcal{I}_2$ may not be an ideal in any order, it can be shown that $\mathcal{I}' = (\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2$ is an ideal of the order $\mathcal{O}_1 \cap \mathcal{O}_2$. This way, we can use Lemma 4.1 to obtain a generator for the principal ideal $\mathcal{I}'/q\mathcal{I}'$. We begin with proving this fact and some relevant related facts about the index of $(\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2$ in $(\mathcal{I}_1 + \mathcal{I}_2)$, which allows us to show that the generator obtained for $\mathcal{I}'/q\mathcal{I}'$ can be used to obtain the required isomorphisms in the clearing lemma.

Lemma 5.8. (i) *If $\mathcal{O}_1$ and $\mathcal{O}_2$ are orders in number field $\mathbf{K}$, then $\mathcal{O}_1 \cap \mathcal{O}_2$ is also an order in $\mathbf{K}$.*

(ii) *If $\mathcal{I}_1$ is an ideal of order $\mathcal{O}_1$, and $\mathcal{I}_2$ is an ideal of $\mathcal{O}_2$, then $(\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2$ is an ideal of order $\mathcal{O}_1 \cap \mathcal{O}_2$.*

(iii) *Let m be an integer such that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_1 \cap \mathcal{O}_2$. Then, $m\mathcal{I}_1 \subset \mathcal{I}_1 \cap \mathcal{O}_2$ and $m\mathcal{I}_2 \subset \mathcal{I}_2 \cap \mathcal{O}_1$. Further, $m(\mathcal{I}_1 + \mathcal{I}_2) \subset (\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2$.*

(iv) *Let m be an integer such that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_1 \cap \mathcal{O}_2$. Then, any $\mathbb{Z}$-basis of $(\mathcal{I}_2 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2$, $\boldsymbol{B}((\mathcal{I}_2 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2)$, can be written as $\boldsymbol{B}(\mathcal{I}_1 + \mathcal{I}_2) \cdot \boldsymbol{M}$, where $\boldsymbol{M}$ is an integer matrix and a prime divides $\det \boldsymbol{M}$ only if it divides m.*

The proof of this lemma can be found in Appendix C.

Lemma 5.9. "Sum of Ideals of Different Orders" Clearing Lemma. *Fix a number field $\mathbf{K}$ with a known $\mathbb{Z}$-basis for its ring of integers $\mathcal{O}_{\mathbf{K}}$. For any relatively prime positive integers q and m, and any orders $\mathcal{O}_1, \mathcal{O}_2$ such that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}' = \mathcal{O}_1 \cap \mathcal{O}_2$, for any ideals $\mathcal{I}_1$ of $\mathcal{O}_1$ and ideals $\mathcal{I}_2$ of $\mathcal{O}_2$, given a generator $\mathbf{g} \in \mathcal{I}' = (\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}'$ for the principal ideal $\mathcal{I}'/q\mathcal{I}'$, and given* $\det(\mathcal{I}_1 + \mathcal{I}_2)$,

(i) *there is an efficiently computable map $\psi : \mathcal{I}_1 + \mathcal{I}_2 \to \mathcal{O}_{\mathbf{K}}$ that induces an efficiently computable $\mathbb{Z}$-module isomorphism $\psi : (\mathcal{I}_1 + \mathcal{I}_2)/q(\mathcal{I}_1 + \mathcal{I}_2) \to \mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$,*

(ii) *there is an efficiently computable map $\phi : m(\mathcal{I}_1 + \mathcal{I}_2)^\vee \to \mathcal{O}_{\mathbf{K}}^\vee$ that induces an efficiently invertible $\mathbb{Z}$-module isomorphism $\phi : m(\mathcal{I}_1 + \mathcal{I}_2)^\vee / qm(\mathcal{I}_1 + \mathcal{I}_2)^\vee \to \mathcal{O}_{\mathbf{K}}^\vee / q\mathcal{O}_{\mathbf{K}}^\vee$,*

(iii) *such that, for any $\mathbf{z} \in \mathcal{I}_1 + \mathcal{I}_2$ and $\mathbf{x} \in m \cdot (\mathcal{I}_1 + \mathcal{I}_2)^\vee$, their polynomial product satisfies*

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

Proof of this lemma can be found in Appendix C.

6 Example Orders and non-Bigenic Ideals

An ideal will be called *bigenic* if it can be generated by two or less elements of the ring. When $\mathcal{O}$ is a strict subring of $\mathcal{O}_{\mathbf{K}}$, it is well known that in such a case $\mathcal{O}$ is not a Dedekind domain, and indeed all prime ideals of $\mathcal{O}$ that are not co-prime to the *conductor ideal* of $\mathcal{O}$ are not invertible (see e.g. Theorem 6.1 in [Cona]) and hence are not part of ideal-class group. 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 sub-orders of $\mathcal{O}_{\mathbf{K}}$ [Cona, Remark 2.3], these non-bigenic ideals have a diagonal Hermite normal form $\mathbb{Z}$-basis, and in any case these example ideals are as it is ideals of the larger ring $\mathcal{O}_{\mathbf{K}}$. We will show below a non-trivial ideal of an order of power-of-two cyclotomic field that requires a minimum of three generators.

Consider the cyclotomic field $\mathbf{K} = \mathbb{Q}[X]/(X^4 + 1)$. It is well known that its ring of integers $\mathcal{O}_{\mathbf{K}}$ is same as the polynomial ring $\mathbb{Z}[X]/(X^4 + 1)$ (see Appendix F). Now consider a sub-order $\mathcal{O}$ of this field with $\mathbb{Z}$-basis $\boldsymbol{B}(\mathcal{O})$ as given below:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

It is not difficult to see that $\mathcal{O}$ forms a ring, e.g. $(4 * a_1 * X) * (2 * a_2 * X^2)$ is an integer multiple of $4 * X^3$, and $(4 * a_3 * X^3) * (2 * a_2 * X^2)$ reduced modulo $X^4 + 1$ is an integer multiple of $4 * X$. Also, check that $\mathcal{O}_{\mathbf{K}} \subset \frac{1}{4} \cdot \mathcal{O}$ and $[\mathcal{O}_{\mathbf{K}} : \mathcal{O}] = 32$. Further, it is easy to check that the conductor ideal of $\mathcal{O}$ is $(4, 4X, 4X^2, 4X^3)$.

Proposition 6.1. *The ideal $\mathcal{I} = (8X, 2X^2 + 2, 4X^3 - 4X)$ of order $\mathcal{O}$ above has the following properties*

(i) *$\mathcal{I}$ is not bigenic,*
(ii) *no rational scaling of $\mathcal{I}$ is a bigenic ideal of $\mathcal{O}$,*
(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.*
(v) *$\mathcal{I}$ is not contained in the conductor ideal of $\mathcal{O}$.*
(vi) *$2\mathcal{I}$ is product of two bigenic ideals, namely $2\mathcal{I} = (2, 4X^3) \cdot (8X, 2X^2 + 2)$, whereas $2\mathcal{I}$ is not bigenic.*
(vii) *$\mathcal{I}$ is not invertible as a fractional ideal of $\mathcal{O}$.*

For a proof of the proposition, see Appendix D, where we also extend it to general power-of-two cyclotomic fields. Properties (i) and (vi) imply that bigenic ideals of $\mathcal{R}$ above do not form a multiplicative group. This is in contrast to principal ideals that do form a multiplicative group which is the basis of definition of ideal class groups [FT91]. It is worth remarking that $(8X, 2X^2 + 2)$ is not a prime ideal as it is contained in $(4X, 2X^2 + 2)$ and it is well-known that all non-zero prime ideals (of any order of a number field) are maximal [Cond, Sec. 8].

6.1 Non-ideal Lattices in Cyclotomic Number Fields

We now give examples of sums of ideals of different orders that are not an ideal of any order in the number field. We will focus on the popular power-of-two cyclotomic number fields. As before, consider the cyclotomic number field $\mathbf{K} = \mathbb{Q}[X]/(X^4 + 1)$. Consider two orders $\mathcal{O}_1$, $\mathcal{O}_2$ in $\mathbf{K}$ given by the following $\mathbb{Z}$-bases.

$$\mathcal{O}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 8 \end{pmatrix} \qquad \mathcal{O}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 8 \end{pmatrix} \qquad \mathcal{O}' = \mathcal{O}_1 \cap \mathcal{O}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 8 \end{pmatrix}$$

Now, consider the ideal $\mathcal{I}_1$ of $\mathcal{O}_1$ given by $(2X + 2)\mathcal{O}_1$, and ideal $\mathcal{I}_2$ of $\mathcal{O}_2$ given by $(2, 2X^2 + 2)\mathcal{O}_2$. It is not difficult to see that a $\mathbb{Z}$-basis of $\mathcal{I}_1 + \mathcal{I}_2$ is $(2, 2X, 2X^2, 8X^3)$. However, $\mathcal{I}_1 + \mathcal{I}_2$ is not an ideal of any order in $\mathbf{K}$ as shown below.

Lemma 6.2. *For $\mathcal{I}_1, \mathcal{I}_2$ as above, $\mathcal{I}_1 + \mathcal{I}_2$, i.e. the lattice given by $\mathbb{Z}$-basis $(2, 2X, 2X^2, 8X^3)$ is not an ideal of any order in the number field $\mathbf{K} = \mathbb{Q}[X]/(X^4+1)$.*

Proof. Suppose $\mathcal{O}_3$ is some order in $\mathbf{K}$ such that the lattice $(2, 2X, 2X^2, 8X^3)$ is an ideal of $\mathcal{O}_3$. By lemma 2.2 any $\mathbb{Z}$-basis of $\mathcal{O}_3$ can be assumed to contain a basis vector 1. Then, it follows by computing Hermite normal form of this basis that w.l.o.g. another basis element is just $c \cdot X$, where c is some integer. If the above is an ideal of $\mathcal{O}_3$, then $c \cdot 2X^2 * X = 2c \cdot X^3$ must also be in the ideal. Given the above $\mathbb{Z}$-basis of the ideal, it follows that $2c$ is a multiple of 8, or c is a multiple of 4. But, this implies that the element $2X$ in in the above lattice is not even in the order $\mathcal{O}_3$, and hence the above lattice is not an ideal of $\mathcal{O}_3$, a contradiction.

References

[AD17] Martin R. Albrecht and Amit Deo. Large modulus ring-LWE $\geq$ module-LWE. In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 267–296. Springer, Heidelberg, December 2017. 1

[AM69] Michael Francis Atiyah and I. G. MacDonald. *Introduction to commutative algebra.* Addison-Wesley-Longman, 1969. 1, 2.2, 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, *ASIACRYPT 2019, Part II*, volume 11922 of *LNCS*, pages 91–120. Springer, Heidelberg, December 2019. 1, 1

[BBS21] M. Bolboceanu, Z. Brakerski, and D. Sharma. On algebraic embedding for unstructures lattices, 2021. `https://eprint.iacr.org/2021/053.pdf`. 1, 1, 1

[BDK$^+$18] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS - kyber: A cca-secure module-lattice-based KEM. In *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018*, pages 353–367. IEEE, 2018. 4

[Ber14] D. Bernstein. A subfield-logarithm attack against ideal lattices. Feb 2014. `http://blog.cr.yp.to/20140213-ideal.html`. 1

[BF14] J.-F. Biasse and C. Fieker. Subexponential class group and unit group computation in large degree number fields. *LMS J. Comput. Math.*, 17 (suppl. A):385–403, 2014. 6, 1, 1

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS 2012*, pages 309–325. ACM, January 2012. 1, 1

[Bra12] Zvika Brakerski. Fully homomorphic encryption without modulus switching from classical GapSVP. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 868–886. Springer, Heidelberg, August 2012. 1

[BS16] J.-F. Biasse and F. Song. A polynomial time quantum algorithm for computing class groups and solving the principal ideal problem in arbitrary degree number fields. *Proc. SODA*, 2016. 6, 1

[CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 559–585. Springer, Heidelberg, May 2016. 1

[CDW17] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Short stickelberger class relations and application to ideal-SVP. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 324–348. Springer, Heidelberg, April / May 2017. 1, 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, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 3–33. Springer, Heidelberg, December 2016. 1

[CGS14] P. Campbell, M. Groves, and D. Shepherd. Soliloquy: A cautionary tale. *ETSI 2nd Quantum-Safe Crypto Workshop*, 2014. 1

[CHK$^+$18] Jung Hee Cheon, Kyoohyung Han, Andrey Kim, Miran Kim, and Yongsoo Song. A full RNS variant of approximate homomorphic encryption. In *Selected Areas in Cryptography - SAC 2018 - 25th International Conference, Calgary, AB, Canada, August 15-17, 2018, Revised Selected Papers*, volume 11349 of *Lecture Notes in Computer Science*, pages 347–368. Springer, 2018. 4

[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, *ASIACRYPT 2017, Part I*, volume 10624 of *LNCS*, pages 409–437. Springer, Heidelberg, December 2017. 1

[Cla84] A. Clark. *Elements of Abstract Algebra*. Dover Books on Mathematics Series. Dover Publications, 1984. 3, 1, E

[Cona] Keith Conrad. The conductor ideal of an order. Expository paper. url: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf`. 1, 1, 2.2, 2.2, 6, A, D, D

[Conb] Keith Conrad. Dedekind's index theorem. Expository papers/Lecture notes. Available at: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekind-index-thm.pdf`. F, F

[Conc] Keith Conrad. The different ideal. Expository papers/Lecture notes. Available at: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf`. 9

[Cond] Keith Conrad. Ideal factorization. Expository paper. url: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf`. 1, 2.2, 2.3, 6

[Cone] Keith Conrad. Personal communication. 2.2, 2.2

[DM15] Léo Ducas and Daniele Micciancio. FHEW: Bootstrapping homomorphic encryption in less than a second. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 617–640. Springer, Heidelberg, April 2015. 1

[Eis13] David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013. 2.1, 2.2

[FT91] A. Fröhlich and M. J. Taylor. *Algebraic Number Theory.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1991. 1, 2.2, 6, D, E, *(i)*, *(iv)*, *(v)*, *(vi)*, *(vii)*, F

[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 ACM STOC*, pages 169–178. ACM Press, May / June 2009. 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, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 75–92. Springer, Heidelberg, August 2013. 1

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory.* Springer-Verlag Berlin, 1990. 1

[JL22] Charanjit S. Jutla and Chengyu Lin. Enhancing ring-lwe hardness using dedekind index theorem. *IACR Cryptol. ePrint Arch. 1631*, 2022. ⋆

[Lan02] Serge Lang. *Algebra.* Springer, 2002. 2.2

[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, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Heidelberg, May / June 2010. 1, 5, 1, 1, 1.1, 1.1, 1.1, 5.2, 5, 5

[LS15] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.*, 75(3):565–599, 2015. 1

[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. 2.7, 2.8, 2.9

[PP19] Chris Peikert and Zachary Pepin. Algebraically structured LWE, revisited. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part I*, volume 11891 of *LNCS*, pages 1–23. Springer, Heidelberg, December 2019. 1, 1

[PR07] Chris Peikert and Alon Rosen. Lattices that admit logarithmic worst-case to average-case connection factors. In David S. Johnson and Uriel Feige, editors, *39th ACM STOC*, pages 478–487. ACM Press, June 2007. 1

[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 ACM STOC*, pages 461–473. ACM Press, June 2017. 1, 1.1, 2.7, 2.5, 5, 5, 5, 5, 5.5, 5, 5, 5

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005. 1, 1.1

[Reg06] Oded Regev. Lattice-based cryptography (invited talk). In Cynthia Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 131–141. Springer, Heidelberg, August 2006. 5

[Reg10] Oded Regev. The learning with errors problem (invited survey). In *2010 IEEE 25th Annual Conference on Computational Complexity*, pages 191–204, June 2010. 5

[RSW18] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the ring-LWE and polynomial-LWE problems. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 146–173. Springer, Heidelberg, April / May 2018. 1

[SSTX09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 617–635. Springer, Heidelberg, December 2009. 1

A Full Proofs of Lemmas

Lemma A.1. (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 $\mathfrak{n}_1, ..., \mathfrak{n}_k$.*

(xiv) *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).*

Proof. Proof of ((*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 $\mathfrak{p}$. 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 ((*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 $\mathfrak{b}\mathfrak{c}$. 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 ((*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: 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 ((*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 $\mathfrak{n}_1, ..., \mathfrak{n}_k$. 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 (*viii*)), and hence maximal ideal $\mathfrak{n}_i$ is itself in maximal ideal $\mathfrak{m}$, an absurdity.

Proof of $((xiv))$. This can be proved easily in multiple ways, but we prefer an argument used in Prop. 2.5 in [LLL82].

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.

The proof of the following lemma is similar to proof of [Cona, Theorem 3.6].
Lemma 2.4 (repeated) An ideal $\mathfrak{b}$ of $\mathcal{O}$ that is relatively prime to principal ideal $m\mathcal{O}$ is a product of prime ideals of $\mathcal{O}$.

Proof. If $\mathfrak{b}$ is prime, we are done. Otherwise let $\mathfrak{p} \supset \mathfrak{b}$ for a maximal ideal $\mathfrak{p}$. We have $\mathfrak{p} + (m) \supset \mathfrak{b} + (m) = \mathcal{O}$, and hence $\mathfrak{p}$ is relatively prime to (m). Thus, $\mathfrak{p}$ cannot contain (m), and hence by Theorem 2.3, $\mathfrak{p}$ is invertible. Let $\mathfrak{b}' = \mathfrak{p}^{-1}\mathfrak{b}$. Since $\mathfrak{p}^{-1}\mathfrak{p} = \mathcal{O}$, $\mathfrak{p}^{-1}\mathfrak{b} \subset \mathcal{O}$ and $\mathfrak{p}\mathfrak{b}' = \mathfrak{b}$. Since $\mathfrak{b} \neq \mathfrak{p}$, $\mathfrak{b}' \neq (1)$. Since $\mathfrak{p}\mathfrak{b}' \subset \mathfrak{b}'$ and the inclusion is strict (if not then for all $k \geq 0$ we have $\mathfrak{b}' = \mathfrak{p}^k \mathfrak{b}' \subset \mathfrak{p}^k$, which is a contradiction for large k since $[\mathcal{O} : \mathfrak{p}^k]$ gets large with k while $[\mathcal{O} : \mathfrak{b}']$ is finite), $\mathfrak{b}'$ as a smaller index in $\mathcal{O}$ than $\mathfrak{b}$. Since $\mathfrak{b}' \supset \mathfrak{b}$ and $\mathfrak{b} + (m) = \mathcal{O}$, we have $\mathfrak{b}' + (m) = \mathcal{O}$. So, by induction on the index of $\mathfrak{b}'$, $\mathfrak{b}'$ is a product of prime ideals. And hence $\mathfrak{b}$ itself is a product of prime ideals.

For the proof of the following lemma we need the concept of the radical (ideal) of an ideal. For an ideal $\mathfrak{a}$ of a ring R, its radical is the set of all $a \in R$ such that $a^n \in \mathfrak{a}$ for some $n \geq 1$. It is easy to check that this is an ideal, and also a prime ideal when $\mathfrak{a}$ is a primary ideal.
Lemma 2.6 (repeated) Let $m = [\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$, and q be a positive integer relatively prime to m. Then, the quotient ring $\mathcal{O}/q\mathcal{O}$ is isomorphic to $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$ by the ring isomorphism $\phi : \mathcal{O}/q\mathcal{O} \rightarrow \mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}} :: \phi(\mathbf{x}) = \ell \cdot \mathbf{x}$, where ℓ is any integer such that $\ell \cdot m = 1 \bmod q$. The isomorphism ϕ is inverted by multiplication by m.

Proof. By lemma 2.2(v) the size of both quotient rings $\mathcal{O}/q\mathcal{O}$ and $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$ is q^n. Further, since $\mathbb{Z} \subset \mathcal{O} \subset \mathcal{O}_{\mathbf{K}}$, the map ϕ maps $\mathcal{O}$ to $\mathcal{O}_{\mathbf{K}}$. We show that it is injective over $\mathcal{O}/q\mathcal{O}$, by showing that it is inverted by multiplication by m. Indeed, $m \cdot \ell \cdot \mathbf{x} = \mathbf{x} \bmod q\mathcal{O}$. Since ϕ is easily seen to be a ring homomorphism from $\mathcal{O}/q\mathcal{O}$ to $\mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$, that completes the proof.

Lemma 4.2 (repeated) For any positive integer q, and for an ideal $\mathfrak{a}$ of $\mathcal{O}$ such that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}$ for m co-prime to q, a $\mathbf{g} \in \mathfrak{a}$ generates the ideal $\mathfrak{a}/q\mathfrak{a}$ iff $\det(\boldsymbol{C}_g) \cdot \det(\boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))/\det(\boldsymbol{B}(\mathfrak{a}))$ is co-prime to q.

Proof. Let $\boldsymbol{B}(\mathcal{O})$ be a $\mathbb{Z}$-basis of $\mathcal{O}$. Since $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}$, by lemma 2.2($v$), we have $m \cdot \boldsymbol{B}(\mathcal{O}_{\mathbf{K}}) = \boldsymbol{B}(\mathcal{O})\boldsymbol{L}$, and $\boldsymbol{B}(\mathcal{O}) = \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{M}$ for some integer matrices $\boldsymbol{L}$ and $\boldsymbol{M}$. Thus, $m \cdot I = \boldsymbol{ML}$ and $m^n = \det \boldsymbol{L} \cdot \det \boldsymbol{M}$. Since m is co-prime to q, both $\det \boldsymbol{M}$ (index of $\mathcal{O}$ in $\mathcal{O}_{\mathbf{K}}$) and $\det \boldsymbol{L}$ are co-prime to q. Thus, by Theorem 3.7, $\mathfrak{a}/q\mathfrak{a}$ is guaranteed to be principal.

Let $\mathbf{g} \in \mathfrak{a}$ be such that it generates the ideal $\mathfrak{a}/q\mathfrak{a}$. First, by lemma 2.10 and lemma 2.2(v),

$$\boldsymbol{C}_g \cdot \boldsymbol{B}(\mathcal{O}) = \boldsymbol{B}(\mathfrak{a}) \cdot \boldsymbol{D}, \tag{5}$$

where $\boldsymbol{D}$ is an integer matrix. To prove the "only if" part, since $\det \boldsymbol{M}$ is co-prime to q, we only need to show that the determinant of $\boldsymbol{D}$ is co-prime to q. Since, $\mathfrak{a} = \mathbf{g}\mathcal{O} + q\mathfrak{a}$, we also have that every column of $\boldsymbol{B}(\mathfrak{a})$ is generated by $\mathbf{g}$ mod $q\mathfrak{a}$. Thus,

$$\boldsymbol{B}(\mathfrak{a}) = \boldsymbol{C}_g\boldsymbol{B}(\mathcal{O})\boldsymbol{U} + q \cdot \boldsymbol{B}(\mathfrak{a})\boldsymbol{T} \tag{6}$$

for some integer matrices $\boldsymbol{U}$ and $\boldsymbol{T}$. Substituting $\boldsymbol{B}(\mathfrak{a}) \cdot \boldsymbol{D}$ for $\boldsymbol{C}_g \cdot \boldsymbol{B}(\mathcal{O})$, and noting that $\boldsymbol{B}(\mathfrak{a})$ is full ranked, we get that $\boldsymbol{D} \cdot \boldsymbol{U} = I \pmod{q}$, which proves that determinant of $\boldsymbol{D}$ is co-prime to q.

For the other direction, since $\boldsymbol{C}_g\boldsymbol{B}(\mathcal{O}) = \boldsymbol{B}(\mathfrak{a}) \cdot \boldsymbol{D}$, and $\det \boldsymbol{M}$ is co-prime to q, the determinant of integer matrix $\boldsymbol{D}$ is co-prime to q. Hence, let $u = \det(\boldsymbol{D})^{-1} \pmod{q}$ and $\boldsymbol{U} = u \cdot \det(\boldsymbol{D}) \cdot \boldsymbol{D}^{-1}$ be an integer matrix. We have $\boldsymbol{D} \cdot \boldsymbol{U} = I \pmod{q}$, and consider the following map ψ:

$$\psi : \mathfrak{a}/q\mathfrak{a} \to \mathcal{O}/q\mathcal{O} :: \psi(\mathbf{z}) = \boldsymbol{B}(\mathcal{O})\boldsymbol{U}\boldsymbol{B}(\mathfrak{a})^{-1}\mathbf{z} \pmod{q\mathcal{O}}$$

For any $\mathbf{z} \in \mathfrak{a}$, and since $\mathbf{g} \in \mathfrak{a}$,

$$\mathbf{g} * \psi(\mathbf{z}) = \boldsymbol{C}_g\boldsymbol{B}(\mathcal{O})\boldsymbol{U}\boldsymbol{B}(\mathfrak{a})^{-1}\mathbf{z} \bmod q\mathfrak{a} = \boldsymbol{B}(\mathfrak{a}) \cdot \boldsymbol{D} \cdot \boldsymbol{U}\boldsymbol{B}(\mathfrak{a})^{-1}\mathbf{z} = \mathbf{z} \bmod q\mathfrak{a}$$

Hence, $\mathbf{z}$ mod $q\mathfrak{a}$ is in $\mathbf{g} \cdot \mathcal{O}/q\mathcal{O}$.

B Characterization of Dual Ideals

Lemma 2.11 (repeated) For an ideal $\mathcal{I}$ of $\mathcal{O}$ with basis $\boldsymbol{B}(\mathcal{I})$

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 $(\boldsymbol{V}^\top\boldsymbol{V})^{-1} \cdot \boldsymbol{B}(\mathcal{I})^{-\top}$ has rational entries,
iii) the dual $\mathcal{I}^\vee$ is a fractional ideal of $\mathcal{O}$.

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 a rational matrix for $\mathcal{I} \subseteq \mathcal{O}$. 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 $\mathbf{g} \in \mathcal{O}$ 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 $\mathcal{O}$. Now, again by commutativity, for every $\mathbf{d} \in \mathcal{O}$, $\mathbf{d}\mathcal{I}^\vee$ is also closed under multiplication by $\mathcal{O}$. Thus (iii) follows from (i) and (ii).

Lemma 2.12 (repeated) For an ideal $\mathcal{I}$ of $\mathcal{O}$, for any $\mathbf{a} \in \mathcal{I}$ and any $\mathbf{b} \in \mathcal{I}^\vee$, $\mathbf{a} * \mathbf{b} \in \mathcal{O}^\vee$.

Proof. Since $\mathcal{I}$ is an ideal of $\mathcal{O}$, $\mathbf{a} * \mathbf{c}$ is in $\mathcal{I}$, for any $\mathbf{c}$ in $\mathcal{O}$. By definition of the dual-ideal (applied to dual of $\mathcal{I}$), $\mathrm{Tr}(\mathbf{b}, \mathbf{a} * \mathbf{c}) \in \mathbb{Z}$. Since this trace is same as trace of $\boldsymbol{V} \cdot (\mathbf{a} * \mathbf{b} * \mathbf{c})$, this also implies that $\mathrm{Tr}(\mathbf{a} * \mathbf{b}, \mathbf{c}) \in \mathbb{Z}$. Since this holds for all $\mathbf{c} \in \mathcal{O}$, again by definition of dual ideal (applied to dual of $\mathcal{O}$), $\mathbf{a} * \mathbf{b}$ is in dual of $\mathcal{O}$, i.e. $\mathcal{O}^\vee$.

Lemma 2.13 (repeated) For $g(X) \in \mathcal{R}_\mathbb{Q}$, we have $\boldsymbol{C}_g(\boldsymbol{V}^\top \boldsymbol{V})^{-1} = (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{C}_g^\top$, and $(\boldsymbol{V}^\top \boldsymbol{V})\boldsymbol{C}_g = \boldsymbol{C}_g^\top (\boldsymbol{V}^\top \boldsymbol{V})$.

Proof. Note that the Vandermonde matrix $\boldsymbol{V}$ diagonalizes the circulant matrix $\boldsymbol{V}\boldsymbol{C}_g\boldsymbol{V}^{-1} = \boldsymbol{D}_g$. Thus,

$$\boldsymbol{V}^\top \boldsymbol{V} \boldsymbol{C}_g = \boldsymbol{V}^\top \boldsymbol{D}_g \boldsymbol{V} = \boldsymbol{V}^\top \boldsymbol{D}_g^\top \boldsymbol{V} = (\boldsymbol{D}_g \boldsymbol{V})^\top \boldsymbol{V} = (\boldsymbol{V}\boldsymbol{C}_g)^\top \boldsymbol{V} = \boldsymbol{C}_g^\top \boldsymbol{V}^T \boldsymbol{V}.$$

Lemma 2.14 (repeated) Let $\mathcal{O}_1$ be a sub-order of $\mathcal{O}_2$, both orders of rank n. If for some integer m, $m\mathcal{O}_2 \subset \mathcal{O}_1$, then $[\mathcal{O}_2 : \mathcal{O}_1]$ divides m^n. Further, $m\mathcal{O}_1^\vee \subset \mathcal{O}_2^\vee$.

Proof. By lemma 2.2(v), $\boldsymbol{B}(\mathcal{O}_1) = \boldsymbol{B}(\mathcal{O}_2)\boldsymbol{M}$, where $\boldsymbol{M}$ is an integer matrix with determinant $[\mathcal{O}_2 : \mathcal{O}_1]$. Now, if $m\mathcal{O}_2 \subset \mathcal{O}_1$, since $m\mathcal{O}_2$ is an additive subgroup of $\mathcal{O}_1$, we again have $m \cdot \boldsymbol{B}(\mathcal{O}_2) = \boldsymbol{B}(\mathcal{O}_1)\boldsymbol{L}$, for some integer matrix $\boldsymbol{L}$. Then, $m \cdot I = \boldsymbol{L}\boldsymbol{M}$, which proves the first claim. The second claim follows by using the basis of dual ideals as given by Lemma 2.11.

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 B.1. *Given $f(X)$ with all distinct roots, its derivative $f'(X)$ shares no common root with $f(X)$.*

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 $\mathcal{O}^\vee$ has the circulant matrix of the inverse of $f'(X)$ as a $\mathbb{Z}$-basis, and since $\mathcal{O}^\vee$ is also a fractional ideal of $\mathcal{O}$, it can also be seen as the fractional ideal [9] 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 B.2. $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} = \boldsymbol{C}_{f'}^{-1}\boldsymbol{M}$.

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 B.3. *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:

Proposition B.4. *For $g(X) \in \mathcal{R}_\mathbb{Q}$, $\boldsymbol{C}_g\boldsymbol{M}$ is symmetric.*

[9] 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 $f'(X)$.

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.

Lemma 2.15 (repeated) For any ideal $\mathcal{I}$ of order $\mathcal{O}$ in number field $\mathbf{K} = \mathbb{Q}[X]/(f(X))$, and $\mathbf{r} \in \mathcal{H}$, where

$$c \ := \ \left(\prod_{i=1}^{n} r_i\right)^{1/n} \cdot ([\mathcal{O} : \mathcal{I}] \cdot \mathrm{disc}(\mathcal{O}))^{-1/n} \ \geq 1,$$

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 $\mathcal{L}_r^\vee = \mathbf{R} \cdot (\boldsymbol{V} \cdot \mathcal{L}(\mathcal{I}))^\vee$. 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 $\mathbf{w} \in \mathcal{I}^\vee$. By lemma 2.2($v$), any basis of $\mathcal{I}$ is given by $\boldsymbol{B}(\mathcal{O}) \cdot \boldsymbol{M}$ where $\boldsymbol{M}$ is an integer matrix and $[\mathcal{O} : \mathcal{I}] = \det(\boldsymbol{M})$.

Claim: for $\mathbf{w} \in \mathcal{I}^\vee$, $\prod_i (\boldsymbol{V}\mathbf{w})_i \ \geq \ \mathrm{disc}(\mathcal{O})^{-1} \cdot \det(\boldsymbol{M})^{-1}$.

Proof of Claim: We proved in lemma 2.11 that $\mathcal{I}^\vee$ is a fractional ideal of $\mathcal{O}$ that is $\mathbb{Z}$-spanned by $(\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-T}$. 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, by lemma 2.10, a $\mathbb{Z}$-basis of principal ideal $(\mathbf{w})$ is given by $\boldsymbol{C}_w\boldsymbol{B}(\mathcal{O})$, which being a sub-ideal of $\mathcal{I}^\vee$ implies (by lemma 2.2(v)) that $\boldsymbol{C}_w\boldsymbol{B}(\mathcal{O}) = (\boldsymbol{V}^\top\boldsymbol{V})^{-1}\boldsymbol{B}(\mathcal{I})^{-T}\boldsymbol{U}$, where $\boldsymbol{U}$ 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 with diagonal the vector $\boldsymbol{V}\mathbf{w}$ (see equation (1)). Since, by above, $\det(\boldsymbol{C}_w)\det(\boldsymbol{B}(\mathcal{O})) \ \geq \ \det(\boldsymbol{V}^\top\boldsymbol{V})^{-1} \cdot \det(\boldsymbol{B}(\mathcal{I}))^{-1}$, we have that $\prod_i (\boldsymbol{V}\mathbf{w})_i \geq \det(\boldsymbol{V}^\top\boldsymbol{V})^{-1} \cdot \boldsymbol{M}^{-1} \cdot \det(\boldsymbol{B}(\mathcal{O}))^{-2}$. Since $\det(\boldsymbol{V}^\top\boldsymbol{V})$ is exactly Δ_f, the claim follows from definition of disc($\mathcal{O}$).

Thus, for any $\mathbf{w}$ in $\mathcal{L}_r^\vee$, $\|\mathbf{w}\|$ 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 $\lambda_1(\mathcal{L}_r^\vee) \geq c\sqrt{n}$. Lemma 2.8 then implies that $1 \geq \eta_\epsilon(\mathcal{L}_r)$, or equivalently $\mathbf{r} \geq \eta_\epsilon(\mathcal{L}(\mathcal{I}))$.

C Ideal Clearing Lemma for Sum of Ideals

Lemma 5.8 (repeated)

(i) If $\mathcal{O}_1$ and $\mathcal{O}_2$ are orders in number field $\mathbf{K}$, then $\mathcal{O}_1 \cap \mathcal{O}_2$ is also an order in $\mathbf{K}$.

(*ii*) If $\mathcal{I}_1$ is an ideal of order $\mathcal{O}_1$, and $\mathcal{I}_2$ is an ideal of $\mathcal{O}_2$, then $(\mathcal{I}_1+\mathcal{I}_2)\cap\mathcal{O}_1\cap\mathcal{O}_2$ is an ideal of order $\mathcal{O}_1 \cap \mathcal{O}_2$.

(*iii*) Let m be an integer such that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_1 \cap \mathcal{O}_2$. Then, $m\mathcal{I}_1 \subset \mathcal{I}_1 \cap \mathcal{O}_2$ and $m\mathcal{I}_2 \subset \mathcal{I}_2 \cap \mathcal{O}_1$. Further, $m(\mathcal{I}_1 + \mathcal{I}_2) \subset (\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2$.

(*iv*) Let m be an integer such that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_1 \cap \mathcal{O}_2$. Then, any $\mathbb{Z}$-basis of $(\mathcal{I}_2+\mathcal{I}_2)\cap\mathcal{O}_1\cap\mathcal{O}_2$, $\boldsymbol{B}((\mathcal{I}_2+\mathcal{I}_2)\cap\mathcal{O}_1\cap\mathcal{O}_2)$, can be written as $\boldsymbol{B}(\mathcal{I}_1+\mathcal{I}_2)\cdot\boldsymbol{M}$, where $\boldsymbol{M}$ is an integer matrix and a prime divides $\det \boldsymbol{M}$ only if it divides m.

Proof. (*i*) Since $\mathcal{O}_1$ and $\mathcal{O}_2$ are orders, both contain one, and hence their intersection does too. Further, there are integers m_1 and m_2 such that $m_1\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_1$ and $m_2\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_2$ (by lemma 2.2(v)). Thus, $m_1 m_2\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_1 \cap \mathcal{O}_2$. And hence a Z-basis of $cO_1 \cap \mathcal{O}_2$, which is obtained as a basis of $(\mathcal{O}_1^* \cup \mathcal{O}_2^*)^*$, is a $\mathbb{Q}$-basis of $\mathbf{K}$ (since the basis of $\mathcal{O}_{\mathbf{K}}$ is a $\mathbb{Q}$-basis of $\mathbf{K}$). It is easy to check that $\mathcal{O}_1 \cap \mathcal{O}_2$ is closed under multiplication, and that finishes the proof of the claim using the definition of an order to be a ring with unit such that its $\mathbb{Z}$-basis is a $\mathbb{Q}$-basis of $\mathbf{K}$.

(*ii*) Let $x \in \mathcal{O}_1 \cap \mathcal{O}_2$ and $y \in (\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2$ be arbitrary. Then xy is in $\mathcal{O}_1$ and $\mathcal{O}_2$ by the closure properties of the orders. Now, let $y = y_1 + y_2$ where $y_1 \in \mathcal{I}_1$ and $y_2 \in \mathcal{I}_2$. Thus, $xy_1 \in \mathcal{I}_1$ and $xy_2 \in \mathcal{I}_2$. So, $xy = xy_1 + xy_2$ is in $\mathcal{I}_1 + \mathcal{I}_2$ as well.

(*iii*) Since $\mathcal{O}_1 \subset \mathcal{O}_b K$, as the latter is the maximal order, we have $m\mathcal{O}_1 \subset m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}_2$. Thus, $m\mathcal{I}_1 \subset m\mathcal{O}_1\ subset\mathcal{O}_2$, and the first claim follows. Next, $m\mathcal{I}_1 + m\mathcal{I}_2 \subset \mathcal{I}_1 \cap \mathcal{O}_2 + \mathcal{I}_2 \cap \mathcal{O}_1$. Thus, $m(\mathcal{I}_1 + \mathcal{I}_2) \subset (\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2$.

(*iv*) Note that $(\mathcal{I}_1+\mathcal{I}_2)\cap\mathcal{O}_1\cap\mathcal{O}_2 = \mathcal{I}_1\cap\mathcal{O}_2+\mathcal{I}_2\cap\mathcal{O}_1$, where addition on the right hand side is of additive groups or $\mathbb{Z}$-modules. Then, by the previous item, $m\mathcal{I}_1 + m\mathcal{I}_2 \subset \mathcal{I}_1 \cap \mathcal{O}_2 + \mathcal{I}_2 \cap \mathcal{O}_1$. Thus, $m(\mathcal{I}_1 + \mathcal{I}_2) \subset (\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2 \subset \mathcal{I}_1+\mathcal{I}_2$. Since all these $\mathbb{Z}$-modules are rank n Z-modules (see lemma 2.2(iv)), we have[10] by lemma 2.2(v), $m\boldsymbol{B}(\mathcal{I}_1 + \mathcal{I}_2) = \boldsymbol{B}((\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2)\boldsymbol{M}_1$ and $\boldsymbol{B}((\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2) = \boldsymbol{B}(\mathcal{I}_1 + \mathcal{I}_2)\boldsymbol{M}$, where $\boldsymbol{M}_1$ and $\boldsymbol{M}$ are $n \times n$ integer matrices (note, $n = [\mathbf{K} : \mathbb{Q}]$). Thus, $m \cdot I = \boldsymbol{M}_1\boldsymbol{M}$. Since $\det \boldsymbol{M}$ is $[\mathcal{I}_1 + \mathcal{I}_2 : (\mathcal{I}_2 + \mathcal{I}_2) \cap \mathcal{O}_1 \cap \mathcal{O}_2]$ by lemma 2.2(v), the claim follows.

Lemma 5.9 (repeated) "Sum of Ideals of Different Orders" Clearing Lemma. Fix a number field $\mathbf{K}$ with a known $\mathbb{Z}$-basis for its ring of integers $\mathcal{O}_{\mathbf{K}}$. For any relatively prime positive integers q and m, and any orders $\mathcal{O}_1, \mathcal{O}_2$ such that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}' = \mathcal{O}_1 \cap \mathcal{O}_2$, for any ideals $\mathcal{I}_1$ of $\mathcal{O}_1$ and ideals $\mathcal{I}_2$ of $\mathcal{O}_2$, given a generator $\mathbf{g} \in \mathcal{I}' = (\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}'$ for the principal ideal $\mathcal{I}'/q\mathcal{I}'$, and given $\det(\mathcal{I}_1 + \mathcal{I}_2)$,

(*i*) there is an efficiently computable map $\psi : \mathcal{I}_1 + \mathcal{I}_2 \to \mathcal{O}_{\mathbf{K}}$ that induces an efficiently computable $\mathbb{Z}$-module isomorphism $\psi : (\mathcal{I}_1 + \mathcal{I}_2)/q(\mathcal{I}_1 + \mathcal{I}_2) \to \mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$,

[10] although lemma 2.2(v) is stated in terms of ideals and orders, the lemma holds for all finite ranked sub-$\mathbb{Z}$-modules of the same rank.

(ii) there is an efficiently computable map $\phi : m(\mathcal{I}_1+\mathcal{I}_2)^\vee \to \mathcal{O}_{\mathbf{K}}^\vee$ that induces an efficiently invertible $\mathbb{Z}$-module isomorphism $\phi : m(\mathcal{I}_1+\mathcal{I}_2)^\vee/qm(\mathcal{I}_1+\mathcal{I}_2)^\vee \to \mathcal{O}_{\mathbf{K}}^\vee/q\mathcal{O}_{\mathbf{K}}^\vee$,

(iii) such that, for any $\mathbf{z} \in \mathcal{I}_1 + \mathcal{I}_2$ and $\mathbf{x} \in m \cdot (\mathcal{I}_1 + \mathcal{I}_2)^\vee$, their polynomial product satisfies

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

Proof. By lemma 5.8, $\mathcal{I}' = (\mathcal{I}_1 + \mathcal{I}_2) \cap \mathcal{O}'$ is an ideal of $\mathcal{O}'$, where $\mathcal{O}'$ is the order $\mathcal{O}_1 \cap \mathcal{O}_2$. Moreover, it is given that $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}'$. Then, by theorem 3.7 ideal $\mathcal{I}'$ of $\mathcal{O}'$ is principal modulo $q\mathcal{I}'$, i.e. $\mathcal{I}'/q\mathcal{I}'$ (as an ideal of $\mathcal{O}'/q\mathcal{I}'$) is principal. Let $\mathbf{g}$ be a generator of this principal ideal. Let $\boldsymbol{B}(\mathcal{O}')$ be a $\mathbb{Z}$-basis of $\mathcal{O}'$. Since $m\mathcal{O}_{\mathbf{K}} \subset \mathcal{O}'$, by lemma 2.2($v$), we have $m \cdot \boldsymbol{B}(\mathcal{O}_{\mathbf{K}}) = \boldsymbol{B}(\mathcal{O}')\boldsymbol{L}$, and $\boldsymbol{B}(\mathcal{O}') = \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})\boldsymbol{M}$ for some integer matrices $\boldsymbol{L}$ and $\boldsymbol{M}$. Thus, $m \cdot I = \boldsymbol{ML}$ and $m^n = \det \boldsymbol{L} \cdot \det \boldsymbol{M}$. Since m is co-prime to q, both $\det \boldsymbol{M}$ (index of $\mathcal{O}'$ in $\mathcal{O}_{\mathbf{K}}$) and $\det \boldsymbol{L}$ are co-prime to q.

Let $\boldsymbol{B}(\mathcal{I}')$ be a $\mathbb{Z}$-basis of $\mathcal{I}'$. Since $\mathbf{g} \in \mathcal{I}'$, by lemma 2.10 and lemma 2.2(v),

$$\boldsymbol{C}_g\boldsymbol{B}(\mathcal{O}') = \boldsymbol{B}(\mathcal{I}') \cdot \boldsymbol{D}, \tag{7}$$

where $\boldsymbol{D}$ is an integer matrix. Since $\mathbf{g}$ generates $\mathcal{I}'/q\mathcal{I}'$, by lemma 4.2 and the fact that $\det \boldsymbol{M}$ is co-prime to q, the determinant of $\boldsymbol{D}$ is co-prime to q. By lemma 5.8 (iv), $\boldsymbol{B}(\mathcal{I}') = \boldsymbol{B}(\mathcal{I}_1 + \mathcal{I}_2)\boldsymbol{M}'$, where a prime divides $\det \boldsymbol{M}'$ only if it divides m. Since m is co-prime to q, it follows that $\det \boldsymbol{M}'$ is co-prime to q. The above equation can be re-written as

$$m \cdot \boldsymbol{C}_g\boldsymbol{B}(\mathcal{O}_{\mathbf{K}}) = \boldsymbol{B}(\mathcal{I}_1 + \mathcal{I}_2) \cdot \boldsymbol{M}' \cdot \boldsymbol{D} \cdot \boldsymbol{L} \tag{8}$$

Denote the determinant of $\boldsymbol{M}'\boldsymbol{DL}$ by d, and let u be an integer such that $u = d^{-1} \bmod q$. Note that d is easily computed as $\det(\boldsymbol{C}_g)*\det(m\cdot\boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))/\det(\boldsymbol{B}(\mathcal{I}_1+\mathcal{I}_2))$.

Now to prove (i)-(iii), consider the following two mappings. For any $\mathbf{z} \in \mathcal{I}_1 + \mathcal{I}_2$ and $\mathbf{x} \in m \cdot (\mathcal{I}_1 + \mathcal{I}_2)^\vee$, define

$$\psi(\mathbf{z}) = d \cdot \mathbf{g}^{-1} * \mathbf{z} \tag{9}$$

$$\phi(\mathbf{x}) = u \cdot \mathbf{g} * \mathbf{x} \tag{10}$$

For (i), we first check that the ψ maps into $\mathcal{O}_{\mathbf{K}}$. Indeed, since $\mathbf{z} \in \mathcal{I}_1 + \mathcal{I}_2$, $\mathbf{z} = \boldsymbol{B}(\mathcal{I}_1+\mathcal{I}_2)\overrightarrow{z}$, for some integer vector $\overrightarrow{z}$. Thus, $\psi(\mathbf{z}) = d\cdot\boldsymbol{C}_g^{-1}\boldsymbol{B}(\mathcal{I}_1+\mathcal{I}_2)\overrightarrow{z}$. By (8),this is same as $\boldsymbol{B}(\mathcal{O}_{\mathbf{K}}) \cdot d \cdot (\boldsymbol{M}'\boldsymbol{DL})^{-1}\overrightarrow{z}$, which shows that $\psi(\mathbf{z}) \in \mathcal{O}_{\mathbf{K}}$.

The induced map $\psi : (\mathcal{I}_1 + \mathcal{I}_2)/q(\mathcal{I}_1 + \mathcal{I}_2) \to \mathcal{O}_{\mathbf{K}}/q\mathcal{O}_{\mathbf{K}}$ is easily inverted by (polynomial) multiplication with $m \cdot \ell \cdot u \cdot \mathbf{g}$, where ℓ is any integer such that $m\cdot\ell = 1 \bmod q$, by noting that $m\cdot\ell\cdot u\cdot d = 1 \bmod q$. Thus, the induced map ψ is an invertible map. It is also surjective since $m\cdot\ell\cdot u\cdot\mathbf{g}*\mathbf{a} = \ell\cdot u\cdot\boldsymbol{C}_g\cdot(m\cdot\mathbf{a})$ is in $\mathcal{I}_1+\mathcal{I}_2$ for any $\mathbf{a} \in \mathcal{O}_{\mathbf{K}}$, as $m\cdot\mathbf{a}$ is in $\mathcal{O}' = \mathcal{O}_1\cap\mathcal{O}_2$. Since, ψ is easily seen to be an $\mathbb{Z}$-module homomorphism, the induced map ψ is an $\mathbb{Z}$-module isomorphism, which is also efficiently computable. This proves (i).

For (ii), we first note that by lemma 2.13 and using (8), for $\mathbf{x} \in m \cdot (\mathcal{I}_1 + \mathcal{I}_2)^\vee$,

$$\begin{aligned} u \cdot \mathbf{g} * \mathbf{x} &= u \cdot (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \boldsymbol{C}_g \cdot \mathbf{x} \\ &= u \cdot (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{C}_g^\top \cdot (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \mathbf{x} \\ &= u \cdot (\boldsymbol{V}^\top \boldsymbol{V})^{-1} (\boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))^{-\top} (\boldsymbol{M'DL})^\top \boldsymbol{B}(\mathcal{I}_1 + \mathcal{I}_2)^\top (\boldsymbol{V}^\top \boldsymbol{V}) \cdot \frac{1}{m} \cdot \mathbf{x} \\ &\in \mathcal{O}_{\mathbf{K}}^\vee \end{aligned}$$

where the last membership follows by noting that $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} (\boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))^{-\top}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_{\mathbf{K}}^\vee$ and $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{B}(\mathcal{I}_1 + \mathcal{I}_2)^{-\top}$ is a $\mathbb{Z}$-basis for $(\mathcal{I}_1 + \mathcal{I}_2)^\vee$ (see lemma 2.11). Now, for the induced map $\phi : m(\mathcal{I}_1 + \mathcal{I}_2)^\vee / qm(\mathcal{I}_1 + \mathcal{I}_2)^\vee \to \mathcal{O}_{\mathbf{K}}^\vee / q\mathcal{O}_{\mathbf{K}}^\vee$, $\phi(\mathbf{x})$ is inverted by (polynomial) multiplication by $d \cdot \mathbf{g}^{-1}$ to $\mathbf{x}$ mod $qm(\mathcal{I}_1 + \mathcal{I}_2)^\vee$.

Further, for any $\mathbf{s} \in \mathcal{O}_{\mathbf{K}}^\vee$, $d \cdot \mathbf{g}^{-1}\mathbf{s}$ lies in $m(\mathcal{I}_1 + \mathcal{I}_2)^\vee$ which is seen as follows: using a basis for $\mathcal{O}_{\mathbf{K}}^\vee$, we have $\mathbf{s} = (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})^{-\top} \overrightarrow{s}$ for some integer vector $\overrightarrow{s}$. Thus, $d \cdot \mathbf{g}^{-1}\mathbf{s}$ is same as $d \cdot \boldsymbol{C}_g^{-1} (\boldsymbol{V}^\top \boldsymbol{V})^{-1} \boldsymbol{B}(\mathcal{O}_{\mathbf{K}})^{-\top} \overrightarrow{s}$. By lemma 2.11, this is same as $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot d \cdot (\boldsymbol{C}_g \boldsymbol{B}(\mathcal{O}_{\mathbf{K}}))^{-\top} \overrightarrow{s}$. By (8) this is same as $(\boldsymbol{V}^\top \boldsymbol{V})^{-1} \cdot m \cdot \boldsymbol{B}(\mathcal{I}_1 + \mathcal{I}_2)^{-\top} \cdot d \cdot (\boldsymbol{M'DL})^{-\top} \overrightarrow{s}$, which by the above $\mathbb{Z}$-basis of $(\mathcal{I}_1 + \mathcal{I}_2)^\vee$ is in $m(\mathcal{I}_1 + \mathcal{I}_2)^\vee$. Thus, the induced map ϕ is an invertible and surjective $\mathbb{Z}$-module homomorphism, that is also efficiently invertible, thus proving (ii).

Now, we move on to prove (iii). Let $\mathbf{z} \in \mathcal{I}_1 + \mathcal{I}_2$ and $\mathbf{x} \in m(\mathcal{I}_1 + \mathcal{I}_2)^\vee$. Write $\mathbf{z} = \mathbf{z}_1 + \mathbf{z}_2$, with $\mathbf{z}_1 \in \mathcal{I}_1$ and $\mathbf{z}_2 \in \mathcal{I}_2$. Now, note that $(\mathcal{I}_1 + \mathcal{I}_2)^\vee = \mathcal{I}_1^\vee \cap \mathcal{I}_2^\vee$. Thus, by lemmas 2.12 and 2.14, $\mathbf{z} * \mathbf{x} = \mathbf{z}_1 * \mathbf{x} + \mathbf{z}_2 * \mathbf{x} \subset m\mathcal{O}_1^\vee + m\mathcal{O}_2^\vee \subset \mathcal{O}_{\mathbf{K}}^\vee$. Thus,

$$\psi(\mathbf{z}) * \phi(\mathbf{x}) \;=\; u \cdot d \cdot \mathbf{z} * \mathbf{x} \;=\; \mathbf{z} * \mathbf{x} \bmod q\mathcal{O}_{\mathbf{K}}^\vee.$$

D Non-bigenic, non-transferable, non-diagonal Ideal

Proposition 6.1 (repeated) The ideal $\mathcal{I} = (8X, 2X^2 + 2, 4X^3 - 4X)$ of order $\mathcal{O}$ above has the following properties

(i) $\mathcal{I}$ is not bigenic,

(ii) no rational scaling of $\mathcal{I}$ is a bigenic ideal of $\mathcal{O}$,

(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.

(v) $\mathcal{I}$ is not contained in the conductor ideal of $\mathcal{O}$.

(vi) $2\mathcal{I}$ is product of two bigenic ideals, namely $2\mathcal{I} = (2, 4X^3) \cdot (8X, 2X^2 + 2)$, whereas $2\mathcal{I}$ is not bigenic.

(vii) $\mathcal{I}$ is not invertible as a fractional ideal of $\mathcal{O}$.

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

Now, assume to the contrary that this ideal is bigenic and generated by $L0 = (\ell_1, \ell_2)$, and as ideals of $\mathcal{O}$, $L0 = \mathcal{I}$. Both ℓ_1 and ℓ_2 must be in the $\mathbb{Z}$-span of $\mathbb{Z}$-basis of the ideal $\mathcal{I}$, which is computed by concatenating the circulant matrices of $4X^3 - 4X$, $2X^2 + 2$, $8X$ (multiplied on the right by the above given $\mathbb{Z}$-basis of $\mathcal{O}$). We also compute its Hermite normal form (HNF) which is as depicted below[11].

$$\begin{pmatrix} 8 & 0 & 2 & 0 \\ 0 & 8 & 0 & 4 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 \end{pmatrix}$$

From the HNF it is clear that ℓ_1 can be written as $4 * b_1 * (X^3 + X) + 2 * c_1 * (X^2 + 1) + 8 * d_1 * X + 8 * e_1$ and similarly, ℓ_2 can be written as $4 * b_2 * (X^3 + X) + 2 * c_2 * (X^2 + 1) + 8 * d_2 * X + 8 * e_2$, where all of $b_1, ..., e_1, b_2, ..., e_2$ are in $\mathbb{Z}$.

Now, note that while polynomial multiplications are to be considered modulo X^4+1, given the definition of $\mathcal{O}$, the monomial X^4 appearing in any ($\mathcal{O}$) element of $\mathcal{I}$ (before reduction modulo X^4+1) must have a coefficient a multiple of $2*2$, and further any monomial of degree six or more must have a coefficient multiple of $4*4$. Thus, it suffices to prove that the ideal of the ring $\mathbb{Z} + 4X\mathbb{Z} + 2X^2\mathbb{Z} + 4X^3\mathbb{Z}[X]$ generated by $(\ell_1, \ell_2, 4X^4 + 4, 4X^5 + 4X)$ does not contain all three of $8X$, $2X^2 + 2$ and $4X^3 + 4X$. As additive semigroups, we have

$$\begin{aligned}
&\ell_1 \cdot (\mathbb{Z} \ + \ 4X\mathbb{Z} \ + \ 2X^2\mathbb{Z} + 4X^3\mathbb{Z}[X]) \ + \ \ell_2 \cdot (\mathbb{Z} \ + \ 4X\mathbb{Z} \ + \ 2X^2\mathbb{Z} + 4X^3\mathbb{Z}[X]) \\
&\quad + \ (4X^4 + 4) \cdot \mathbb{Z} \ + \ (4X^5 + 4X) \cdot \mathbb{Z} \ + \ 16 \cdot \mathbb{Z}[X] \\
&\subseteq (4 * b_1 * (X^3 + X) + 2 * c_1 * (X^2 + 1) + 8 * d_1 * X + 8 * e_1) \cdot (\mathbb{Z} \ + \ 4X\mathbb{Z} \ + \ 2X^2\mathbb{Z} + 4X^3\mathbb{Z}[X]) \\
&\quad + \ (2 * c_2 * (X^2 + 1) + 8 * d_2 * X + 8 * e_2) \cdot (\mathbb{Z} \ + \ 4X\mathbb{Z} \ + \ 2X^2\mathbb{Z} + 4X^3\mathbb{Z}[X]) \\
&\quad + \ (4X^4 + 4) \cdot \mathbb{Z} \ + \ (4X^5 + 4X) \cdot \mathbb{Z} \ + \ 16 \cdot \mathbb{Z}[X] \\
&\subseteq (8 * b_1 * (-X + X^3) + 4 * c_1 * (X^2 - 1)) \cdot \mathbb{Z} + 8 * c_1 * (X^3 + X) \cdot \mathbb{Z} + 8 * c_1 * (X^3 - X) \cdot \mathbb{Z} \\
&\quad + \ (4 * b_1 * (X^3 + X) + 2 * c_1 * (X^2 + 1) + 8 * d_1 * X + 8 * e_1) \cdot \mathbb{Z} \\
&\quad + \ 4 * c_2 * (X^2 - 1) \cdot \mathbb{Z} \ + \ 8 * c_2 * (X^3 + X) \cdot \mathbb{Z} \ + \ 8 * c_2 * (X^3 - x) \cdot \mathbb{Z} \\
&\quad + \ (2 * c_2 * (X^2 + 1) + 8 * d_2 * X + 8 * e_2) \cdot \mathbb{Z} \\
&\quad + \ (4X^4 + 4) \cdot \mathbb{Z} \ + \ (4X^5 + 4X) \cdot \mathbb{Z} \ + \ 16 \cdot \mathbb{Z}[X]
\end{aligned}$$

$$\begin{aligned}
&\subseteq (8 * b_1 * (-X + X^3) + 4 * c_1 * (X^2 - 1)) \cdot \mathbb{Z} + 8 * c_1 * (X^3 + X) \cdot \mathbb{Z} \\
&\quad + \ (4 * b_1 * (X^3 + X) + 2 * c_1 * (X^2 + 1) + 8 * d_1 * X + 8 * e_1) \cdot \mathbb{Z} \\
&\quad + \ 4 * c_2 * (X^2 - 1) \cdot \mathbb{Z} \ + \ 8 * c_2 * (X^3 + X) \cdot \mathbb{Z} \ + \ (2 * c_2 * (X^2 + 1) + 8 * d_2 * X + 8 * e_2) \cdot \mathbb{Z} \\
&\quad + \ (4X^4 + 4) \cdot \mathbb{Z} \ + \ (4X^5 + 4X) \cdot \mathbb{Z} \ + \ 16 \cdot \mathbb{Z}[X]
\end{aligned}$$

Now, note that w.l.o.g. each of d_1, e_1, d_2, e_2 can be taken to be either zero or one. Moreover, to obtain $4(X^3 + X)$ that is in $\mathcal{I}$, b_1 must be 1 (modulo 2). Similarly,

[11] This has/can been computed by hand, but has also been confirmed by a number theory software.

to obtain $2(X^2+1)$, c_2 must be 1 (modulo 2). Then, because of the presence of the term $8*c_2*(X^3+X)\cdot\mathbb{Z}$, and hence also $8*c_2*(X^3-X)\cdot\mathbb{Z}$, we can ignore $8*c_1*(X^3+X)\cdot\mathbb{Z}$ term, as well as remove $8*b_1*(-X+X^3)$ from the first term. Similarly, because of the presence of the term $4*c_2*(X^2-1)\cdot\mathbb{Z}$, we can also ignore $4*c_1*(X^2-1)$ from the first term. Thus, the above simplifies to

$$\begin{aligned}&(4*(X^3+X)+2*c_1*(X^2+1)+8*d_1*X+8*e_1)\cdot\mathbb{Z}\\ &+\ 4*(X^2-1)\cdot\mathbb{Z}\ +\ 8*(X^3+X)\cdot\mathbb{Z}\ +\ (2*(X^2+1)+8*d_2*X+8*e_2)\cdot\mathbb{Z}\\ &+\ (4X^4+4)\cdot\mathbb{Z}\ +\ (4X^5+4X)\cdot\mathbb{Z}\ +\ 16\cdot\mathbb{Z}[X]\end{aligned}$$

Now, even c_1 can be w.l.o.g. assumed to be zero or one, and further, $\mathbb{Z}$ can be limited to be just $\mathbb{Z}/2\mathbb{Z}$. Now introduce new independent variables y_3 (for (X^3+X)), y_2 (for (X^2+1)), y_1 (for X), and we need to prove that $4y_3$, $2y_2$, $8y_1$ cannot all be in the semigroup

$$\begin{aligned}&8\cdot\mathbb{Z}/2\mathbb{Z}\ +\ 8*y_3\cdot\mathbb{Z}/2\mathbb{Z}\ +\ (4*y_3+2*c_1*y_2+8*d_1*y_1+8*e_1)\cdot\mathbb{Z}/2\mathbb{Z}\\ &+(2*y_2+8*d_2*y_1+8*e_2)\cdot\mathbb{Z}/2\mathbb{Z}\end{aligned}$$

Now to generate $2y_2$, we can only use the last term (keeping it non-zero), which implies that $d_2=e_2=0$. Further, to generate $4y_3$, we must use the term $(4*y_3+2*c_1*y_2+8*d_1*y_1+8*e_1)$, which implies that $d_1=e_1=0$ (since $d_2,e_2=0$). But, then $8y_1$ cannot be generated. 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 $8X$, any rational scaling of $\mathcal{I}$ that keeps it as a subset of $\mathcal{O}$ 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 $\mathcal{O}_{\mathbf{K}}$. Now, X is in $\mathcal{O}_{\mathbf{K}}$. but $(2X^2+2)\cdot X=(2X^3+2X)$ is not in $\mathcal{I}$, and hence $\mathcal{I}$ is not closed under multiplication by $\mathcal{O}_{\mathbf{K}}$.

Next, consider the set $\frac{p}{q}\cdot\mathcal{I}$, for co-prime integers p,q. From the $\mathbb{Z}$-basis of the ideal $\mathcal{I}$ above, then $\frac{8p*X}{q}$, $\frac{2p*(X^2+1)}{q}$, $\frac{4*p*(X^3+X)}{q}$ form a $\mathbb{Z}$-basis of $\frac{p}{q}\cdot\mathcal{I}$. However, $\frac{2p*(X^2+1)}{q}*X=\frac{2p*(X^3+X)}{q}$ is not in the $\mathbb{Z}$-span of the above basis, and hence this does not form a fractional ideal of $\mathcal{O}_{\mathbf{K}}$.

Item (v) is easy to see as the conductor ideal has all terms a multiple of four.

To prove the item (vi), note that $(2,4X^3)\cdot(8X,2X^2+2)=(16X,4X^2+4,-32,8X^3-8X)$. But, $(4X^2+4)*(2X^2-2)=2*(4X^4-4)=8X^4-8=-16$. Thus, 16 is in the ideal, and further $8X^3-8X+16X$ is also in the ideal, and hence $(2,4X^3)\cdot(8X,2X^2+2)=2\mathcal{I}$. Further, it is easy to see that if $2\mathcal{I}$ were to be bigenic it would imply that $\mathcal{I}$ itself is bigenic, which contradicts (i).

Finally, (vii) follows from lemma D.2 below.

Lemma D.1. *If an ideal $\mathfrak{a}$ of order $\mathcal{O}$ is co-prime to the conductor ideal $\mathfrak{c}_{\mathcal{O}}$ of $\mathcal{O}$, then ffraka is bigenic.*

Proof. We have that $\mathfrak{a} + \mathfrak{c}_{\mathcal{O}} = \mathcal{O}$. Thus there exists $\alpha \in \mathfrak{a}$ and $\gamma \in \mathfrak{c}_{\mathcal{O}}$ such that $\alpha + \gamma = 1$. Thus, $\alpha \cdot \mathcal{O} + \gamma \cdot \mathcal{O} = \mathcal{O}$. Since $\gamma \cdot \mathcal{O} \subset \mathfrak{c}_{\mathcal{O}} \subset \mathcal{O}$, we have that $\alpha \cdot \mathcal{O} + \mathfrak{c}_{\mathcal{O}} = \mathcal{O}$. Thus, the principal ideal $\alpha \cdot \mathcal{O}$ is co-prime to the conductor ideal. Hence, by [Cona, Corollary 3.11], $alpha \cdot \mathcal{O}$ has a unique factorization into prime ideals, and similarly, $\mathfrak{a}$ itself has a unique factorization into prime ideals, with the former containing prime factors in addition to the prime factors of the latter. Then by a usual argument, similar to that for Dedekind domains, it follows that there is a $\beta \in \mathfrak{a}$, such that $(\alpha, \beta) = \mathfrak{a}$.

Lemma D.2. *If an ideal $\mathfrak{a}$ of an order $\mathcal{O}$ is not bigenic then it is non-invertible.*

Proof. Suppose to the contrary that $\mathfrak{a}$ is invertible. Then, it is in some ideal-class of $\mathcal{O}$, and by [Cona, Theorem 5.2] this ideal-class has a representative that is co-prime to the conductor ideal $\mathfrak{c}_{\mathcal{O}}$. Thus, by lemma D.1 this representative is bigenic, say generated by (β_1, β_2). Since $\mathfrak{a}$ and this ideal are in the same ideal-class, we have that $(\alpha) \cdot \mathfrak{a} = (\gamma) \cdot (\beta_1, \beta_2)$, for some $\alpha, \gamma \in \mathcal{O}$. Since, $\mathcal{O}$ is Noetherian, let $\mathfrak{a} = (a_1, a_2, ..., a_r)$. We have that $(\alpha a_1, \alpha a_2, ..., \alpha a_r) = (\gamma\beta_1, \gamma\beta_2)$. Moreover, it is the case that both $\gamma\beta_1$ and
$gammabeta_2$ are in the principal ideal (α). So, let $\gamma\beta_1 = \alpha\delta_1$, and $\gamma\beta_2 = \alpha\delta_2$, for some $\delta_1, \delta_2 \in \mathcal{O}$. Thus, we have $(\alpha a_1, \alpha a_2, ..., \alpha a_r) = (\alpha\delta_1, \alpha\delta_2)$, or $(a_1, a_2, ..., a_r) = (\delta_1, \delta_2)$, which contradicts the fact that $\mathfrak{a}$ is not bigenic.

General Power of Two Cyclotomics Let $\boldsymbol{L} = \mathbb{Q}[X]/(X^n + 1)$ be a power-of-two cyclotomic number field, i.e. n is a power of two. As is well known, the ring of integers $\mathcal{O}_{\boldsymbol{L}}$ of $\boldsymbol{L}$ is same as $\mathbb{Z}[X]/(X^n + 1)$ (see Appendix F). Let $n >= 4$. Then, it is well known that $\boldsymbol{L}$ can be viewed as a degree $n/4$ extension field of $\mathbf{K} = \mathbb{Q}[X]/(X^4 + 1)$, namely by the isomorphism $\boldsymbol{L} = \mathbf{K}[Y]/(Y^{n/4} - X)$ – this is so because $Y^{n/4} - X$ is an Eisenstein polynomial over $\mathbf{K}$, which follows from the fact that X is not in the square of any prime ideal of $\mathcal{O}_{\mathbf{K}}$. Further, it can be shown that the ring of integers $\mathcal{O}_{\boldsymbol{L}}$ of $\boldsymbol{L}$ is same as $\mathcal{O}_{\mathbf{K}}[Y]$ with $Y^{n/4} = X$ (see e.g. [FT91, Theorem 24]). Now, mimicking the order $\mathcal{O}$ of $\mathbf{K}$, consider the following ring $\mathcal{O}^*$ with unity with the following $\mathbb{Z}$-basis:

$$\begin{aligned}&(1, 2Y, 2Y^2, ..., 2Y^{n/4-1}, 4X, 4XY, 4XY^2, ..., 4XY^{n/4-1},\\ &2X^2, 2X^2Y, 2X^2Y^2, ..., 2X^2Y^{n/4-1}, 4X^3, 4X^3Y, 4X^3Y^2, ..., 4X^3Y^{n/4-1})\end{aligned}$$

It can be checked that the above forms a ring with $X^4 = -1$ and $Y^{n/4} = X$, and further that its fraction field is just $\boldsymbol{L}$. Thus, $\mathcal{O}^*$ is an order in $\boldsymbol{L}$. Now, consider the ideal $\mathcal{I}$ of $\mathcal{O}^*$ generated by $(16X, 4X^2 + 4, 8X^3 - 8X)$. It continues to enjoy all the properties of Proposition 6.1.

E Introduction to Dedekind Domains

A **Dedekind domain** is a non-trivial integral domain in which every non-zero fractional ideal is invertible. An ideal is called proper if it not same as (0) or

(1). A major theorem of Dedekind domain states that every proper ideal of a Dedekind domain can be uniquely (upto re-ordering) factored as a product of proper prime ideals (see e.g. [FT91] or [Cla84]). Further, every proper prime ideal is a maximal ideal.

Let R be a subring of a ring R'. An element $x \in R'$ is said to be **integral** over R if it satisfies a monic polynomial equation, where the polynomial has coefficients in R. The **ring of integers**, denoted $\mathcal{O}_{\mathbf{K}}$ of a number field $\mathbf{K}$ are elements of $\mathbf{K}$ that are integral over $\mathbb{Z}$. It is well-known that the ring of integers $\mathcal{O}_{\mathbf{K}}$ of a number field is a Dedekind domain (see e.g. [FT91]).

For a prime number p, if an ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbf{K}}$ contains the ideal (p) (of $\mathcal{O}_{\mathbf{K}}$), we say that $\mathfrak{a}$ lies above p. Another well-known property of Dedekind domains is that every prime ideal of $\mathcal{O}_{\mathbf{K}}$ lies above some prime p. An alternative equivalent definition of Dedekind domain is that it is an integrally-closed Noetherian domain in which every nonzero prime ideal is maximal.

For any ideal $\mathfrak{a}$ of the Dedekind domain $\mathcal{O}_{\mathbf{K}}$, the (absolute) **norm** of $\mathfrak{a}$, $N(\mathfrak{a})$, is defined to be $[\mathcal{O}_{\mathbf{K}} : \mathfrak{a}]$, i.e. the cardinality of the residue class ring $\mathcal{O}_{\mathbf{K}}/\mathfrak{a}$. We state the following facts as a lemma (see any text on algebraic number theory for proofs, for instance [FT91])

Lemma E.1. (i) *Let $\mathfrak{p}$ denote a non-zero prime ideal of $\mathcal{O}_{\mathbf{K}}$ and let r be a positive integer. Then, we have an isomorphism of additive groups: $\mathcal{O}_{\mathbf{K}}/\mathfrak{p} \cong \mathfrak{p}^r/\mathfrak{p}^{r+1}$ (see II.1.16 of [FT91]).*

(ii) *For a prime ideal $\mathfrak{p}$, $N(\mathfrak{p}^r) = (N(\mathfrak{p}))^r$.*

(iii) *For any two non-zero ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_{\mathbf{K}}$, $N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$.*

(iv) *If $\mathfrak{a}$ is a prime ideal of $\mathcal{O}_{\mathbf{K}}$ lying above prime p, then $\mathcal{O}_{\mathbf{K}}/\mathfrak{a}$ is a field extension of finite field $\mathbb{Z}_p$ of some finite degree e. Further, $N(\mathfrak{a}) = p^e$. (see (II.1.37) of [FT91]).*

(v) *The norm of a principal ideal (a), $N((a))$, is same as the (absolute value of) field norm of a, i.e. $N_{\mathcal{O}_{\mathbf{K}}/\mathbb{Q}}(a)$. (see (II.1.38) of [FT91], and see section 2.4 for definition of field norm).*

(vi) *The discriminant of any monic irreducible polynomial $f(X)$, Δ_f, divides $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]^2$, where $\mathbf{K} = \mathbb{Q}[X]/(f(X))$ and $\mathcal{R} = \mathbb{Z}[X]/(f(X))$ (see (II.1.39) of [FT91]).*

(vii) *The norm of an ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbf{K}}$ is same as the (absolute value of) determinant of any $\mathbb{Z}$-basis of $\mathfrak{a}$. (see (II.1.39) of [FT91]).*

F Introduction to 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 F.1. *If $m = m_1 m_2$ 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 $\mathcal{O}_{\mathbf{K}}$ 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 [Conb]. 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 $\Delta_{\mathbf{K}}$ (as also the discriminant of the ring of integers, or the cyclotomic ring).

Theorem F.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 F.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[12] that a prime p divides $[\mathcal{O}_{\mathbf{K}} : \mathcal{R}]$ only if p^2 is a factor of $\Delta_{\Phi_m(X)}$. By corollary B.3 , 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

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

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 $\mathit{\Delta}_{f_1}\mathit{\Delta}_{f_2}$ 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, $\mathit{\Delta}_{\Phi_m(X)}$ 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 [Conb], 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 $\Phi_{p^r}(X)$.