



# Counting irreducible representations of the Heisenberg group over the integers of a quadratic number field

Shannon Ezzat

Cape Breton University, 1250 Grand Lake Road, Sydney, Nova Scotia, Canada

## ARTICLE INFO

### Article history:

Received 13 October 2010

Available online 8 October 2013

Communicated by Martin Liebeck

### Keywords:

Representation growth

Asymptotic group theory

Quadratic number fields

Nilpotent groups

## ABSTRACT

We calculate the representation zeta function of the Heisenberg group over the integers of a quadratic number field. In general, the representation zeta function of a finitely generated torsion-free nilpotent group enumerates equivalence classes of representations, called twist-isoclasses. This calculation is based on an explicit description of a representative from each twist-isoclass. Our method of construction involves studying the eigenspace structure of the elements of the image of the representation and then picking a suitable basis for the underlying vector space.

© 2013 Elsevier Inc. All rights reserved.

## 1. Introduction

Let  $G$  be a finitely generated torsion-free nilpotent group. Let  $\chi$  be a 1-dimensional complex representation and  $\rho$  an  $n$ -dimensional complex representation of  $G$ . We define the product  $\chi \otimes \rho$  to be a *twist* of  $\rho$ . Two representations  $\rho$  and  $\rho_*$  are *twist-equivalent* if, for some 1-dimensional representation  $\chi$ ,  $\chi \otimes \rho \cong \rho_*$ . This twist-equivalence is an equivalence relation on the set of irreducible representations of  $G$ . In [18] Lubotzky and Magid call the equivalence classes *twist-isoclasses*. They also show that there are only finitely many irreducible  $n$ -dimensional complex representations up to twisting and that for each  $n \in \mathbb{N}$  there is a finite quotient  $N$  of  $G$  such that each  $n$ -dimensional irreducible representation  $\rho$  of  $G$  is twist-equivalent to one that factors through  $N$ . Henceforth we call the complex representations of  $G$  simply representations. We denote the number of twist-isoclasses of irreducible representations of dimension  $n$  by  $r_n(G)$  or  $r_n$  if no confusion will arise.

Consider the formal Dirichlet series

$$\zeta_G(s) = \sum_{n=1}^{\infty} r_n(G)n^{-s}. \quad (1)$$

E-mail address: [bangteng.xu@eku.edu](mailto:bangteng.xu@eku.edu).

If  $G$  is a finitely generated torsion-free nilpotent group then by [22, Lemma 2.1],  $\zeta_G(s)$  converges on a right half plane of  $\mathbb{C}$ , say  $D$ , where  $D := \{s \in \mathbb{C} \mid \Re(s) > \alpha\}$  for some  $\alpha \in \mathbb{R}$ ; we call  $\zeta_G : D \rightarrow \mathbb{C}$  the representation zeta function of  $G$ . Note that in [23,16,22] this function is denoted  $\zeta_G^{\text{tr}}(s)$ . For a prime  $p$ , define

$$\zeta_{G,p}(s) := \sum_{n=0}^{\infty} r_{p^n}(G) p^{-ns}, \tag{2}$$

to be the  $p$ -local representation zeta function of  $\zeta_G(s)$ . Since  $G$  is nilpotent, each finite quotient decomposes as a direct product of its Sylow- $p$  subgroups. Since the irreducible representations of a direct product of finite groups are tensor products of irreducible representations of its factors, we have the Euler product  $\zeta_G(s) = \prod_p \zeta_{G,p}(s)$  [22, Introduction]. Moreover, it was shown by Hrushovski and Martin [13, Theorem 8.4] that each  $p$ -local representation zeta function is a rational function in  $p^{-s}$ .

The idea of using zeta functions to study the representation growth of groups is motivated by subgroup growth, where one uses zeta functions to count finite index subgroups. The study of subgroup growth of finitely generated nilpotent groups by zeta functions was introduced in [11]. In that paper, the authors calculate the normal subgroup zeta function of the Heisenberg group over the ring of integers of a number field of degree at most two [11, Prop. 8.2]. These zeta functions were given, in part, in terms of the Dedekind zeta function of the associated number field. Research on subgroup zeta functions of nilpotent groups continued in papers such as [9,10,8,23].

One can study the growth rate of the sequence  $r_n(G)$  without necessarily explicitly constructing the zeta function. We call this study *representation growth*. Representation growth has been used to study other classes of groups. We briefly mention some work done in this area. For the following groups,  $r_n(G)$  counts irreducible representations, as opposed to twist-isoclasses as with nilpotent groups. The idea of using zeta functions to study representation growth was introduced in [24], in which Witten studies compact Lie groups. Later, representation growth was studied for  $S$ -arithmetic groups by Lubotzky and Martin [19] and, using the language of representation zeta functions, Larsen and Lubotzky [17]. Jaikin, in [14], studies representation zeta functions of compact  $p$ -adic analytic groups with property FAB. In [4] Avni et al. study representation zeta functions of compact  $p$ -adic analytic and arithmetic groups; see also the research announcement [3]. In [2] they prove a conjecture of Larsen and Lubotzky (see [17, Conjecture 1.5]). In [1] Avni shows that arithmetic groups in characteristic zero which satisfy the congruence subgroup property have representation zeta functions with rational abscissa of convergence. Bartholdi and de la Harpe study representation zeta functions of wreath products with finite groups [5]. In [15], Kassabov and Nikolov study representation growth of some profinite groups. Craven gives lower bounds for representation growth for profinite and pro- $p$  groups [7].

Representation growth of finitely generated nilpotent groups has been studied in [23] by Voll and [22] by Stasinski and Voll. Very few examples of representation zeta functions of finitely generated nilpotent groups have appeared in the literature (see [22, Theorem B] and [13, Example 8.12]). Let

$$H(\mathbb{Z}) := \langle x, y, z \mid [x, y] = z, z \text{ is central} \rangle \tag{3}$$

and let  $\zeta(s)$  be the Riemann zeta function. Note that  $H(\mathbb{Z})$  is isomorphic to the group of  $3 \times 3$  upper-unitriangular matrices over the rational integers; this is normally called the discrete Heisenberg group. Then, by [13, Example 8.12],  $\zeta_{H(\mathbb{Z})}(s)$  is given by

$$\zeta_{H(\mathbb{Z})}(s) = \frac{\zeta(s-1)}{\zeta(s)} \tag{4}$$

(the coefficients  $r_{p^n}(H(\mathbb{Z}))$  were originally calculated in [21, Theorem 5]). This has a simpler shape than the corresponding normal subgroup zeta function in [20, Chapter 15].

Let  $d$  be a square-free integer and define  $O_d$  to be the ring of integers of the number field  $\mathbb{Q}(\sqrt{d})$ . We denote by  $H(O_d)$  the Heisenberg group over  $O_d$ , that is the group of  $3 \times 3$  upper unitriangular matrices over the ring  $O_d$ .

Let  $\zeta_K^{\mathbf{D}}$  be the Dedekind zeta function of a number field  $K$ . The main theorem of this paper is as follows:

**Theorem 1.1.** *The representation zeta function of  $H(O_d)$  is*

$$\zeta_{H(O_d)}(s) = \frac{\zeta_{\mathbb{Q}(\sqrt{d})}^{\mathbf{D}}(s-1)}{\zeta_{\mathbb{Q}(\sqrt{d})}^{\mathbf{D}}(s)}.$$

We remark that an analogous theorem holds for the Heisenberg group over the rational integers; that is, if  $\mathbb{Q}(\sqrt{d})$  is replaced by  $\mathbb{Q}$  (see Eq. (4)).

We can use this theorem to determine the abscissa of convergence of these representation zeta functions.

**Corollary 1.2.** *For any quadratic number field  $\mathbb{Q}(\sqrt{d})$  the abscissa of convergence of  $\zeta_{H(O_d)}(s)$  is 2.*

Let  $\mathbf{G}$  be a group scheme defined over the ring of integers  $O$  of a number field  $K$ . For  $O'$  a ring extension of  $O$ , denote the group of  $O'$ -points of  $\mathbf{G}$  by  $\mathbf{G}(O')$ . Groups of the form  $\mathbf{G}(O')$  give an important class of examples for representation growth. The papers [17,2,4,1] deal with semisimple  $\mathbf{G}$ , while [22] deals with unipotent  $\mathbf{G}$ , giving rise to finitely generated nilpotent groups  $\mathbf{G}(O)$ .

Suppose the group scheme  $\mathbf{G}$  is unipotent. Stasinski and Voll, in [22, Theorem A] and [22, Remark 2.3], show that the following Euler factorization holds:

$$\zeta_{\mathbf{G}(O)}(s) = \prod_P \zeta_{\mathbf{G}(O_P)}(s), \tag{5}$$

where  $P$  runs through the non-zero prime ideals of  $O$ ,  $\zeta_{\mathbf{G}(O_P)}(s)$  counts twist isoclasses of continuous representations of  $\mathbf{G}(O_P)$ , and  $O_P$  is the completion of  $O$  at  $P$ . For the group scheme associated to a nilpotent Lie lattice the authors also show that, for almost all prime ideals of  $O$ , there is one rational “template” for the local factors which, for any finite extension of the local ring  $O_P$ , say  $O'_P$ , gives all  $\zeta_{\mathbf{G}(O'_P)}(s)$ . Furthermore, it can be shown that these local zeta functions are rational in  $q^{-fs}$ , where  $q$  is the residue field cardinality of  $O_P$  and  $f = f(O'_P, O_P)$  is the relative degree of inertia. We direct the reader to [22] for a precise statement of these results.

Theorem A of [22] also tells us that, for almost all  $P$ , the local representation zeta functions  $\zeta_{\mathbf{G}(O'_P)}(s)$  satisfy a functional equation (which is a refinement of [23, Theorem D]) and, additionally, that these local zeta functions are rational functions in  $q^{-fs}$ . Moreover, in [22, Theorem B] the authors calculate all of the  $P$ -local representation zeta functions of three families of groups arising from unipotent group schemes; indeed, the representation zeta function of  $H(O_d)$ , Theorem 1.1 in our paper, appears as a special case of their result (note that we can identify  $H(O)$  with the group of  $O$ -points of a unipotent group scheme  $H$  defined over  $\mathbb{Z}$ ).

As a special case of [22, Theorem B], Stasinski and Voll prove the following result, which generalizes Theorem 1.1.

**Theorem 1.3.** *Let  $K$  be an arbitrary algebraic number field and  $O$  its ring of integers. Then*

$$\zeta_{H(O)}(s) = \frac{\zeta_K^{\mathbf{D}}(s-1)}{\zeta_K^{\mathbf{D}}(s)}.$$

We remark that [Theorem 1.3](#) was stated as a conjecture in an earlier version of the present paper, before the appearance of [\[22\]](#).

When the group scheme  $\mathbf{G}$ , defined over the number field  $K$ , is semisimple there are some similar results to the unipotent case discussed above. As in the unipotent case, Larsen and Lubotzky [\[17, Proposition 1.3\]](#) showed that, for semisimple arithmetic groups satisfying the congruence subgroup property, there is a decomposition of representation zeta functions into local factors (with extra factors coming from the archimedean completions of  $K$ ). Work by Avni et al. [\[3, Theorem A\]](#), [\[4, Theorem A\]](#), has proven that the representation zeta functions of a certain class of compact  $p$ -adic analytic groups related to  $\mathbf{G}$  also behave uniformly under extension of scalars.

From now on we restrict our attention to finitely generated torsion-free nilpotent groups. In the paper [\[23\]](#), Voll uses the Kirillov orbit method, as established by Howe [\[12\]](#), to compute  $p$ -local representation zeta functions. One counts twist-isoclasses of a finitely generated torsion-free nilpotent group  $G$  by counting the coadjoint orbits of the Lie ring associated to  $G$ . However, this Kirillov orbit method has the restriction that in general it excludes a finite number of primes. We note that both the Kirillov orbit method and the techniques of the present paper reduce to counting solutions to polynomial equations, although in the Kirillov orbit method this counting is disguised in the machinery of Igusa local zeta functions.

Our techniques are quite general. They could, in principle, be used to calculate all  $p$ -local representation zeta functions, and therefore the global representation zeta function, of any finitely generated torsion-free nilpotent group. However, in practice this may not be feasible—as the complexity of the eigenspace structure of the irreducible representations increases, the complexity of the calculation would increase quite quickly. Note that we rely on less mathematical machinery than the Kirillov orbit method and thus can be appreciated with minimal technical background; moreover, it explicitly gives all of the irreducible representations. The technically deeper approach in [\[23\]](#) and [\[22\]](#) allows for easier computations in many cases since one counts characters without constructing the representations explicitly.

The techniques used in [\[23\]](#) and [\[22\]](#) are not valid for all primes for an arbitrary nilpotent group. It is worth noting, however, that [\[22, Section 2.4\]](#) introduces a method for class-2 finitely generated nilpotent groups obtained from unipotent group schemes, including the groups we study, that is valid for all primes. The constructive method we introduce differs from this approach. The author will use it to calculate the full global representation zeta functions of the groups  $M_n := \langle y, x_1, \dots, x_n \mid [y, x_i] = x_{i+1}, i = 1, \dots, n - 1 \rangle, n \in \{3, 4\}$  of nilpotency class  $n$  in a forthcoming paper.

In [\[23\]](#) it was discovered that representation zeta functions satisfy the following functional equation:

**Theorem 1.4.** (See [\[23, Theorem D\]](#).) *Let  $G$  be a finitely generated torsion-free nilpotent group with derived subgroup  $G'$  with Hirsch length  $d'$ . Then, for almost all primes,*

$$\zeta_{G,p}(s) \Big|_{p \rightarrow p-1} = p^{d'} \zeta_{G,p}(s). \tag{6}$$

This functional equation has been strengthened and refined, as previously mentioned, by Stasinski and Voll in [\[22, Theorem A\]](#). Indeed, they give a functional equation that applies to  $\zeta_{H(O_d),p}(s)$ , for all  $p$ , in [\[22, Corollary 1.3\]](#). We note that  $\zeta_{H(O_d),p}(s)$  does indeed satisfy the functional equation of [Theorem 1.4](#) if  $p$  is not ramified.

Let  $p$  be a rational prime and write  $p = \prod_{P|(p)} P^{e_P}$ , where  $P$  is a prime ideal of  $O_d$  and  $e_P$  is the ramification index of  $P$ . We call  $\prod_{P|(p)} \zeta_{\mathbb{Q}(\sqrt{d}),P}^{\mathbf{D}}$  the  $p$ -local Dedekind zeta function. It is easy to see that the Euler product of the  $p$ -local representation zeta functions of  $H(O_d)$  can be refined to an Euler product of  $P$ -local Dedekind zeta functions by factorization; that is,

$$\zeta_{H(O_d),p}(s) = \prod_{P|(p)} \frac{\zeta_{\mathbb{Q}(\sqrt{d}),P}^{\mathbf{D}}(s-1)}{\zeta_{\mathbb{Q}(\sqrt{d}),P}^{\mathbf{D}}(s)}. \tag{7}$$

The functional equation in [22, Corollary 1.3] can be obtained by a short computation of the functional equations satisfied by the  $P$ -local Dedekind zeta functions.

The structure of the paper is as follows. Section 2 introduces some definitions and notation. Section 3 contains the proof of the main theorem which is separated into three parts: studying eigenspace behaviour, picking a suitable basis, and counting the numbers of twist-isoclasses, respectively.

## 2. Preliminaries

We remind the reader of some standard concepts in algebraic number theory. For more details see, for example, [6, Section 10.5].

**Definition 2.1.** Let  $K$  be an algebraic number field and  $O_K$  its ring of integers. Then  $\zeta_K^{\mathbf{D}}(s) = \sum_{I \subseteq O_K} (N_{K/\mathbb{Q}}(I))^{-s}$  is the *Dedekind zeta function* of  $K$  where  $I$  runs through the non-zero ideals of  $O_K$  and  $N_{K/\mathbb{Q}}(I)$  is the norm of  $I$  with respect to  $\mathbb{Q}$ .

The zeta function  $\zeta_K^{\mathbf{D}}(s)$  has an Euler product decomposition

$$\zeta_K^{\mathbf{D}}(s) = \prod_{P \subseteq O_K} \frac{1}{1 - (N_{K/\mathbb{Q}}(P))^{-s}},$$

where  $P$  runs over all non-zero prime ideals of  $O_K$ . This decomposition reflects the unique factorization of ideals of  $O_K$ .

We recall another standard definition [6, Section 3.3].

**Definition 2.2.** Let  $p$  be a rational prime, and consider the ideal  $(p) \triangleleft O_d$ . If  $(p)$  is prime then  $p$  is *inert*. If  $(p)$  is the product of two distinct prime ideals then  $p$  *splits*. If  $(p)$  is the square of a prime ideal then  $p$  is *ramified*.

This definition is equivalent to the equation  $x^2 - \Delta \equiv 0 \pmod{p}$  having 0, 2, or 1 solution, respectively and where  $\Delta$  is the discriminant of  $\mathbb{Q}(\sqrt{d})$ . We note that  $\Delta = 4d$  if  $d \equiv 2, 3 \pmod{4}$  and  $\Delta = d$  if  $d \equiv 1 \pmod{4}$ . We also note that there are only a finite number of ramified primes and a prime  $p$  is ramified if and only if it divides the discriminant of the number field.

The following is a well known result.

**Proposition 2.3.** Let  $p$  be a prime and  $\mathbb{Q}(\sqrt{d})$  be a quadratic number field. Then the  $p$ -local Dedekind zeta function of  $\mathbb{Q}(\sqrt{d})$  is

$$\zeta_{\mathbb{Q}(\sqrt{d}),p}^{\mathbf{D}}(s) = \begin{cases} \frac{1}{1-p^{-2s}} & \text{if } p \text{ is inert,} \\ \left(\frac{1}{1-p^{-s}}\right)^2 & \text{if } p \text{ splits,} \\ \frac{1}{1-p^{-s}} & \text{if } p \text{ is ramified.} \end{cases} \tag{8}$$

To aid our study of the representation zeta function of  $H(O_d)$  we choose an appropriate presentation. It is easily seen that the following six matrices generate  $H(O_d)$ :

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad x_d = \begin{pmatrix} 1 & D & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$y = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad y_d = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & D \\ 0 & 0 & 1 \end{pmatrix},$$

$$z = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad z_d = \begin{pmatrix} 1 & 0 & D \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

where  $D = \sqrt{d}$  if  $d \equiv 2, 3 \pmod{4}$  and  $D = \frac{1+\sqrt{d}}{2}$  if  $d \equiv 1 \pmod{4}$ . Note that  $(1, D)$  is a  $\mathbb{Z}$ -basis for  $O_d$ .

It can be shown that a presentation for this group is given by

$$\langle x, x_d, y, y_d, z, z_d \mid [x, y] = z, [x, y_d] = [x_d, y] = z_d, [x_d, y_d] = z^d \rangle$$

if  $d \equiv 2, 3 \pmod{4}$  and

$$\langle x, x_d, y, y_d, z, z_d \mid [x, y] = z, [x, y_d] = [x_d, y] = z_d, [x_d, y_d] = z^{\frac{d-1}{4}} z_d \rangle$$

if  $d \equiv 1 \pmod{4}$ . By convention, commutators that cannot be deduced from the relations that appear are trivial.

Before we prove the main result of the paper, we tabulate the notation used herein for easy reference:

$H(O_d)$	the Heisenberg group over the integers of $\mathbb{Q}(\sqrt{d})$
$d$	a square-free integer
$D_l$	$d$ if $d \equiv 2, 3 \pmod{4}$ ; $l + \frac{d-1}{4}$ if $d \equiv 1 \pmod{4}$
$\langle a_1, \dots, a_k \rangle$	the group generated by $a_1, \dots, a_k$
$\phi$	the Euler phi function
$(M)_{i,j}$	the $(i, j)$ th entry of matrix $M$
$G \cdot x$	the orbit of $x$ under the action of a group $G$
$[a, b]$	the commutator of group elements $a$ and $b$ , that is, $aba^{-1}b^{-1}$

In this paper, matrix entries that are blank are assumed to be 0.

### 3. Proof of Theorem 1.1

#### 3.1. Studying eigenspaces

We begin the proof of the main theorem by studying the twists of some irreducible representation  $\rho : H(O_d) \rightarrow \text{GL}_p^n(\mathbb{C})$ .

**Definition 3.1.** A twist-isoclass is of dimension  $n \in \mathbb{N}$  if the representations in the twist-isoclass are of dimension  $n$ .

We note that this is not to be confused with the dimension of a twist-isoclass as a subvariety (see [18] for details).

It is easy to show that there is only 1 twist-isoclass of dimension 1: that is,  $r_1 = 1$ , where  $r_1$  is the first coefficient in  $\zeta_{H(O_d)}(s)$ .

**Lemma 3.2.** Let  $\rho : H(O_d) \rightarrow \text{GL}_n(\mathbb{C})$  be an irreducible representation and let  $J = \{x, y, x_d, y_d\}$ . Then there exists a representation  $\chi : H(O_d) \rightarrow \text{GL}_1(\mathbb{C})$  such that for each  $j \in J$  we have that 1 is an eigenvalue of  $\chi \otimes \rho(j)$ .

**Proof.** Let  $\rho : H(O_d) \rightarrow \text{GL}_n(\mathbb{C})$  be an irreducible representation and for each  $j \in J$  let  $\lambda_j$  be an eigenvalue of  $\rho(j)$ . We can twist any irreducible representation by any 1-dimensional representation and remain in the same twist-isoclass. We deduce that we can choose a 1-dimensional representation  $\chi$  such that  $\chi(j) = (\lambda_j)^{-1}$ .  $\square$

We call a representation *good* if 1 is an eigenvalue of all of the non-central images of the generators.

We will show that the images of the generators of any irreducible representation of  $H(O_d)$ , up to twisting, can be written as matrices in a certain canonical form and that any set of matrices satisfying this form is, in fact, isomorphic to the images of the generators for some irreducible representation of  $H(O_d)$ . Finally, if two irreducible representations are not twist-equivalent, their associated canonical forms differ.

Let  $p$  be a prime,  $n \geq 1$ , and  $\rho : H(O_d) \rightarrow GL_{p^n}(\mathbb{C})$  be a good irreducible representation. Let

$$\begin{aligned} A &:= \rho(x), & A_d &:= \rho(x_d), \\ B &:= \rho(y), & B_d &:= \rho(y_d), \\ \Lambda &:= \rho(z), & \Lambda_d &:= \rho(z_d). \end{aligned}$$

Our aim in the first two sections is to choose a basis for  $\mathbb{C}^{p^n}$  such that the images of our generators in  $GL_{p^n}(\mathbb{C})$  are in a “nice” form. This basis will be chosen so that  $A$  and  $A_d$  are diagonal matrices,  $B$  and  $B_d$  are block permutation matrices, and  $\Lambda$  and  $\Lambda_d$  are scalar matrices. To avoid extra notation, for the rest of the paper we do not distinguish between a linear operator and its matrix with respect to some basis. Also, we identify scalars with scalar matrices; in particular, for  $\lambda$  a root of unity, we will call the matrix  $\lambda I$  a root of unity as well.

Since  $z$  and  $z_d$  are central in  $H(O_d)$ , by Schur’s lemma we must have that  $\Lambda$  and  $\Lambda_d$  are homotheties. By [18, Theorem 6.6],  $\rho$ , up to twisting, factors through a finite quotient of  $H(O_d)$ , say  $\overline{H(O_d)}$ . Therefore, without loss of generality, the representation  $\rho$  is such that the images of elements of  $H(O_d)$  under  $\rho$  must have finite order. Hence, for every  $g \in \overline{H(O_d)}$  we have  $g^k = e$  for some minimal  $k$ . It then follows that  $\rho(g)^k = I$  and the minimum polynomial of  $\rho(g)$  is  $x^k - 1$ . Since the  $k$ th roots of unity are distinct, this polynomial factors over the complex numbers into  $k$  distinct linear factors. Thus  $A$ ,  $A_d$ ,  $B$ , and  $B_d$  must be diagonalizable and have eigenvalues which are roots of unity, and  $\Lambda$  and  $\Lambda_d$  must be roots of unity. It is important to note that twisting does not affect the diagonalizability of the images of the generators; twisting is simply multiplication by scalars. Also, since  $[A, A_d] = I$ ,  $A$  and  $A_d$  are simultaneously diagonalizable.

**Definition 3.3.** Let  $X, Y \in GL_{p^n}(\mathbb{C})$ . If  $[X, Y] = Z$  for some homothety  $Z \in GL_{p^n}(\mathbb{C})$  then we say  $X$  is *Z-arrangeable*, or simply *arrangeable*, under  $Y$ .

Denote by  $E_{X,\lambda}$  the eigenspace of the linear operator  $X$  with eigenvalue  $\lambda$ . If there will be no confusion we may omit  $X$ .

**Lemma 3.4.** Let  $X$  be *Z-arrangeable* under  $Y$ . Then  $YE_{X,\lambda} = E_{X,Z\lambda}$ .

**Proof.** Let  $\mathbf{v}$  be an eigenvector of  $X$  such that  $X\mathbf{v} = \lambda\mathbf{v}$ . Then

$$XY\mathbf{v} = ZYX\mathbf{v} = ZY\lambda\mathbf{v} = Z\lambda Y\mathbf{v}.$$

Therefore  $Y\mathbf{v}$  is also an eigenvector of  $X$  and  $YE_{X,\lambda} = E_{X,Z\lambda}$ . The converse is similar.  $\square$

**Lemma 3.5.** There are  $p^r$  eigenspaces of  $A$  each of dimension  $p^m$  for some  $r, m$  where  $r + m = n$ .

**Proof.** Since  $[A, B] = \Lambda$  and  $[A, B_d] = \Lambda_d$  we have that  $A$  is arrangeable under  $B$  and  $B_d$ . By Lemma 3.4,  $B$  and  $B_d$  must send an eigenspace of  $A$  of some dimension, say  $\gamma$ , to another eigenspace of dimension  $\gamma$ . Therefore the direct sum of all eigenspaces of dimension  $\gamma$  forms a stable subspace of  $\rho$ . Since  $\rho$  is irreducible by assumption, all eigenspaces of  $A$  must be of dimension  $\gamma$ . Lemma 3.4,

along with the assumption that  $\rho$  is good, lets us additionally conclude that the eigenvalues of  $A$  are powers of  $\Lambda$ .

Since  $A$  is diagonalizable,  $A$  has  $\omega$  distinct eigenvalues of multiplicity  $\gamma$  for some  $\omega$ . Since  $p^n = \omega\gamma$  this shows us that  $\omega$  and  $\gamma$  must be powers of  $p$ , say  $\omega = p^r$  for some  $r$  and  $\gamma = p^m$  for some  $m$ .  $\square$

We state a simplified version of [Lemma 3.5](#) without proof.

**Lemma 3.6.** *Let  $X, Y, Z \in GL_{p^r}(\mathbb{C})$ , where  $Z$  is a primitive  $p^r$ th root of unity, such that  $[X, Y] = Z$ . Then there are  $p^r$  distinct 1-dimensional eigenspaces of  $X$ .*

Let  $E_\lambda := E_{A,\lambda}$  and let  $E := \{E_\lambda \mid \lambda \text{ is an eigenvalue of } A\}$ .

**Lemma 3.7.** *Both  $\Lambda$  and  $\Lambda_d$  must be  $p^r$ th roots of unity, and at least one must be a primitive root.*

**Proof.** Let  $E_1$  be the eigenspace of  $A$  with eigenvalue 1. By [Lemma 3.4](#) and the group relations of  $H(O_d)$  we have that  $B \cdot E_1 = E_\Lambda$  and  $B_d \cdot E_1 = E_{\Lambda_d}$  with the other generators acting trivially on  $E_1$ . Since by [Lemma 3.5](#)  $A$  has  $p^r$  distinct eigenspaces, we have that  $|\langle B \rangle \cdot E_1| = p^k$  and  $|\langle B_d \rangle \cdot E_1| = p^{k_d}$  for some  $k, k_d \leq r$ . Thus  $\Lambda$  is a primitive  $p^k$ th root of unity and  $\Lambda_d$  is a primitive  $p^{k_d}$ th root of unity. Finally, since there are exactly  $p^r$  distinct eigenspaces of  $A$ , at least one of  $k, k_d$  must equal  $r$ .  $\square$

The proof of [Lemma 3.7](#) shows that, in fact, at least one of  $B$  and  $B_d$  permutes the eigenspaces of  $A$  transitively, depending on whether  $\Lambda$  or  $\Lambda_d$  are  $p^r$ th primitive roots of unity. To deal with both cases, we break the argument into two separate parts.

**Case 1.**  $\Lambda$  is a primitive  $p^r$ th root of unity.

Since  $\Lambda$  is primitive we can deduce that  $E = \{E_1, E_\Lambda, E_{\Lambda^2}, \dots, E_{\Lambda^{p^r-1}}\}$ . We know that  $B$  permutes  $E$  transitively and since  $\Lambda$  is primitive,  $B$  must correspond to a  $p^r$ -cycle permutation, say  $\sigma_B$ . This, together with the fact that  $B$  and  $B_d$  commute and that in  $S_n$  only powers of  $n$ -cycles commute with  $n$ -cycles, allows us to deduce that the permutation of  $E$  corresponding to  $B_d$ , say  $\sigma_{B_d}$ , is  $\sigma_B^l$  for some  $l$ . Therefore we have that

$$\Lambda_d = \Lambda^l \tag{9}$$

since  $B_d$  sends  $E_\lambda$  to  $E_{\Lambda^l \lambda}$  and  $[A, B_d] = \Lambda_d$ . Define  $D_l$  as  $d$  if  $d \equiv 2, 3 \pmod{4}$  and  $\frac{d-1}{4} + l$  if  $d \equiv 1 \pmod{4}$ . Then we can say that  $[A_d, B_d] = \Lambda^{D_l}$ .

**Lemma 3.8.** *The eigenvalues of  $B$  and  $B_d$  are  $p^r$ th roots of unity. Moreover,  $B$  has all  $p^r$ th roots of unity as eigenvalues.*

**Proof.** Since the commutator relation is antisymmetric we have that  $[B, A] = \Lambda^{-1}$ . Therefore  $B$  is  $\Lambda^{-1}$ -arrangeable under  $A$ . We recall that 1 is an eigenvalue of  $B$ . Since  $\Lambda$  is a primitive  $p^r$ th root of unity, we have, by [Lemma 3.4](#), that  $B$  has at least  $p^r$  distinct eigenspaces and all  $p^r$  roots of unity are eigenvalues of  $B$ . However, since  $B$  is  $\Lambda_d^{-1}$ -arrangeable under  $A_d$  and  $\Lambda_d$  is a  $p^r$ th root of unity then, by a similar argument to that of [Lemma 3.7](#), the  $\langle A, A_d \rangle$  orbit of the eigenspace of  $B$  with eigenvalue 1 will be a stable subspace of  $\mathbb{C}^{p^n}$ . But since  $\rho$  is irreducible, we have that this must be the entire space and so this action is transitive. So  $B$  has at most  $p^r$  distinct eigenspaces. The argument for  $B_d$ , using the appropriate commutator relations and without the condition that it has all  $p^r$ th roots of unity as eigenvectors, is similar.  $\square$



3.2. Picking a basis

We now choose a basis  $\Theta_1$  for  $E_1$  and construct the rest of the basis of  $\mathbb{C}^{p^n}$  in the following way. Define  $\Theta_{\Lambda^k} := B^k \cdot \Theta_1$  for  $1 \leq k \leq p^r - 1$  such that  $\Theta_{\Lambda^k}$  is a basis for  $E_{\Lambda^k}$ . Then we have a basis  $\Theta := \Theta_1 \cup \dots \cup \Theta_{\Lambda^{p^r-1}}$  for  $\mathbb{C}^{p^n}$  with respect to which  $A$  and  $A_d$  are diagonal. Since  $\rho$  is good, 1 is an eigenvalue of  $A$  and  $A_d$ . We can choose  $\Theta_1$  such that  $(A_d)_{1,1} = 1$ ,

$$A = \begin{pmatrix} I_{p^m} & & & & \\ & \Lambda I_{p^m} & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \Lambda^{p^r-1} I_{p^m} \end{pmatrix},$$

and

$$B = \begin{pmatrix} 0_{p^m} & & & P \\ I_{p^m} & \ddots & & \\ & \ddots & \ddots & \\ & & I_{p^m} & 0_{p^m} \end{pmatrix}$$

where  $I_{p^m}$  and  $0_{p^m}$  are, respectively, the identity and null matrices of size  $p^m$ , and for some matrix  $P$  of size  $p^m$ . However, by Lemma 3.8,  $B^{p^r} = I$ . This implies that  $P = I_{p^m}$ .

Since  $A$  is arrangeable under  $B_d$ , Lemmas 3.4 and 3.8 imply that  $B_d$  must be a generalized block permutation matrix with blocks of size  $p^m$ ; that is it has exactly one non-zero block in each block row and block column. Since  $[B, B_d] = I$  and  $\sigma_{B_d} = \sigma_B^l$  a simple computation shows that  $B_d$  is the block matrix

$$B_d = \begin{pmatrix} 0_{p^m} & & & R \\ & \ddots & & \\ & & \ddots & \\ R & & & R \\ & \ddots & & \\ & & R & \\ & & & \ddots & \\ & & & & 0_{p^m} \end{pmatrix} \tag{10}$$

for some matrix  $R$  of size  $p^m$  with respect to  $\Theta$ , and the  $R$  in the first block column is in the  $l$ th block row.

Since  $A_d$  is diagonal let

$$A_d = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_{p^r} \end{pmatrix}$$

for some diagonal matrices  $J_i$ ,  $1 \leq i \leq p^r$  of size  $p^m$ . Since  $[A_d, B] = \Lambda^l$ ,  $A_d$  is  $\Lambda^l$ -arrangeable under  $B$ . Therefore by Lemma 3.4 and for some matrix  $J$  of size  $p^m$ , we have that

$$A_d = \begin{pmatrix} J & & & \\ & \Lambda^l J & & \\ & & \ddots & \\ & & & \Lambda^{(p^r-1)l} J \end{pmatrix}.$$

A straightforward calculation using the relation  $[A_d, B_d] = \Lambda^{D_l}$  gives us the equation  $JR = \Lambda^{l^2-D_l} R J$ . Therefore  $J$  is  $(\Lambda^{l^2-D_l})$ -arrangeable under  $R$ . Let  $H$  be the Heisenberg group over the rational integers as defined in Eq. (3) and note that  $\langle J, R \rangle \cong H$ . The homomorphism  $x \mapsto J, y \mapsto R$  defines a representation of  $H$ .

Assume that  $S$  is a non-zero  $(J, R)$ -stable irreducible subspace of  $E_1$ , say, by Lemma 3.6, of dimension  $p^k$  where  $k < m$ . It is clear that  $\langle A \rangle \cdot S = S$  and since  $S$  is  $J$ -stable we have that  $\langle A_d \rangle \cdot S = S$ . It is also clear by Lemma 3.4 that  $\langle B \rangle \cdot S = \{S, BS, B^2S, \dots, B^{p^r-1}S\}$  where the  $B^i S$  are distinct. Since  $S$  is  $R$ -stable and  $\sigma_{B_d} = \sigma_B^l$  we have that  $B_d \cdot S = B^l \cdot S$  and therefore  $\langle B_d \rangle \cdot S \subseteq \langle B \rangle \cdot S$ . We also note that  $\langle A \rangle \cdot B^i S = \Lambda^i S = S$  and  $\langle A_d \rangle \cdot B^i S = \Lambda^{li} S = S$  for  $0 \leq i \leq p^r - 1$ . Therefore the size of the orbit  $H(O_d) \cdot S$  is  $p^r$  and the dimension of the subspace spanned by  $H(O_d) \cdot S$  is  $p^{r+k}$ . Since  $p^{r+k} < p^{r+m} = p^n$  we have that this is a proper stable subspace of  $\rho$ . But since  $\rho$  is irreducible this is a contradiction. This implies that the representation of the subgroup generated by  $\langle J, R \rangle$  on  $E_1$  has no stable subspaces and is therefore irreducible. Since this is a representation of  $H$ , by Nunley and Magid’s result on the irreducible representations of  $H$  [21, Theorem 5], we could have chosen  $\Theta_1$  at the start of this subsection so that

$$R = \begin{pmatrix} 0 & & & 1 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ & & & 1 & 0 \end{pmatrix} \tag{11}$$

and therefore

$$J = \begin{pmatrix} 1 & & & \\ & \Lambda^{l^2-D_l} & & \\ & & \ddots & \\ & & & \Lambda^{(p^m-1)(l^2-D_l)} \end{pmatrix}.$$

By [21, Theorem 5] we can now deduce that

$$\Lambda^{l^2-D_l} \text{ is a primitive } p^m \text{th root of unity.} \tag{12}$$

**Lemma 3.9.**  $r \geq m$ .

**Proof.** By Eq. (10) we have that

$$B_d^{p^r} = \begin{pmatrix} R^{p^r} & & & \\ & R^{p^r} & & \\ & & \ddots & \\ & & & R^{p^r} \end{pmatrix}.$$

But by Lemma 3.8,

$$B_d^{p^r} = \begin{pmatrix} I_{p^m} & & & \\ & I_{p^m} & & \\ & & \ddots & \\ & & & I_{p^m} \end{pmatrix}.$$

Therefore  $R^{p^r} = I_{p^m}$  and, since  $R$  corresponds to a  $p^m$ -cycle,  $r \geq m$ .  $\square$

From Lemma 3.9 and Eq. (12) we deduce that

$$l^2 \equiv D_l \pmod{p^{r-m}} \tag{13}$$

and

$$l^2 \not\equiv D_l \pmod{p^{r-m+1}} \tag{14}$$

for  $0 \leq l < p^r$ . Since if  $m = 0$  then any  $p^m$ th root of 1 is primitive, condition (14) applies only if  $m \neq 0$ . We remark that these two conditions can be expressed as

$$v_p(l^2 - D_l) = r - m \tag{15}$$

where  $v_p(x)$  is the  $p$ -adic valuation of  $x$ .

We have now completely determined all of our matrices. That is,

$$A = \begin{pmatrix} I_{p^m} & & & \\ & \Lambda I_{p^m} & & \\ & & \ddots & \\ & & & \Lambda^{p^r-1} I_{p^m} \end{pmatrix},$$

$$B = \begin{pmatrix} 0_{p^m} & & & I_{p^m} \\ I_{p^m} & & & \\ & \ddots & & \\ & & \ddots & \\ & & & I_{p^m} & 0_{p^m} \end{pmatrix},$$

$$A_d = \begin{pmatrix} J & & & \\ & \Lambda^l J & & \\ & & \ddots & \\ & & & \Lambda^{(p^r-1)l} J \end{pmatrix},$$

and

$$B_d = \begin{pmatrix} 0 & & & R & & \\ & \ddots & & & \ddots & \\ & & \ddots & & & R \\ R & & & \ddots & & \\ & \ddots & & R & & \\ & & & & \ddots & 0 \end{pmatrix}$$

where

$$J = \begin{pmatrix} 1 & & & \\ & \Lambda^{l^2-D_l} & & \\ & & \ddots & \\ & & & \Lambda^{(p^r-1)(l^2-D_l)} \end{pmatrix}$$

and

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

There are  $(1 - p^{-1})p^r$  choices for the primitive root of unity  $\Lambda$ . The number of choices for  $\Lambda_d = \Lambda^l$ —that is, the number of the solutions to congruences (13) and (14)—will be analyzed in Section 3.3.

**Case 2.**  $\Lambda_d$  is a primitive  $p^r$ th root of unity. The analysis in this case is similar to Case 1. However, in order to avoid overcounting, we also assume the condition

$$\Lambda \text{ is not a primitive } p^r \text{th root of unity.} \tag{16}$$

Following the methods in Case 1, but switching the roles of  $B$  and  $B_d$ , we obtain the matrices

$$A = \begin{pmatrix} I_{p^m} & & & \\ & \Lambda_d I_{p^m} & & \\ & & \ddots & \\ & & & \Lambda_d^{p^r-1} I_{p^m} \end{pmatrix},$$

$$B_d = \begin{pmatrix} 0_{p^m} & & & I_{p^m} \\ I_{p^m} & \ddots & & \\ & \ddots & \ddots & \\ & & I_{p^m} & 0_{p^m} \end{pmatrix},$$

$$A_d = \begin{pmatrix} J & & & \\ & \Lambda_d^{lD_l} J & & \\ & & \ddots & \\ & & & \Lambda_d^{(p^r-1)lD_l} J \end{pmatrix},$$

and

$$B = \begin{pmatrix} 0 & & & R \\ & \ddots & & \\ & & \ddots & R \\ R & & & \\ & \ddots & & \\ & & R & \\ & & & 0 \end{pmatrix}$$

where

$$J = \begin{pmatrix} 1 & & & \\ & \Lambda_d^{l^2 D_{l-1}} & & \\ & & \ddots & \\ & & & \Lambda_d^{(p^r-1)(l^2 D_{l-1})} \end{pmatrix}$$

and

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

This allows us to recover the conditions

$$l^2 D_l \equiv 1 \pmod{p^{r-m}} \tag{17}$$

and

$$l^2 D_l \not\equiv 1 \pmod{p^{r-m+1}} \tag{18}$$

for  $0 \leq l < p^r$ , where condition (18) does not apply when  $m = 0$ . We remark that these two equations can be written as

$$v_p(l^2 D_l - 1) = r - m. \tag{19}$$

This concludes the case distinctions.

Call Eqs. (13) and (14), the **Case 1** conditions and Eqs. (17) and (18) the **Case 2** conditions. Note that the **Case 2** conditions imply that  $l$  is invertible modulo  $p$ . However, since we are assuming condition (16) in **Case 2**, we have that  $p \mid l$ . Thus, there are only solutions to the **Case 2** conditions when  $r = m$ .

Now we check that all matrices of this form give us an irreducible representation of  $H(O_d)$ . This is clear; take matrices  $\{A, B, A_d, B_d, \Lambda, \Lambda_d\}$  of the forms above. Then an easy calculation shows that the associated relations for  $H(O_d)$  hold. Since  $z, z_d$  are commutators, they remain fixed under twisting. Since the matrices  $A, B, A_d$ , and  $B_d$  are determined by  $\Lambda$  and  $\Lambda_d$ , two such ordered sets of matrices define twist-equivalent representations if and only if they coincide.

The form of  $\zeta_{H(O_d),p}(s)$  depends on  $p$  and  $d$ . This subsection therefore implies the following:

**Proposition 3.10.** *There is a 1-1 correspondence between the set of  $p^n$ -dimensional twist-isoclasses of  $H(O_d)$  and the set of solutions to conditions (13), (14) in **Case 1** or (16), (17), (18) in **Case 2** such that  $r + m = n, 0 \leq m \leq r \leq n$ .*

### 3.3. Calculating the zeta function

**Proposition 3.10** allows us to calculate each  $\zeta_{H(O_d),p}(s)$  by counting solutions to conditions (13) and (14) in **Case 1** and (17) and (18) in **Case 2** modulo  $p^n$  for each  $n \geq 0$ . To count the number of solutions we use Hensel’s Lemma to lift solutions of the conditions modulo  $p$  if  $p$  is not ramified; if  $p$  is ramified, the computation is nevertheless straightforward. We demonstrate the computations and then summarize the results in a table. We note three things: there are always  $(1 - p^{-1})p^r$  choices

for  $\Lambda$  in Case 1 and  $\Lambda_d$  in Case 2, in Case 2 it is easy to see there are  $(1 - p^{-1})p^{n-1}$  solutions when  $r = m$  and 0 otherwise, and there is only 1 irreducible twist-isoclass when  $n = 0$ . The following cases assume  $n \neq 0$ .

For ease of understanding we tabulate the conditions with their reference numbers:

Case 1	$\Lambda$ is a primitive $p^r$ th root of unity	
	$l^2 \equiv D_l \pmod{p^{r-m}}$	(13)
	$l^2 \not\equiv D_l \pmod{p^{r-m+1}}$ for $r \neq n$	(14)
Case 2	$\Lambda_d$ is a primitive $p^r$ th root of unity	
	$\Lambda$ is not a primitive $p^r$ th root of unity	
	$l^2 D_l \equiv 1 \pmod{p^{r-m}}$	(17)
	$l^2 D_l \not\equiv 1 \pmod{p^{r-m+1}}$ for $r \neq n$	(18)

Assume  $p$  is inert. This implies that  $d$  is not a square modulo  $p$ . Thus, in this case, there are no solutions to the Case 1 or Case 2 conditions unless  $r = m$ . Given  $\Lambda$ , and since  $r + m = n$ , there are  $p^{\frac{n}{2}}$  choices for  $\Lambda_d$  in Case 1. Therefore, with Case 2 contributing  $(1 - p^{-1})p^{\frac{n}{2}}(p^{\frac{n}{2}-1})$  in the even case,

$$r_{p^n} = \begin{cases} (1 - p^{-1})p^{\frac{n}{2}}p^{\frac{n}{2}} + (1 - p^{-1})p^{\frac{n}{2}}(p^{\frac{n}{2}-1}) & \text{for even } n, \\ 0 & \text{for odd } n \end{cases}$$

and

$$\zeta_{H(O_d),p}(s) = \sum_{n=0}^{\infty} r_{p^n} p^{-ns} = 1 + \sum_{m=1}^{\infty} (1 - p^{-2})(p^{2-2s})^m = \frac{1 - p^{-2s}}{1 - p^{2-2s}}.$$

Assume  $p$  splits. There are two solutions to the equation  $l^2 \equiv D_l \pmod{p}$  and Hensel's Lemma allows us to "lift" these solutions to solutions in  $\mathbb{Z}/p^{r-m}\mathbb{Z}$ , thus giving us the two unique solutions to  $l^2 \equiv D_l \pmod{p^{r-m}}$ . When  $r = n$ , there are two solutions to condition (13) and therefore  $2(1 - p^{-1})p^n$  choices for the pair  $\Lambda$  and  $\Lambda_d$  in the Case 1 conditions. If, for fixed  $r$  and  $m$ ,  $r > m$  and  $m > 0$  then there are two solutions in  $\mathbb{Z}/p^{r-m}\mathbb{Z}$  to condition (13) and therefore  $2p^m$  solutions for  $0 \leq l \leq p^r - 1$ . Of these solutions, all but  $2p^{m-1}$  satisfy condition (14). Therefore, given  $\Lambda$ , there are  $2(1 - p^{-1})p^m$  choices for  $\Lambda_d$  and  $2(1 - p^{-1})^2 p^n$  choices for the pair  $\Lambda$  and  $\Lambda_d$  in Case 1. If  $r = m = \frac{n}{2}$  then there are  $p^m$  solutions to condition (13), of which all but  $2p^{m-1}$  satisfy condition (14). Therefore there are  $(1 - 2p^{-1})(1 - p^{-1})p^n$  choices for the pair  $\Lambda$  and  $\Lambda_d$  in Case 1. Summing all cases together, and noting that Case 2 contribution is 0 in the odd case and  $(1 - p^{-1})p^{n-1}$  in the even case, we have

$$r_{p^n} = \begin{cases} 2(1 - p^{-1})p^n + \frac{n-1}{2}2(1 - p^{-1})^2 p^n & \text{if } n \text{ is odd,} \\ 2(1 - p^{-1})p^n + \frac{n-2}{2}2(1 - p^{-1})^2 p^n \\ \quad + (1 - 2p^{-1})(1 - p^{-1})p^n + (1 - p^{-1})p^{n-1} & \text{if } n \text{ is even.} \end{cases} \tag{20}$$

Strikingly, in both cases this simplifies to

$$r_{p^n} = ((1 + p^{-1}) + (1 - p^{-1})n)(1 - p^{-1})p^n$$

and therefore

$$\begin{aligned} \zeta_{H(O_d),p}(s) &= \sum_{n=0}^{\infty} r_{p^n} p^{-ns} \\ &= 1 + \sum_{n=1}^{\infty} (1 - p^{-1})(p^{1-s})^n [(1 + p^{-1}) + (1 - p^{-1})n] \end{aligned}$$

$$\begin{aligned}
 &= 1 + \sum_{n=1}^{\infty} (1 - p^{-2})(p^{1-s})^n + \sum_{n=1}^{\infty} (1 - p^{-1})^2 n(p^{1-s})^n \\
 &= 1 + \frac{(1 - p^{-2})p^{1-s}}{1 - p^{1-s}} + \frac{(1 - p^{-1})^2 p^{1-s}}{(1 - p^{1-s})^2} \\
 &= \left( \frac{1 - p^{-s}}{1 - p^{1-s}} \right)^2.
 \end{aligned}$$

Assume  $p$  is ramified. This is the case if  $d \equiv 0 \pmod{p}$  for any  $d$  or if  $p = 2$  and  $d \equiv 2, 3 \pmod{4}$ . Then there are solutions to the [Case 1](#) and [Case 2](#) conditions only when  $r - m = 0$  or  $r - m = 1$ . If  $d \equiv 2, 3 \pmod{4}$  and  $d \equiv 0 \pmod{p}$  then 0 is the solution to  $l^2 \equiv d \pmod{p}$  but since  $d$  is squarefree  $d \equiv kp \pmod{p^2}$  for some invertible  $k \in \mathbb{Z}/p^2\mathbb{Z}$ . Therefore  $l^2 = d$  has no solutions modulo  $p^2$ . If  $d \equiv 2, 3 \pmod{4}$  and  $p = 2$  then  $l^2 \equiv d$  has a solution modulo  $p$  but since  $d$  is a quadratic non-residue modulo 4 it has no solutions modulo 4. If  $d \equiv 1 \pmod{4}$  and  $d \equiv 0 \pmod{p}$  then  $l^2 - l + \frac{d-1}{4} = 0$  has the unique solution  $l \equiv 2^{-1} \pmod{p}$ . And since  $d$  is squarefree  $d \equiv kp \pmod{p^2}$  for some invertible  $k \in \mathbb{Z}/p^2\mathbb{Z}$ . Then the above equation can be rearranged to the form  $(2l - 1)^2 \equiv kp \pmod{p^2}$ , which clearly has no solutions. Then if  $r - m = 0$ , then there are  $p^m$  solutions to condition (13) and all but  $p^{m-1}$  of these satisfy condition (14). Therefore, given  $\Lambda$  there are  $(1 - p^{-1})p^m$  choices for  $\Lambda_d$  and  $(1 - p^{-1})(1 - p^{-1})p^n$  choices for the pair  $\Lambda$  and  $\Lambda_d$  in [Case 1](#) and, as usual,  $(1 - p^{-1})p^{n-1}$  choices in [Case 2](#). If  $r - m = 1$ , a similar calculation to the ones above yields that there are  $(1 - p^{-1})p^n$  choices in [Case 1](#). Therefore

$$r_{p^n} = (1 - p^{-1})p^n$$

and thus

$$\begin{aligned}
 \zeta_{H(O_d), p}(s) &= 1 + \sum_{n=1}^{\infty} (1 - p^{-1})p^n p^{-ns} \\
 &= 1 + (1 - p^{-1}) \sum_{n=1}^{\infty} (p^{1-s})^n \\
 &= \frac{1 - p^{-s}}{1 - p^{1-s}}.
 \end{aligned}$$

The preceding results are tabulated for easy reference. Note that, for  $k \geq 1$ , we have that  $\phi(p^k) = (1 - p^{-1})p^k$ :

Prime behaviour	$r_{p^n}; n > 0$	$\zeta_{H(O_d), p}(s)$
inert	$\begin{cases} (1 + p^{-1})\phi(p^n) & \text{for even } n \\ 0 & \text{for odd } n \end{cases}$	$\frac{1 - p^{-2s}}{1 - p^{2-2s}}$
splits	$\phi(p^n)(n(1 - p^{-1}) + 1 + p^{-1})$	$\left(\frac{1 - p^{-s}}{1 - p^{1-s}}\right)^2$
ramified	$\phi(p^n)$	$\frac{1 - p^{-s}}{1 - p^{1-s}}$

By [Proposition 2.3](#) we can say that

$$\zeta_{H(O_d)}(s) = \frac{\zeta_{\mathbb{Q}(\sqrt{d})}^{\mathbf{D}}(s - 1)}{\zeta_{\mathbb{Q}(\sqrt{d})}^{\mathbf{D}}(s)}.$$

## Acknowledgments

The author would like to thank Ben Martin for overall guidance and the many great suggestions for the structure of the paper. The author would also like to show appreciation to the referee for their helpful suggestions.

## References

- [1] N. Avni, Arithmetic groups have rational representation growth, *Ann. of Math. (2)* 174 (2) (2011) 1009–1056.
- [2] N. Avni, B. Klopsch, U. Onn, C. Voll, Arithmetic groups, base change and representation growth, preprint, <http://arxiv.org/pdf/1110.6092>.
- [3] N. Avni, B. Klopsch, U. Onn, C. Voll, On representation zeta functions of groups and a conjecture of Larsen–Lubotzky, *C. R. Math. Acad. Sci. Paris, Ser. I* 348 (2010) 363–367.
- [4] N. Avni, B. Klopsch, U. Onn, C. Voll, Representation zeta functions of compact  $p$ -adic analytic groups and arithmetic groups, *Duke Math. J.* 162 (2013) 111–197.
- [5] L. Bartholdi, P. de la Harpe, Representation zeta functions of wreath products with finite groups, *Groups Geom. Dyn.* 4 (2) (2010) 209–249.
- [6] H. Cohen, *Number Theory: Analytic and Modern Tools*, Springer, 2007.
- [7] D.A. Craven, Lower bounds for representation growth, *J. Group Theory* 13 (6) (2010) 873–890.
- [8] M. du Sautoy, F. Grunewald, Analytic properties of zeta functions and subgroup growth, *Ann. of Math. (2)* 152 (3) (2000) 793–833.
- [9] M.P.F. du Sautoy, F.J. Grunewald, Analytic properties of Euler products of Igusa-type zeta functions and subgroup growth of nilpotent groups, *C. R. Math. Acad. Sci. Paris, Ser. I* 329 (5) (1999) 351–356.
- [10] M.P.F. du Sautoy, F.J. Grunewald, Analytic properties of zeta functions and subgroup growth, *Ann. of Math. (2)* 152 (3) (2000) 793–833.
- [11] F.J. Grunewald, D. Segal, G.C. Smith, Subgroups of finite index in nilpotent groups, *Invent. Math.* 93 (1988) 185–223.
- [12] Roger E. Howe, On representations of discrete, finitely generated, torsion-free, nilpotent groups, *Pacific J. Math.* 73 (2) (1977) 281–305.
- [13] E. Hrushovski, B. Martin, Zeta functions from definable equivalence relations, preprint, <http://arxiv.org/pdf/math/0701011>.
- [14] A. Jaikin-Zapirain, Zeta functions of representations of compact  $p$ -adic analytic groups, *J. Amer. Math. Soc.* 19 (1) (2006) 91–118 (electronic).
- [15] M. Kassabov, N. Nikolov, Cartesian products as profinite completions, *Int. Math. Res. Not. IMRN* (2006).
- [16] B. Klopsch, N. Nikolov, C. Voll, A newcomer's guide to zeta functions of groups and rings, in: Dan Segal (Ed.), *Lectures on Profinite Topics in Group Theory*, in: London Math. Soc. Stud. Texts, vol. 77, Cambridge University Press, 2011, Chapter authored by Christopher Voll.
- [17] M. Larsen, A. Lubotzky, Representation growth of linear groups, *J. Eur. Math. Soc. (JEMS)* 10 (2) (2008) 351–390.
- [18] A. Lubotzky, A.R. Magid, Varieties of representations of finitely generated groups, *Mem. Amer. Math. Soc.* 58 (336) (1985), xi+117.
- [19] A. Lubotzky, B. Martin, Polynomial representation growth and the congruence subgroup problem, *Israel J. Math.* 144 (2004) 293–316.
- [20] A. Lubotzky, D. Segal, *Subgroup Growth*, Birkhäuser-Verlag, 2000.
- [21] A.R. Magid, C. Nunley, Simple representations of the integral Heisenberg group, *Contemp. Math.* 82 (1989) 89–96.
- [22] A. Stasinski, C. Voll, Representation zeta functions of nilpotent groups and generating functions for Weyl groups of type  $B$ , *Amer. J. Math.* (2013), in press, <http://arxiv.org/pdf/1104.1756v1.pdf>.
- [23] C. Voll, Functional equations for zeta functions of groups and rings, *Ann. of Math.* 172 (2) (2010) 1181–1218.
- [24] E. Witten, On quantum gauge theories in two dimensions, *Comm. Math. Phys.* 141 (1) (1991) 153–209.