

The Witt classes of $\mathfrak{so}(2r)2r$

Eric C. Rowell, Yuze Ruan & Yilong Wang

To cite this article: Eric C. Rowell, Yuze Ruan & Yilong Wang (2022) The Witt classes of $\mathfrak{so}(2r)2r$, Communications in Algebra, 50:12, 5246-5265, DOI: [10.1080/00927872.2022.2083630](https://doi.org/10.1080/00927872.2022.2083630)

To link to this article: <https://doi.org/10.1080/00927872.2022.2083630>



Published online: 10 Jun 2022.



Submit your article to this journal [↗](#)



Article views: 47






View related articles [↗](#)



View Crossmark data [↗](#)



The Witt classes of $\mathfrak{so}(2r)_{2r}$

Eric C. Rowell^a , Yuze Ruan^b , and Yilong Wang^b 

^aDepartment of Mathematics, Texas A&M University, College Station, TX, USA; ^bYanqi Lake Beijing Institute of Mathematical Science and Applications (BIMSA) Huairou, Beijing, China

ABSTRACT

We study the Witt classes of the modular categories $\mathfrak{so}(2r)_{2r}$ associated with quantum groups of type D_r at $(4r - 2)$ -th roots of unity. From these classes we derive infinitely many Witt classes of order 2 that are linearly independent modulo the subgroup generated by the pointed modular categories. In particular, we produce an example of a simple, completely anisotropic modular category that is not pointed whose Witt class has order 2, answering a question of Davydov, Müger, Nikshych and Ostrik. Our results show that the trivial Witt class $[\text{Vec}]$ has infinitely many square roots modulo the pointed classes, in analogy with the recent construction of infinitely many square roots of the Ising Witt classes modulo the pointed classes constructed in a similar way from certain type B_r modular categories. We compare the subgroups generated by the Ising square roots and $[\text{Vec}]$ square roots and provide evidence that they also generate linearly independent subgroups.

ARTICLE HISTORY

Received 2 August 2021
Revised 25 March 2022
Communicated by Julia Plavnik

KEYWORDS

Higher central charge;
quantum group modular
category; signature;
Witt group

2020 MATHEMATICS SUBJECT

CLASSIFICATION
18M20; 11E81;
17B37; 18M15

1. Introduction

Modular categories play a central role in the study of 2-dimensional topological phases of matter [19], invariants of 3-manifolds [31] and conformal field theory [16]. The problem of classifying modular categories led to the definition [5] of the Witt group \mathcal{W} for non-degenerate braided fusion categories, generalizing the Witt group for abelian groups equipped with non-degenerate quadratic forms (see [8]). Two non-degenerate braided fusion categories \mathcal{C} and \mathcal{D} are Witt equivalent if they are equivalent “modulo Drinfeld centers,” i.e., if $\mathcal{C} \boxtimes \mathcal{Z}(\mathcal{A}) \cong \mathcal{D} \boxtimes \mathcal{Z}(\mathcal{B})$ for some fusion categories \mathcal{A}, \mathcal{B} .

Recently [20] it was shown that the 8 Witt classes of Ising categories have infinitely many independent square roots modulo the subgroup generated by pointed categories. This was achieved using the *signature*, a new Witt class invariant related to the higher central charge introduced in [22]. From this a verification of a conjecture of [6] was derived, namely, that the torsion subgroup $s\mathcal{W}_2$ of the super-Witt group has infinite rank. The categories representing the square roots of the Ising Witt classes are of the form $\mathfrak{so}(N)_N$ with N odd, obtained from the (Lie type B) quantum groups $U_q \mathfrak{so}(N)$ at $q = e^{\pi i/(4N-4)}$. In this article we study the case N even, obtained from (Lie type D) quantum groups of $U_q \mathfrak{so}(N)$ with $q = e^{\pi i/(2N-2)}$. From these we obtain infinitely many Witt classes of order 2, which intersect trivially with the subgroup generated by the pointed and Ising classes. Thus we have infinitely many square roots of the trivial Witt class $[\text{Vec}]$, modulo the subgroup generated by the pointed and Ising Witt classes. From this we derive an affirmative answer to [5, Question 6.8]: there *does* exist a completely anisotropic simple

modular category whose Witt class has order 2. We also compare the Lie type D Witt classes studied here with the Lie type B Witt classes of [20]. Although we cannot show there are no relations among them, we do find an infinite sequence of type D classes that intersects trivially with the infinite sequence of type B Witt classes used in [20] to verify the conjecture of [6].

Our results further illustrate the usefulness of the signature for distinguishing Witt classes. The methods we use are number-theoretical and thus require carefully chosen parameters. It would be interesting to understand the relations among all of these Witt classes. We believe that the examples we study provide infinitely many Witt-independent examples of non-pointed completely anisotropic simple modular categories (so-called property S categories) with order 2 Witt classes, but we only verify a single example.

Here is a more detailed outline of this article. After providing the notation and context of the problem we derive square roots of $[\text{Vec}]$ from quantum groups of Lie type D_r , treating the r odd and r even case separately. Next we compute their signatures, and use them to find a subsequence of these Witt classes that are linearly independent, modulo the subgroup generated by pointed and Ising categories. Next we compare the Witt subgroups we study with those of [20]. Finally we show that at least one square root of $[\text{Vec}]$ is both simple and anisotropic, answering a question of [5].

2. Preliminaries and notation

We assume some familiarity with the standard notions in the theory of fusion categories, referring the reader to [10] for a complete treatment. Mainly to fix notation we provide some details.

2.1. Fusion categories

A *fusion category* over \mathbb{C} is a semisimple, \mathbb{C} -linear abelian, rigid monoidal category with finite-dimensional Hom-spaces and finitely many isomorphism classes of simple objects among which is the tensor unit $\mathbb{1}$ [11]. For any fusion category \mathcal{C} , we denote by $\text{Irr}(\mathcal{C})$ a complete set of representatives of the isomorphism classes of \mathcal{C} . The tensor product endows $K_0(\mathcal{C})$, the Grothendieck group of \mathcal{C} , with a ring structure. More precisely, we have $X \otimes Y = \sum_{Z \in \text{Irr}(\mathcal{C})} N_{X,Y}^Z Z$ for any $X, Y \in \text{Irr}(\mathcal{C})$, where

$$N_{X,Y}^Z := \dim_{\mathbb{C}} \mathcal{C}(X \otimes Y, Z).$$

For any $X \in \text{Irr}(\mathcal{C})$, let \mathcal{N}_X be the square matrix of size $|\text{Irr}(\mathcal{C})|$ such that $(\mathcal{N}_X)_{Y,Z} = N_{X,Y}^Z$ for any $Y, Z \in \text{Irr}(\mathcal{C})$. The *Frobenius-Perron dimension* of $X \in \text{Irr}(\mathcal{C})$, denoted by $\text{FPdim}(X)$, is the largest positive eigenvalue for \mathcal{N}_X (see [11]). The Frobenius-Perron dimension of \mathcal{C} is defined to be

$$\text{FPdim}(\mathcal{C}) = \sum_{X \in \text{Irr}(\mathcal{C})} \text{FPdim}(X)^2.$$

Let \mathcal{C} be a fusion category. The rigidity of \mathcal{C} means that for any object $V \in \mathcal{C}$, there is a left dual $(V^*, \text{ev}_V, \text{coev}_V)$, where $V^* \in \mathcal{C}$ is an object, $\text{ev}_V : V^* \otimes V \rightarrow \mathbb{1}$ and $\text{coev}_V : \mathbb{1} \rightarrow V \otimes V^*$ are morphisms satisfying the duality conditions in [10, Def. 2.10.1]. The notion of a right dual is similarly defined [10, Def. 2.10.2]. It is well-known that dual objects are unique up to isomorphism (see, for example, [1, Lem. 2.1.5]). A simple object $X \in \text{Irr}(\mathcal{C})$ is called *invertible* if ev_X and coev_X above are isomorphisms. A fusion category is *pointed* if all of its simple objects are invertible. We denote the maximal pointed fusion subcategory of \mathcal{C} by \mathcal{C}_{pt} . If $\text{Irr}(\mathcal{C}_{\text{pt}}) = \{\mathbb{1}\}$, then \mathcal{C} is called *unpointed*.

The *global dimension* $\dim(\mathcal{C})$ of a fusion category \mathcal{C} was introduced in [17, Def. 2.5]. By [11, Rmk. 2.5], $\dim(\mathcal{C})$ is a totally positive algebraic integer. We denote the positive square root of $\dim(\mathcal{C})$ by $\sqrt{\dim(\mathcal{C})}$, which will play a central role in our results. Finally, a fusion category \mathcal{C} is called *pseudounitary* if $\dim(\mathcal{C}) = \text{FPdim}(\mathcal{C})$.

2.2. Braided and ribbon fusion categories

Let \mathcal{C} be a fusion category. A *braiding* on \mathcal{C} is a natural isomorphism $\beta_{V,W} : V \otimes W \xrightarrow{\cong} W \otimes V$ satisfying the Hexagon axioms (see [10, Chap. 8]). A fusion category equipped with a braiding is called a *braided fusion category*. For any fusion subcategory \mathcal{D} in \mathcal{C} , the *centralizer* of \mathcal{D} in \mathcal{C} , denoted by \mathcal{D}' , is the full fusion subcategory of \mathcal{C} generated by objects $V \in \mathcal{C}$ such that $\beta_{W,V} \circ \beta_{V,W} = \text{id}_{V \otimes W}$ for all $W \in \mathcal{D}$. The centralizer \mathcal{C}' of \mathcal{C} itself is called the *Müger center* of \mathcal{C} . A braided fusion category \mathcal{C} is called *non-degenerate* if $\text{Irr}(\mathcal{C}') = \{1\}$, i.e., \mathcal{C}' is equivalent to Vec , the category of finite-dimensional vector spaces over \mathbb{C} . For any fusion category \mathcal{C} , its *Drinfeld center*, denoted by $\mathcal{Z}(\mathcal{C})$, is the category with objects of the form $(V, c_{-,V})$, where $V \in \mathcal{C}$ and $c_{W,V} : W \otimes V \xrightarrow{\cong} V \otimes W$ is a natural family of isomorphisms satisfying the half-braiding conditions in [13, Def. XIII.4.1]. It is well-known that $\mathcal{Z}(\mathcal{C})$ is a non-degenerate braided fusion category (see, for example, [8, Cor. 3.9]). A braided fusion category \mathcal{C} is called *symmetric* if $\mathcal{C}' = \mathcal{C}$. The fusion category $\text{Rep}(G)$ of finite-dimensional complex representations of a finite group G , endowed with the standard braiding, is a symmetric fusion category also denoted by $\text{Rep}(G)$ for convenience. A symmetric fusion category equivalent to $\text{Rep}(G)$ for some finite group G is called *Tannakian*.

A *ribbon structure* on a braided fusion category \mathcal{C} equipped with a braiding β is a natural isomorphism $\theta : \text{id}_{\mathcal{C}} \rightarrow \text{id}_{\mathcal{C}}$ of the identity functor satisfying $\theta_{V^*} = \theta_V^*$ and

$$\theta_{V \otimes W} = (\theta_V \otimes \theta_W) \circ \beta_{W,V} \circ \beta_{V,W} \quad (2.1)$$

for any $V, W \in \mathcal{C}$. In particular, for any $X \in \text{Irr}(\mathcal{C})$, θ_X is equal to a non-zero scalar times id_X . By an abuse of notation, we denote both the scalar and the isomorphism itself by θ_X for all simple X , and we call θ_X the (*topological*) *twist* of X . It is shown by Vafa [32] that for all $X \in \text{Irr}(\mathcal{C})$, θ_X is a root of unity, so $\text{ord}(T_{\mathcal{C}}) := \text{lcm}\{\text{ord}(\theta_X) \mid X \in \text{Irr}(\mathcal{C})\}$ is finite. A braided fusion category \mathcal{C} with a ribbon structure θ is called a *ribbon fusion category*, or a *premodular category*. In a premodular category, endomorphisms are equipped with a canonical trace valued in \mathbb{C} . In particular, this leads to well-defined *quantum dimensions* d_V for objects $V \in \mathcal{C}$, and one has $\dim(\mathcal{C}) = \sum_{X \in \text{Irr}(\mathcal{C})} d_X^2$. For details, see [1, 11]. A premodular category \mathcal{C} is called *modular* if the underlying braided fusion category is non-degenerate.

Numerical invariants of modular categories can be obtained from quantum dimensions and twists. For example, for any modular category \mathcal{C} and any integer $n \in \mathbb{Z}$, the n -th *Gauss sum* is defined in [22] as $\tau_n(\mathcal{C}) = \sum_{X \in \text{Irr}(\mathcal{C})} d_X^2 \theta_X^n$. When $\tau_n \neq 0$, the n -th *central charge* is defined to be

$$\xi_n(\mathcal{C}) := \frac{\tau_n(\mathcal{C})}{|\tau_n(\mathcal{C})|}, \quad (2.2)$$

where the denominator on the right hand side represents the (complex) absolute value of $\tau_n(\mathcal{C})$. By [11, Prop. 2.10] and the finiteness of $\text{ord}(T_{\mathcal{C}})$, the complex conjugate of $\tau_n(\mathcal{C})$ equals to $\tau_{-n}(\mathcal{C})$ for all $n \in \mathbb{Z}$. In particular, when $n = 1$, by [10, Prop. 8.15.4] we can also write

$$\xi_1(\mathcal{C}) = \frac{\tau_1(\mathcal{C})}{\sqrt{\dim(\mathcal{C})}}. \quad (2.3)$$

These invariants provide insights on modular categories and the Witt group, as is demonstrated in [20, 22].

Finally, we will need the following classification result on pointed braided fusion categories (for details, see [10, Sec. 8.4]): such categories are parameterized by pairs (H, Q) and denoted by $\mathcal{C}(H, Q)$, where H is a finite abelian group and $Q : H \rightarrow \mathbb{C}^\times$ is a quadratic form on H . Simple objects in $\mathcal{C}(H, Q)$ are in one-to-one correspondence to the elements of H . Moreover, $\mathcal{C}(H, Q)$ is a ribbon fusion category whose ribbon structure is determined by the twists $\theta_a = Q(a)$ for $a \in H = \text{Irr}(\mathcal{C}(H, Q))$, and it is modular if and only if the map $(a, b) \mapsto \frac{Q(a+b)}{Q(a)Q(b)}$ is a non-degenerate bicharacter on H .

An important example of pointed modular categories is the *semion* modular category [24], denoted by **Sem**. Using the notation above, we characterize **Sem** as $\mathcal{C}(\mathbb{Z}/2\mathbb{Z}, Q)$ with $Q(a) = i^{a^2}$ for $a \in \mathbb{Z}/2\mathbb{Z}$, which implies

$$\xi_1(\mathbf{Sem}) = \exp\left(\frac{\pi i}{4}\right). \quad (2.4)$$

2.3. Witt group \mathcal{W}

The concept of Witt equivalence of non-degenerate braided fusion categories is introduced in [5]. More precisely, two non-degenerate braided fusion categories \mathcal{C} and \mathcal{D} are Witt equivalent if there exist fusion categories \mathcal{A} and \mathcal{B} such that $\mathcal{C} \boxtimes \mathcal{Z}(\mathcal{A}) \cong \mathcal{D} \boxtimes \mathcal{Z}(\mathcal{B})$. We denote the Witt equivalence class of a category \mathcal{C} by $[\mathcal{C}]$. Under the Deligne product, Witt equivalence classes form an abelian group denoted by \mathcal{W} . The Witt group \mathcal{W} of non-degenerate braided fusion categories can be viewed as a generalization of the classical Witt group of non-degenerate quadratic forms on abelian groups (i.e., metric groups), which generate the pointed part of \mathcal{W} denoted by \mathcal{W}_{pt} (for details, see [5, 8]). In addition to mathematical interests, the study of the Witt group is also closely related to phase transitions driven by anyon condensation and symmetry gauging in topological phases of matter [2, 3].

Numerical invariants are powerful tools in the study of the structure of the Witt group. For example, the first central charge ξ_1 (see (2.2)) is used in the study of conformal embeddings of rational vertex operator algebras associated to affine Lie algebras [5]. Another important Witt invariant, namely, the *signature homomorphism*, is introduced in [20]. Here, we briefly recall the definition. For any fusion category \mathcal{C} , it is well-known that $\text{FPdim}(\mathcal{C})$ is totally positive algebraic integer [11]. Therefore, its positive square root, denoted by $\sqrt{\text{FPdim}(\mathcal{C})}$, is a totally real algebraic integer, and the signature of \mathcal{C} is then defined to be the sign of its Galois conjugates. More precisely, let $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of \mathbb{Q} , then the signature of \mathcal{C} is the function

$$\varepsilon_{\mathcal{C}} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \{\pm 1\}, \quad \sigma \mapsto \text{sgn}\left(\sigma(\sqrt{\text{FPdim}(\mathcal{C})})\right). \quad (2.5)$$

By Galois theory, it is easy to see that $\varepsilon_{\mathcal{C}}$ factors through any Galois extension of \mathbb{Q} containing $\sqrt{\text{FPdim}(\mathcal{C})}$. Therefore, in the sections below, we will use large enough fields (instead of $\bar{\mathbb{Q}}$) to simplify computations. Let $\mathcal{U}_2 := \{\pm 1\}^{\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})}$ be the group of functions from $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to $\{\pm 1\}$. Then by [20, Thm. 3.4], the signature map induces a well-defined group homomorphism

$$I : \mathcal{W} \rightarrow \mathcal{U}_2, \quad [\mathcal{C}] \mapsto \varepsilon_{\mathcal{C}}, \quad (2.6)$$

which is the main technical tool in this paper.

It is natural to pursue constructions of new non-degenerate braided fusion categories that are Witt equivalent to a given one, and taking local modules of connected étale algebras is one such construction. Let \mathcal{C} be a braided fusion category with braiding β . The notion of a *connected étale algebra* object $A \in \mathcal{C}$ is defined in [5, Sec. 3.1]. It is shown in [5] that if $A \in \mathcal{C}$ is a connected étale algebra, then \mathcal{C}_A , the category of right A -modules, is a fusion category. Moreover, according

to [14, 23], β descends to A -module maps for *local* modules. Here a (right) A -module M with A -action $\alpha : M \otimes A \rightarrow M$ is called *local* (or *dyslectic*) if it satisfies $\alpha \circ \beta_{A,M} \circ \beta_{M,A} = \alpha$. As an immediate consequence, \mathcal{C}_A^0 , the full subcategory of \mathcal{C}_A of local modules of A , is a braided fusion category. In [5, Sec. 3], it is pointed out that if \mathcal{C} is a ribbon fusion category with ribbon structure θ , then a rigid algebra $A \in \mathcal{C}$ in the sense of [14] is connected étale with non-zero quantum dimension if and only if $\theta_A = \text{id}$. Group symmetry provides examples of the local module construction. Namely, when \mathcal{C} contains a Tannakian fusion subcategory $\text{Rep}(G)$ for some finite group G , then the regular algebra $A = \text{Fun}(G)$ is a connected étale algebra in \mathcal{C} . The corresponding local module \mathcal{C}_A^0 can also be characterized in the context of de-equivariantization [5, 8].

The importance of the local module construction is well illustrated in the combination of Corollary 3.32 and Proposition 5.4 of [5]: for any non-degenerate braided fusion category \mathcal{C} and any connected étale algebra $A \in \mathcal{C}$, we have

$$\text{FPdim}(\mathcal{C}_A^0) = \frac{\text{FPdim}(\mathcal{C})}{\text{FPdim}(A)^2} \quad \text{and} \quad [\mathcal{C}] = [\mathcal{C}_A^0]. \quad (2.7)$$

Therefore, in order to study the Witt class of \mathcal{C} , it suffices to study the smaller category \mathcal{C}_A^0 .

By taking the local module category of a maximal connected étale algebra in a non-degenerate braided fusion category \mathcal{C} , one gets a “minimal” representative in its Witt class in the following sense. A non-degenerate braided fusion category is called *completely anisotropic* if it does not contain any connected étale algebra other than $\mathbb{1}$. It is shown in [5, Thm. 5.13] that any Witt class contains a unique (up to braided equivalence) completely anisotropic representative. While specific Witt classes can be difficult to compare in practice, having a completely anisotropic representative is particularly useful. A fusion category \mathcal{C} is called *simple* if \mathcal{C} has no non-trivial fusion subcategories. There are examples of completely anisotropic categories which are not simple and vice versa. It is then interesting to consider the categories which are “minimal” in both senses, which leads to the concept of *property S* [5, Sec. 5.4]. A non-degenerate braided fusion category \mathcal{C} has property S if it is completely anisotropic, simple and unpointed. The subgroup of \mathcal{W} generated by the categories with property S is denoted by \mathcal{W}_S .

3. Categorical data and local modules of $\mathfrak{so}(2r)_{2r}$

In this section, we set up notations and provide the categorical data. We will also discuss basic properties of the local modules of the quantum group modular categories $\mathfrak{so}(2r)_{2r}$.

3.1. Categorical data of $\mathfrak{so}(2r)_{2r}$

Quantum groups give prominent examples of modular categories whose origin traces back to the dawn of the subject [9, 15]. For any simple Lie algebra \mathfrak{g} over \mathbb{C} and a positive integer k called the *level*, one gets a modular category \mathfrak{g}_k by taking the semisimplification of the tilting module category of the quantum group $U_q(\mathfrak{g})$ specialized at a root of unity q determined by \mathfrak{g} and k . The reader is referred to [1, 25] for details.

Let $r \geq 3$ be an integer and \mathcal{C}_r be the quantum group modular category $\mathfrak{so}(2r)_{2r}$. In this section, we study the structure of the Witt subgroup generated by these categories using the signature homomorphism (see (2.5)). Necessary data and notation is given below. For more details, see, for example, [1, 12, 25].

- Orthonormal basis for the inner product space $(\mathbb{R}^r, (\cdot|\cdot)) : \{e_1, \dots, e_r\}$.
- The set of positive roots: $\Delta_+ = \{e_j \pm e_k | 1 \leq j < k \leq r\}$. Root lattice: Ω . Coroot lattice: Ω^\vee .
- Half sum of positive roots: $\rho = (r-1)e_1 + (r-2)e_2 + \dots + e_{r-1}$.

- Fundamental weights: $\omega_j = \sum_{i=1}^j e_i$, $1 \leq j \leq r-2$; $\omega_{r-1} = \frac{1}{2} \sum_{i=1}^{r-1} e_i - \frac{1}{2} e_r$, $\omega_r = \frac{1}{2} \sum_{i=1}^r e_i$.
- Dual Coxeter number: $h^\vee = 2r-2$. The set of dominant weights: Φ_+ . Weight lattice: \mathfrak{P} .
- The fundamental alcove \mathfrak{A}_r is in one-to-one correspondence with the set of simple objects of \mathcal{C}_r .

$$\mathfrak{A}_r = \{\lambda \in \Phi_+ : (\lambda|e_1 + e_2) \leq 2r\} = \text{Irr}(\mathcal{C}_r). \quad (3.8)$$

- Quantum parameter: $q = \exp\left(\frac{\pi i}{(2r+h^\vee)}\right) = \exp\left(\frac{\pi i}{4r-2}\right)$. Twist of simple objects:

$$\theta_\lambda = q^{(\lambda|\lambda+2\rho)}, \quad \forall \lambda \in \mathfrak{A}_r. \quad (3.9)$$

- First central charge:

$$\xi_1(\mathcal{C}_r) = \exp\left(\frac{\pi i r^2}{4}\right). \quad (3.10)$$

Remark 3.1. We discuss the case when $r=2$ here, and will not include this case in the rest of the paper. The Lie algebra $\mathfrak{so}(4) \cong \mathfrak{su}(2) \times \mathfrak{su}(2)$ is not simple, but one can define, for completeness, $\mathfrak{so}(4)_4 := \mathfrak{su}(2)_4 \boxtimes \mathfrak{su}(2)_4$. According to [5, 6.4(4)], $[\mathfrak{so}(4)_4] = [\mathfrak{su}(2)_2]^2 = [\mathcal{C}(\mathbb{Z}/3\mathbb{Z}, \mathbb{Q})]^2$ with $Q(a) = e^{2\pi i a^2/3}$. In particular, $[\mathfrak{so}(4)_4]^2 = [\text{Vec}]$ in the Witt group, consistent with the $r \geq 3$ cases.

In Section 4, we will need the following auxiliary function. We adopt the standard notation and write the floor and ceiling functions as $x \mapsto \lfloor x \rfloor, x \mapsto \lceil x \rceil$ respectively.

Lemma 3.2. For any integers $r \geq 3$ and $j \geq 1$, define $\mathfrak{d}_r(j) := |\{\alpha \in \Delta_+ : (\alpha|\rho) = j\}|$. Then

$$\mathfrak{d}_r(j) = \begin{cases} r - \lfloor \frac{j}{2} \rfloor & \text{if } 1 \leq j \leq r-1, \\ r - \lceil \frac{j+1}{2} \rceil & \text{if } r \leq j \leq 2r-3, \\ 0 & \text{otherwise.} \end{cases} \quad (3.11)$$

Proof. Let $\alpha \in \Delta_+$ be a positive root, there are two cases. If $\alpha = e_a + e_b$ for some $1 \leq a < b \leq r$, $(\alpha|\rho) = 2r - (a+b)$, then $1 \leq (\alpha|\rho) \leq 2r-3$; if $\alpha = e_a - e_b$ for some $1 \leq a < b \leq r$, $(\alpha|\rho) = b-a$, then $1 \leq b-a \leq r-1$. Therefore, $\mathfrak{d}_r(j) = 0$ for all $j > 2r-3$.

Define

$$\begin{aligned} \mathfrak{l}_r^+(i) &= |\{(a, b) \in \mathbb{Z}^2 : 1 \leq a < b \leq r, a+b = i\}|, \\ \mathfrak{l}_r^-(i) &= |\{(a, b) \in \mathbb{Z}^2 : 1 \leq a < b \leq r, b-a = i\}|. \end{aligned}$$

For $1 \leq j \leq 2r-3$, we have:

$$\mathfrak{d}_r(j) = \mathfrak{l}_r^+(2r-j) + \mathfrak{l}_r^-(j).$$

It's clear by induction that

$$\mathfrak{l}_r^+(j) = \begin{cases} \lfloor \frac{j-1}{2} \rfloor & 3 \leq j \leq r, \\ \lceil \frac{2r-j}{2} \rceil & r+1 \leq j \leq 2r-1, \end{cases}$$

and

$$\mathfrak{l}_r^-(j) = \begin{cases} r-j & 1 \leq j \leq r-1, \\ 0 & r \leq j \leq 2r-3. \end{cases}$$

Therefore, if $1 \leq j \leq r-1$, then $\mathfrak{d}_r(j) = r-j + \lfloor \frac{j}{2} \rfloor = r - \lfloor \frac{j}{2} \rfloor$; if $r \leq j \leq 2r-3$, then we have $\mathfrak{d}_r(j) = \lceil \frac{2r-j-1}{2} \rceil = r - \lceil \frac{j+1}{2} \rceil$. \square

Lemma 3.3. For any integer $r \geq 3$, let $S_r = \{1 \leq j \leq 2r - 3 : \mathfrak{d}_r(j) \cdot j \equiv 1 \pmod{2}\}$. Then $|S_r|$ is even.

Proof. From (3.11), for any $r \geq 3$, let $k = (r - r \bmod 4)/4$, then

$$S_r = \begin{cases} \{4m + 3, 4n + 1 : 0 \leq m \leq k - 1, k \leq n \leq 2k - 1\} & \text{if } r \equiv 0 \pmod{4}, \\ \{4m + 1, 4n + 3 : 0 \leq m \leq k - 1, k \leq n \leq 2k - 1\} & \text{if } r \equiv 1 \pmod{4}, \\ \{4m + 3, 4n + 1 : 0 \leq m \leq k - 1, k + 1 \leq n \leq 2k\} & \text{if } r \equiv 2 \pmod{4}, \\ \{4m + 1, 4n + 3 : 0 \leq m \leq k, k \leq n \leq 2k\} & \text{if } r \equiv 3 \pmod{4}. \end{cases}$$

In any of the cases above, $|S_r|$ is even, so we are done. \square

For simplicity, we adopt the following conventions. For any positive integer n , we set $\zeta_n := \exp\left(\frac{2\pi i}{n}\right)$, and we use \mathbb{Q}_n to denote the cyclotomic field $\mathbb{Q}(\zeta_n)$. For any $m \in \mathbb{N}$ and k coprime to m , we use σ_k to denote the element in $\text{Gal}(\mathbb{Q}_m/\mathbb{Q})$ sending ζ_m to ζ_m^k . If m is a positive odd integer, and $a \in \mathbb{Z}$, then we denote the *Jacobi symbol* of a modulo m by $\left(\frac{a}{m}\right)_J$.

Lemma 3.4. Let r and u be positive integers such that $8(2r - 1)|u$. Then for any $k \in \mathbb{Z}$ with $\gcd(k, u) = 1$, and any $j \in \mathbb{Z}$, we have

$$\sigma_k\left(\sin\left(\frac{j\pi}{4r-2}\right)\right) = \left(\frac{-1}{k}\right)_J \sin\left(\frac{kj\pi}{4r-2}\right). \quad (3.12)$$

in the cyclotomic field \mathbb{Q}_u .

Proof. The assumption that $8(2r - 1)|u$ implies both ζ_{4r-2} and i are in \mathbb{Q}_u . Since k is odd, $\sigma_k(i) = \left(\frac{-1}{k}\right)_J i$. Now the lemma follows from $\sin\left(\frac{j\pi}{4r-2}\right) = \frac{\zeta_{4r-2}^j - \zeta_{4r-2}^{-j}}{2i}$. \square

Recall that for a ribbon fusion category \mathcal{C} , $\text{ord}(T_{\mathcal{C}}) = \text{lcm}\{\text{ord}(\theta_X) \mid X \in \text{Irr}(\mathcal{C})\}$ (see Section 2.2).

Lemma 3.5. For any integer $r \geq 3$, let $N_r = \text{ord}(T_{\mathcal{C}_r})$. Then we have $N_r = 2^s(2r - 1)$ for some integer $0 \leq s \leq 4$, and $\sqrt{\dim(\mathcal{C}_r)} \in \mathbb{Q}_{N_r}$.

Proof. Since $2e_1, \omega_r \in \mathfrak{A}_r$ (see (3.8)), by (3.9) we have

$$\begin{aligned} \theta_{2e_1} &= q^{(2e_1|2e_1+2\rho)} = q^{4r} = -\exp\left(\frac{\pi i}{2r-1}\right), \\ \theta_{\omega_r} &= q^{(\omega_r|\omega_r+2\rho)} = q^{\frac{(2r-1)r}{4}} = \exp\left(\frac{r\pi i}{8}\right). \end{aligned}$$

Moreover, since for any $\lambda \in \mathfrak{A}_r$, $(\lambda|\lambda + 2\rho) \in \frac{1}{4}\mathbb{Z}$, $\theta_\lambda = q^{(\lambda|\lambda+2\rho)}$ is $16(2r - 1)$ -th root of unity. Therefore, if r is even, then $2r - 1 \mid N_r \mid 16(2r - 1)$. When r is odd, we have $16(2r - 1) \mid N_r \mid 16(2r - 1)$, and so $N_r = 16(2r - 1)$. This proves the first part of the lemma.

By [21, Thm. 5.5], $d_\lambda \in \mathbb{Q}_{N_r}$ for any $\lambda \in \mathfrak{A}_r$, which implies $\tau_1(\mathcal{C}_r) \in \mathbb{Q}_{N_r}$. Moreover, by (3.10), when r is even, $\xi_1(\mathcal{C}_r) = \pm 1 \in \mathbb{Z} \subset \mathbb{Q}_{N_r}$, and when r is odd, we have $\xi_1(\mathcal{C}_r) = \exp\left(\frac{\pi i}{4}\right) \in \mathbb{Q}_{N_r}$. Therefore, in light of (2.3), $\sqrt{\dim(\mathcal{C}_r)} = \tau_1(\mathcal{C}_r)/\xi_1(\mathcal{C}_r) \in \mathbb{Q}_{N_r}$. \square

Remark 3.6. In the rest of the paper, the N_r 's are used to bound the conductors of the cyclotomic fields in which we perform explicit computations. The key information to extract from the above lemma is that $(2r - 1)$ is the largest odd factor of N_r , while the exact value of N_r is not needed for our purpose.

3.2. Local modules of \mathcal{C}_r

In order to study the Witt subgroup generated by \mathcal{C}_r , it is natural to find connected étale algebras in it, and to study the Witt class of the corresponding local module category (or condensation), as is explained in Section 2.3. It turns out that \mathcal{C}_r contains a Tannakian symmetric fusion subcategory, and the corresponding local module admits further decomposition when r is odd.

Details on the above discussions are provided in the following lemma. Recall that a fusion category is unpointed if it has only 1 invertible object, and the semion modular category is defined in Section 2.2.

For any fusion category \mathcal{C} and object $U \in \mathcal{C}$, we denote by $\langle U \rangle$ the full fusion subcategory of \mathcal{C} generated by all the subobjects of U . If w is a collection of Witt classes or Witt subgroups, then $\langle w \rangle$ is the subgroup of \mathcal{W} generated by w .

Lemma 3.7. *For any $r \geq 3$, we have*

$$\begin{cases} (\mathcal{C}_r)_{\text{pt}} \supset \text{Rep}(\mathbb{Z}/2\mathbb{Z}), & \text{if } r \text{ is odd;} \\ (\mathcal{C}_r)_{\text{pt}} \cong \text{Rep}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}), & \text{if } r \text{ is even.} \end{cases}$$

Let $A_r = \text{Fun}(\mathbb{Z}/2\mathbb{Z})$ for odd r and $A_r = \text{Fun}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ for even r be the corresponding connected étale algebras, then we have the following decomposition for the local modules

$$(\mathcal{C}_r)_{A_r}^0 \cong \begin{cases} \mathbf{Sem} \boxtimes \mathcal{D}_r, & \text{if } r \text{ is odd;} \\ \mathcal{D}_r, & \text{if } r \text{ is even,} \end{cases}$$

where \mathcal{D}_r is an unpointed modular category.

Proof. Let $\lambda_1 = 2r\omega_{r-1}$, $\lambda_2 = 2r\omega_1$, and $\lambda_3 = 2r\omega_r$. One can check easily that $\lambda_j \in \mathfrak{A}_r$ for $1 \leq j \leq 3$, and by [26, 27], these are all the nontrivial invertible objects in \mathcal{C}_r . Moreover, when r is odd, $\lambda_1^{\otimes j} = \lambda_j$ for $j = 1, 2, 3$, and when r is even, $\lambda_i^2 = \mathbb{1}$ and $\lambda_1 \otimes \lambda_2 = \lambda_3$ (see, for example, [26, Lem. 2]).

Therefore, $(\mathcal{C}_r)_{\text{pt}} \cong \mathcal{C}(\mathbb{Z}/4\mathbb{Z}, Q_1)$ for odd r , $(\mathcal{C}_r)_{\text{pt}} \cong \mathcal{C}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, Q_2)$ for even r , where Q_1 and Q_2 are quadratic forms determined by the following twist values:

$$\begin{aligned} \theta_{\lambda_1} &= q^{(4r\omega_{r-1}-2r\omega_r|4r\omega_{r-1}-2r\omega_r+2\rho)} = q^{2r^2(r-1)+r^2} = \exp\left(\frac{r^2}{2}\pi i\right), \\ \theta_{\lambda_2} &= q^{(2r\omega_1|2r\omega_1+2\rho)} = q^{2r(4r-2)} = \exp(2r\pi i) = 1, \\ \theta_{\lambda_3} &= q^{(2r\omega_r|2r\omega_r+2\rho)} = q^{r^2(2r-1)} = \exp\left(\frac{r^2}{2}\pi i\right). \end{aligned} \quad (3.13)$$

When r is odd, the fusion subcategory of \mathcal{C}_r generated by the object λ_2 is equivalent to the symmetric fusion category $\text{Rep}(\mathbb{Z}/2\mathbb{Z})$, which contains the connected étale algebra $A_r = \mathbb{1} \oplus \lambda_2 = \text{Fun}(\mathbb{Z}/2\mathbb{Z})$. Since $\lambda_1 \otimes \lambda_2 = \lambda_3$, by (2.1), we have

$$\theta_{\lambda_3} \cdot \text{id}_{\lambda_1 \otimes \lambda_2} = \theta_{\lambda_3} \cdot \text{id}_{\lambda_3} = \theta_{\lambda_1 \otimes \lambda_2} = \beta_{\lambda_2, \lambda_1} \circ \beta_{\lambda_1, \lambda_2} \circ (\theta_{\lambda_1} \cdot \text{id}_{\lambda_1} \otimes \theta_{\lambda_2} \cdot \text{id}_{\lambda_2}),$$

where for $j = 1, 2, 3$, θ_{λ_j} refers to the twist values above, and $\theta_{\lambda_1 \otimes \lambda_2}$ denotes the twist isomorphism. Therefore, we have $\beta_{\lambda_2, \lambda_1} \circ \beta_{\lambda_1, \lambda_2} = \text{id}_{\lambda_1 \otimes \lambda_2}$, so λ_1 is in the centralizer of $\text{Rep}(\mathbb{Z}/2\mathbb{Z})$. Similarly, we have $\lambda_3 \in \text{Rep}(\mathbb{Z}/2\mathbb{Z})'$.

Let $F : \mathcal{C}_r \rightarrow (\mathcal{C}_r)_{A_r}$, $X \mapsto X \otimes A_r$ be the free module functor, which is a monoidal functor (see [5, Sec. 3.3]). Let $V := F(\lambda_1)$, then $V \otimes V = F(\lambda_1 \otimes \lambda_1) = F(\mathbb{1})$ (note that $F(\mathbb{1})$ is the tensor unit of $(\mathcal{C}_r)_{A_r}^0$), i.e., V is of order 2. By the above discussions, we have $V \in (\mathcal{C}_r)_{A_r}^0 = (\mathcal{C}_r)_{\mathbb{Z}/2\mathbb{Z}}^0$. Moreover, by [14, Thm. 1.8], we have

$$d_V = d_{\lambda_1} = 1,$$

and by [14, Thm. 1.17], $\theta_V = \theta_{\lambda_1} = i$. Therefore, V generates a modular subcategory in $(\mathcal{C}_r)_{A_r}^0$ which is equivalent to **Sem**. Thus, by the double centralizer theorem [18, Thm. 4.2], we have $(\mathcal{C}_r)_{A_r}^0 \cong \mathbf{Sem} \boxtimes \mathcal{D}_r$, where \mathcal{D}_r is the centralizer of **Sem** in $(\mathcal{C}_r)_{A_r}^0$. In particular, $\mathcal{D}_r \cap \mathbf{Sem} = \langle F(\mathbb{1}) \rangle$.

When r is even, $\theta_{\lambda_j} = 1$ for $j = 1, 2, 3$, so (2.1) implies that $(\mathcal{C}_r)_{\text{pt}}$ is equivalent to the symmetric fusion category $\text{Rep}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$, which contains the connected étale algebra $A_r = \mathbb{1} \oplus \lambda_1 \oplus \lambda_2 \oplus \lambda_3 = \text{Fun}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. In this case, we can simply set $\mathcal{D}_r := (\mathcal{C}_r)_{A_r}^0$.

It remains to show that \mathcal{D}_r is unpointed for any r . Consider the forgetful functor $G : (\mathcal{C}_r)_{A_r} \rightarrow \mathcal{C}_r$, which is the adjoint of F (see [14]). On the one hand, by [14, Thm. 1.18], any $X \in \text{Irr}((\mathcal{D}_r)_{\text{pt}})$ must satisfy $d_{G(X)} = d_{A_r} \in \mathbb{Z}$. On the other hand, by [29], all the objects in \mathcal{C}_r with integral dimension are contained in $(\mathcal{C}_r)_{\text{pt}}$. Moreover, it is easy to see that any $X \in (\mathcal{C}_r)_{A_r}$ is a subobject of $F(G(X))$. Therefore, for any $X \in \text{Irr}((\mathcal{D}_r)_{\text{pt}})$, we have $X \in F((\mathcal{C}_r)_{\text{pt}})$.

By the above discussions, when r is odd, $F((\mathcal{C}_r)_{\text{pt}}) = \langle F(\lambda_1) \rangle \cong \mathbf{Sem}$; when r is even, $F((\mathcal{C}_r)_{\text{pt}}) = \langle F(\mathbb{1}) \rangle$ (recall that $F(\mathbb{1})$ is the tensor unit of $(\mathcal{C}_r)_{A_r}^0$). Therefore, $\{F(\mathbb{1})\} \subset \text{Irr}((\mathcal{D}_r)_{\text{pt}}) \subset \text{Irr}(F((\mathcal{C}_r)_{\text{pt}}) \cap \mathcal{D}_r) = \{F(\mathbb{1})\}$. \square

In particular, by [8], Lemma 3.7 implies that $\text{FPdim}(\mathcal{C}_r) = 8\text{FPdim}(\mathcal{D}_r)$ if r is odd, and $\text{FPdim}(\mathcal{C}_r) = 16\text{FPdim}(\mathcal{D}_r)$ if r is even. Moreover, we immediately see that

$$[\mathcal{C}_r] = \begin{cases} [\mathbf{Sem} \boxtimes \mathcal{D}_r] & \text{if } r \text{ is odd,} \\ [\mathcal{D}_r] & \text{if } r \text{ is even,} \end{cases} \quad (3.14)$$

Now the conformal embedding $\mathfrak{so}(m)_n \times \mathfrak{so}(n)_m \subset \mathfrak{so}(mn)_1$ (see, for example, [5]) implies that

$$[\mathcal{C}_r]^2 = \begin{cases} [\mathbf{Sem}]^2 & \text{if } r \text{ is odd,} \\ [\text{Vec}] & \text{if } r \text{ is even,} \end{cases}$$

and so for any $r \geq 3$, we have

$$[\mathcal{D}_r]^2 = [\text{Vec}]. \quad (3.15)$$

4. The Witt subgroup generated by \mathcal{D}_r

In this section, we study the Witt subgroup generated by $[\mathcal{D}_r]$ using the signature homomorphism (2.5). By [28, Lem. 2.4], \mathcal{D}_r is pseudounitary, i.e., $\dim(\mathcal{D}_r) = \text{FPdim}(\mathcal{D}_r)$, which is a quotient of $\dim(\mathcal{C}_r)$ by 8 or 16 (see above). For simplicity, we set

$$D_r := \sqrt{\dim(\mathcal{D}_r)} \quad (\text{positive square root}). \quad (4.16)$$

To compute the signature, we will combine the lemmas in Section 3.1 with the well-known formulae of $\sqrt{\dim(\mathcal{C}_r)}$ in terms of trigonometric functions [1, Thm. 3.3.20]. (Note that in [4, Thm. 3], a formula for the global dimension is provided, but to compute the signature, one needs to take the square root). As a reminder, the definition of the function $\mathfrak{d}_r(j)$ can be found in Lemma 3.2.

Lemma 4.1. *Let $r \geq 3$ be odd. Then $D_r \in \mathbb{Q}_{8N_r}$ and*

$$D_r = Y \sqrt{2r-1} \left(\prod_{j=1}^{2r-3} \sin \frac{j\pi}{4r-2} \right)^{-\mathfrak{d}_r(j)}, \quad (4.17)$$

where $Y = 2^{\frac{-2r^2+3r+1}{2}} \cdot (2r-1)^{\frac{r-1}{2}} \in \mathbb{Q}$.

Proof. Recall that when r is odd, $8\dim(\mathcal{D}_r) = \dim(\mathcal{C}_r)$. Therefore, $D_r \in \mathbb{Q}_{8N_r}$ follows from [Lemma 3.5](#) and the fact that $\sqrt{2} \in \mathbb{Q}_8$. According to [1, Thm. 3.3.20] and the information on positive roots in [Section 3.1](#), we have

$$\begin{aligned} D_r &= \frac{1}{2\sqrt{2}} \sqrt{|\mathfrak{P}/((2r + h^\vee)\mathfrak{Q}^\vee)|} \prod_{\alpha \in \Delta_+} \left(2 \sin \left(\frac{(\alpha|\rho)}{2r + h^\vee} \pi \right) \right)^{-1} \\ &= Y\sqrt{2r-1} \prod_{\alpha \in \Delta_+} \left(\sin \left(\frac{(\alpha|\rho)}{4r-2} \pi \right) \right)^{-1}, \end{aligned}$$

and we are done by definition. \square

Lemma 4.2. *Let $r \geq 4$ be even. Then $D_r \in \mathbb{Q}_{N_r}$ and*

$$D_r = Z \left(\prod_{j=1}^{2r-3} \sin \frac{j\pi}{4r-2} \right)^{-\mathfrak{d}_r(j)}, \quad (4.18)$$

where $Z = 2^{\frac{(3-2r)r}{2}} \cdot (2r-1)^{\frac{r}{2}} \in \mathbb{Q}$.

Proof. Note that when r is even, $16\dim(\mathcal{D}_r) = \dim(\mathcal{C}_r)$. Then the statement of the lemma follows from the similar argument as in [Lemma 4.1](#) and [Lemma 3.5](#). \square

The above lemmas imply the following periodicity result on the signature, which is important to the theorems below.

Proposition 4.3. *Let $r \geq 3$ be any integer. If $k \equiv k' \pmod{4r-2}$ and $\gcd(k, 4r-2) = 1$, then $\sigma_k(D_r) = \sigma_{k'}(D_r)$. In particular, $\varepsilon_{\mathcal{D}_r}(\sigma_k) = \varepsilon_{\mathcal{D}_r}(\sigma_{k'})$.*

Proof. From [Lemma 3.5](#), we have k, k' are both coprime to $8N_r$, so the signatures are well defined. Assume r is odd. When $k \equiv k' \pmod{8r-4}$, from (3.12) and the fact that $|\Delta_+| = r(r-1)$ is even, we have

$$\sigma_{k'}(D_r) = \left(\left(\frac{-1}{k'} \right)_J \left(\frac{-1}{k} \right)_J \right)^{|\Delta_+|} \sigma_k(D_r) = \sigma_k(D_r).$$

Note that $\sum_{j=1}^{2r-3} \mathfrak{d}_r(j) = |\Delta_+|$. Therefore, it suffices to consider the case when $k' = 4r-2+k$. Without loss of generality, assume $k \equiv 1 \pmod{4}$, $k' \equiv 3 \pmod{4}$. By assumption, r is odd, so $2r-1 \equiv 1 \pmod{4}$, and we have $\sigma_k(\sqrt{2r-1}) = \sigma_{k'}(\sqrt{2r-1})$ since $\sqrt{2r-1} \in \mathbb{Q}_{2r-1}$ [33]. By (4.17), [Lemmas 3.3](#) and [3.4](#), we have

$$\begin{aligned} \sigma_{k'}(D_r) &= \left(\frac{-1}{k'} \right)_J^{|\Delta_+|} Y\sqrt{2r-1} \prod_{j=1}^{2r-3} \left(\sin \frac{(k+4r-2)j\pi}{4r-2} \right)^{-\mathfrak{d}_r(j)} \\ &= Y\sqrt{2r-1} \prod_{j=1}^{2r-3} \left((-1)^j \sin \frac{kj\pi}{4r-2} \right)^{-\mathfrak{d}_r(j)} \\ &= (-1)^{|\mathcal{S}_r|} \sigma_k(D_r) \\ &= \sigma_k(D_r). \end{aligned}$$

When r is even, the proof is similar.

In the following, we determine the structure of the Witt subgroup generated by families of $[\mathcal{D}_r]$'s. The key point is to show that there are no nontrivial relations in the groups under study. To achieve this goal, we use special Galois elements to distinguish the signature homomorphisms of the $[\mathcal{D}_r]$'s, and the parity of r determines the way to find such Galois elements. Naturally, from now on, we separate cases according to the parity of r .

4.1. The case when r is odd

In this subsection, let $r \geq 3$ be an odd integer.

Proposition 4.4. *For any positive integer $r \equiv 5 \pmod{8}$, we have $\varepsilon_{\mathcal{D}_r}(\sigma_r) = -1$.*

Proof. From Lemma 3.5, $\gcd(r, 8N_r) = \gcd(r, 2r - 1) = 1$. Let $r = 4k + 1$ for some odd integer k . By (3.11), it is clear that $\mathfrak{d}_r(j)$ is odd when $j \in \{4m + 1, 4(m + 1), 4n + 2, 4n + 3 \mid 0 \leq m \leq k - 1, k \leq n \leq 2k - 1\}$. By Lemma 4.1, [20, Lem. 6.2, 6.3] and the quadratic reciprocity, we have:

$$\begin{aligned} \varepsilon_{\mathcal{D}_r}(\sigma_r) &= \left(\frac{r}{2r-1}\right)_J (-1)^{\sum_{m=0}^{k-1} \left(\left\lfloor \frac{(4m+1)r}{4r-2} \right\rfloor + \left\lfloor \frac{4(m+1)r}{4r-2} \right\rfloor\right) + \sum_{n=k}^{2k-1} \left(\left\lfloor \frac{4n+2}{4r-2} \right\rfloor + \left\lfloor \frac{(4n+3)r}{4r-2} \right\rfloor\right)} \\ &= \left(\frac{-1}{r}\right)_J (-1)^{\sum_{m=0}^{k-1} (m+m+1) + \sum_{n=k}^{2k-1} (n+n)} = (-1)^k = -1. \end{aligned}$$

Now we are ready to determine the subgroup of \mathcal{W} generated by $[\mathcal{D}_r]$ for a collection of odd r 's. Let $\{a_j\}_{j \geq 1}$ be a sequence of prime numbers such that $a_j \equiv 9 \pmod{16}$ and $a_j < a_{j+1}$. Such a sequence exists due to the Dirichlet prime number theorem. Let $r_j = \frac{a_j+1}{2}$, then $r_j \equiv 5 \pmod{8}$ and $a_j = 2r_j - 1$.

Theorem 4.5. *The Witt subgroup generated by $\{[\mathcal{D}_{r_j}]\}_{j \geq 1}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}^{\oplus \mathbb{N}}$.*

Proof. Since $[\mathcal{D}_r]$ has order 2 in the Witt group (see (3.15)), it suffices to show that no finite product of distinct $[\mathcal{D}_{r_j}]$ yields $[\text{Vec}]$. To that end, let $\mathcal{D} := \boxtimes_{i=1}^n \mathcal{D}_{r_{j_i}}$ for some subsequence $1 \leq j_1 < \dots < j_n$, and we compute one of its signature values as follows.

From Lemma 3.5 and Lemma 4.1, we have $\sqrt{\dim(\mathcal{D})} \in \mathbb{Q}_N$, where $N = \text{lcm}_{1 \leq i \leq n} \{8N_{r_{j_i}}\}$. Let $K = \text{lcm}_{2 \leq i \leq n} \{2a_{j_i}\}$, then $\gcd(a_{j_1}, K) = 1$ by construction. Hence, by Bezout's identity, there exist $x, y \in \mathbb{Z}$ such that

$$xa_{j_1} + yK = 1.$$

Let $k = -(r_{j_1} - 1)xa_{j_1} + r_{j_1}$. Since $2 \mid (r_{j_1} - 1)$, we have

$$k \equiv 1 \pmod{K}, \quad k \equiv r_{j_1} \pmod{2a_{j_1}}. \quad (4.19)$$

In particular, by Lemma 3.5 $\gcd(k, N) = 1$.

Since $2a_{j_i} = 4r_{j_i} - 2$, by Proposition 4.3 and Proposition 4.4, there exists $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, such that $\sigma|_{\mathbb{Q}_N} = \sigma_k$, and

$$\varepsilon_{\mathcal{D}_{r_{j_1}}}(\sigma) = -1 \text{ and } \varepsilon_{\mathcal{D}_{r_{j_i}}}(\sigma) = 1 \ (i \neq 1).$$

This implies that $\varepsilon_{\mathcal{D}}(\sigma) = -1$. Therefore, by [20, Thm. 3.5], $[\mathcal{D}] \neq [\text{Vec}]$. □

Consider $\mathcal{I} := (\mathfrak{sl}_2)_2$. It is an Ising modular category, i.e., \mathcal{I} is not pointed and $\text{FPdim}(\mathcal{I}) = 4$. It is extensively studied in [8, Appendix B]. Since $[\mathcal{I}]^2 \in \mathcal{W}_{\text{pt}}$ and both \mathcal{W}_{pt} and $\langle [\mathcal{I}] \rangle$ are contained in the 2-torsion part of \mathcal{W} (see [5]), it is natural to compare these Witt subgroups with the one we just studied. Let H denote the group generated by $\{[\mathcal{D}_{r_j}]\}_{j \geq 1}$.

Theorem 4.6. *We have $H \cap \langle \mathcal{W}_{\text{pt}}, [\mathcal{I}] \rangle = \{[\text{Vec}]\}$.*

Proof. It suffices to show product of any finite set in $\{[\mathcal{D}_{r_j}]\}$ intersect trivially with $\langle \mathcal{W}_{\text{pt}}, [\mathcal{I}] \rangle$. To that end, let $\mathcal{D} := \boxtimes_{i=1}^n \mathcal{D}_{r_{j_i}}$ for some $1 \leq j_1 < \dots < j_n$. If $[\mathcal{D}] \in H \cap \mathcal{W}_{\text{pt}}$ is nontrivial, there exists a finite abelian group L and a non-degenerate quadratic form $Q: L \rightarrow \mathbb{C}^\times$ such that the corresponding pointed modular category $\mathcal{L} = \mathcal{C}(L, Q)$ satisfies $[\mathcal{L}] = [\mathcal{D}]$ in \mathcal{W} . We compare their signatures as follows.

Let $h = |L|$, $N = h \cdot \text{lcm}_{1 \leq i \leq n} \{8N_{r_{j_i}}\}$, then both \sqrt{h} and $\sqrt{\dim(\mathcal{D})}$ are in the field \mathbb{Q}_N . We write $h = h_1 h_2$, where $\gcd(h_1, a_{j_1}) = 1$, $h_2 = a_{j_1}^s$ for some $s \geq 1$. Let $K = h_1 \cdot \text{lcm}_{2 \leq i \leq n} \{2a_{j_i}\}$, we have $\gcd(a_{j_1}, K) = 1$. Hence, from Bezout's identity, there exist $x, y \in \mathbb{Z}$, such that:

$$xa_{j_1} + yK = 1$$

Let $k = -(r_{j_1} - 1)xa_{j_1} + r_{j_1}$, since $2|(r_{j_1} - 1)$, we have:

$$k \equiv 1 \pmod{K}, \quad k \equiv r_{j_1} \pmod{2a_{j_1}}.$$

Again by Lemma 3.5, $\gcd(k, N) = 1$. By Proposition 4.3 and Proposition 4.4, there exists $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, such that $\sigma|_{\mathbb{Q}_N} = \sigma_k$ and

$$\varepsilon_{\mathcal{D}_{r_{j_1}}}(\sigma) = -1, \text{ and } \varepsilon_{\mathcal{D}_{r_{j_i}}}(\sigma) = 1 \ (i \neq 1),$$

which implies $\varepsilon_{\mathcal{D}}(\sigma) = -1$.

Since $k \equiv 1 \pmod{4}$, $k \equiv 1 \pmod{h_1}$ and $r_{j_1} \equiv 1 \pmod{4}$, so by [20, Lem. 6.2], we have

$$\begin{aligned} \varepsilon_{\mathcal{L}}(\sigma) &= \text{sgn}\left(\sigma_k\left(\sqrt{h_1 h_2}\right)\right) = \left(\frac{k}{h_1}\right)_J \left(\frac{k}{h_2}\right)_J = \left(\frac{k}{a_{j_1}}\right)_J^s \\ &= \left(\frac{r_{j_1}}{2r_{j_1} - 1}\right)_J^s = \left(\frac{2r_{j_1} - 1}{r_{j_1}}\right)_J^s = \left(\frac{-1}{r_{j_1}}\right)_J^s = 1. \end{aligned}$$

Therefore, $\varepsilon_{\mathcal{D}} \neq \varepsilon_{\mathcal{L}}$, which contradicts to [20, Thm. 3.5]. So $H \cap \mathcal{W}_{\text{pt}}$ is trivial.

Since $[\mathcal{I}]^2 \in \mathcal{W}_{\text{pt}}$, if $[\mathcal{D}] = [\mathcal{I}]^m [\mathcal{H}']$ for some $[\mathcal{H}'] \in \mathcal{W}_{\text{pt}}$, then by the above discussions, we must have m is odd. Let $\kappa = \xi_1(\mathcal{I})$, then κ is a primitive 16-th root of unity. Moreover, it is well-known that the first central charge of a pointed modular category is an 8-th root of unity (see [7]). Consequently, there exists some $\ell \in \mathbb{Z}$ such that $\xi_1(\mathcal{H}') = \kappa^\ell$. Moreover, by (3.14) and the multiplicativity of the central charge [8], we have $\xi_1(\mathcal{D}_r) = 1$. Therefore,

$$1 = \xi_1(\mathcal{D}) = \xi_1(\mathcal{I})^m \xi_1(\mathcal{H}') = \kappa^m \cdot \kappa^{2\ell} = \kappa^{m+2\ell}.$$

However, as m is odd, the right hand side can never be 1, so we get a contradiction. Thus, we must have $H \cap \langle \mathcal{W}_{\text{pt}}, [\mathcal{I}] \rangle = \{[\text{Vec}]\}$. \square

In view of (3.14), (3.15), and combining all the results above, we have the following corollary.

Corollary 4.7. *The image of $[\text{Vec}]$ has infinitely many square roots in $\mathcal{W}/\langle \mathcal{W}_{\text{pt}}, [\mathcal{I}] \rangle$, hence the same is true of $[\text{Sem}]^2$. \square*

4.2. The case when r is even

In this subsection, let $r \geq 4$ be an even integer.

Proposition 4.8. *Let $r \equiv 4 \pmod{8}$, $s \equiv 6 \pmod{8}$ we have*

$$\varepsilon_{\mathcal{D}_r}(\sigma_{2r+1}) = \varepsilon_{\mathcal{D}_s}(\sigma_{s-1}) = -1.$$

Proof. From Lemma 3.5, $\gcd(2r+1, N_r) = \gcd(2r+1, 2r-1) = 1$ and $\gcd(s-1, N_s) = \gcd(s-1, 2s-1) = 1$. Similar to the proof of Proposition 4.4, let $r = 4k$, $s = 4l+2$ for some odd integers k, l . By (3.11), it is clear that $\mathfrak{d}_r(j)$ is odd when $j \in \{4m+2, 4m+3, 4n, 4n+1 \mid 0 \leq m \leq k-1, k \leq n \leq 2k-1\}$ and $\mathfrak{d}_s(j)$ is odd when $j \in \{4m+2, 4m+3, 4n, 4n+1 \mid 0 \leq m \leq l-1, l+1 \leq n \leq 2l\}$. Since $2r+1 \equiv 1 \pmod{4}$, $l-1 \equiv 1 \pmod{4}$, by (4.18), [20, Lem. 6.1], we have:

$$\begin{aligned} \varepsilon_{\mathcal{D}_r}(\sigma_{2r+1}) &= (-1)^{\sum_{m=0}^{k-1} \left(\left\lfloor \frac{(4m+2)(2r+1)}{4r-2} \right\rfloor + \left\lfloor \frac{(4m+3)(2r+1)}{4r-2} \right\rfloor \right) + \sum_{n=k}^{2k-1} \left(\left\lfloor \frac{4n(2r+1)}{4r-2} \right\rfloor + \left\lfloor \frac{(4n+1)(2r+1)}{4r-2} \right\rfloor \right)} \\ &= (-1)^{\sum_{m=0}^{k-1} (2m+1+2m+1) + \sum_{n=k}^{2k-1} (2n+1+2n)} \\ &= (-1)^k = -1 \end{aligned}$$

and

$$\begin{aligned} \varepsilon_{\mathcal{D}_s}(\sigma_{s-1}) &= (-1)^{\sum_{m=0}^{l-1} \left(\left\lfloor \frac{(4m+2)(s-1)}{4r-2} \right\rfloor + \left\lfloor \frac{(4m+3)(s-1)}{4r-2} \right\rfloor \right) + \sum_{n=l+1}^{2l} \left(\left\lfloor \frac{4n(s-1)}{4r-2} \right\rfloor + \left\lfloor \frac{(4n+1)(s-1)}{4r-2} \right\rfloor \right)} \\ &= (-1)^{\sum_{m=0}^{l-1} (m+m) + \sum_{n=l+1}^{2l} (n-1+n)} \\ &= (-1)^l = -1. \end{aligned}$$

Let $\{b_j\}_{j \geq 1}$, $\{c_j\}_{j \geq 1}$ be two increasing sequences of prime numbers such that $b_j \equiv 7 \pmod{16}$ and $c_j \equiv 11 \pmod{16}$. Such sequences exist due to the Dirichlet prime number theorem. Let $r_j = \frac{b_j+1}{2}$, $s_j = \frac{c_j+1}{2}$, then $r_j \equiv 4 \pmod{8}$ and $s_j \equiv 6 \pmod{8}$.

Theorem 4.9. $\{[\mathcal{D}_{r_j}]\}_{j \geq 1}$ and $\{[\mathcal{D}_{s_j}]\}_{j \geq 1}$ each generate a group isomorphic to $\mathbb{Z}/2\mathbb{Z}^{\oplus \mathbb{N}}$ in the Witt group, and the intersection of these groups is trivial.

Proof. Similar to the argument as in Theorem 4.5, it suffices to show that no finite product of distinct $[\mathcal{D}_{r_j}]$ or $[\mathcal{D}_{s_j}]$ yields $[\text{Vec}]$. To that end, let $\mathcal{D} := \boxtimes_{i=1}^n \mathcal{D}_{r_{j_i}}$, and $\tilde{\mathcal{D}} := \boxtimes_{i=1}^n \mathcal{D}_{s_{l_i}}$ for arbitrary finite subsets of $\{r_j\}$ and $\{s_j\}$, respectively. Suppose $[\mathcal{D}] = [\tilde{\mathcal{D}}] = [\text{Vec}]$, we compare their signatures.

First, note that $\sqrt{\dim(\mathcal{D})} \in \mathbb{Q}_N$, $\sqrt{\dim(\tilde{\mathcal{D}})} \in \mathbb{Q}_{\tilde{N}}$, where $N = \text{lcm}_{1 \leq i \leq n} \{N_{r_{j_i}}\}$ and $\tilde{N} = \text{lcm}_{1 \leq i \leq n} \{\tilde{N}_{s_{l_i}}\}$. Let $K = \text{lcm}_{2 \leq i \leq n} \{2b_{j_i}\}$, $M = \text{lcm}_{2 \leq i \leq n} \{2c_{l_i}\}$, then $\gcd(b_{j_1}, K) = 1$, $\gcd(c_{l_1}, M) = 1$ by construction. Hence, by Bezout's identity, there exist $x, y, z, w \in \mathbb{Z}$ such that

$$xb_{j_1} + yK = 1 \quad zc_{l_1} + wM = 1.$$

Let $k = -(2r_{j_1})xb_{j_1} + 2r_{j_1} + 1$, $t = -(s_{l_1} - 2)zc_{l_1} + s_{l_1} - 1$. Since $2|2r_{j_1}$ and $2|s_{l_1} - 2$, we have

$$\begin{aligned} k &\equiv 1 \pmod{K}, \quad k \equiv r_{j_1} \pmod{2b_{j_1}}, \\ t &\equiv 1 \pmod{M}, \quad t \equiv s_{l_1} - 1 \pmod{2c_{l_1}}. \end{aligned}$$

Since $2b_{j_1} = 4r_{j_1} - 2$, $2c_{l_1} = 4s_{l_1} - 2$, we have $\gcd(k, N) = \gcd(t, \tilde{N}) = 1$ (Lemma 3.5). By Proposition 4.3 and Proposition 4.4, there exist $\sigma, \eta \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma|_{\mathbb{Q}_N} = \sigma_k$, $\eta|_{\mathbb{Q}_{\tilde{N}}} = \eta_t$

$$\varepsilon_{\mathcal{D}_{r_{j_1}}}(\sigma) = \varepsilon_{\mathcal{D}_{s_{l_1}}}(\eta) = -1 \text{ and } \varepsilon_{\mathcal{D}_{r_{j_i}}}(\sigma) = \varepsilon_{\mathcal{D}_{s_{l_i}}}(\eta) = 1 \text{ (} i \neq 1 \text{)}.$$

This implies that

$$\varepsilon_{\mathcal{D}}(\sigma) = \varepsilon_{\tilde{\mathcal{D}}}(\eta) = -1,$$

which contradicts [20, Thm. 3.5]. Moreover, by considering the products of the categories in two different families, and the fact that b_j, c_j are distinct primes, the trivial intersection follows from the same argument as above (consider the least common multiple for all $2b_{j_i}$'s and $2c_{i_i}$'s except $2b_{j_1}$). \square

Let H' denote the group generated by $\{[\mathcal{D}_{r_j}]\}_{j \geq 1}$ and $\{[\mathcal{D}_{s_j}]\}_{j \geq 1}$. Similar to Theorem 4.6, we have

Theorem 4.10. *We have $H' \cap \langle \mathcal{W}_{\text{pt}}, [\mathcal{I}] \rangle = \{[\text{Vec}]\}$.*

Proof. From the proof of Theorem 4.6, 4.9 and Proposition 4.8, it suffices to check for any j , $2r_j + 1 \equiv 1 \pmod{4}$, $s_j - 1 \equiv 1 \pmod{4}$ and $\left(\frac{2r_j+1}{2r_j-1}\right)_j = \left(\frac{s_j-1}{2s_j-1}\right)_j = 1$. Indeed, $\left(\frac{2r_j+1}{2r_j-1}\right)_j = \left(\frac{2}{2r_j-1}\right)_j = 1$ (since when $p \equiv \pm 1 \pmod{8}$, $\left(\frac{2}{p}\right)_j = 1$), and others are also easy to check. \square

5. Relation with Witt subgroup generated by $\mathfrak{so}(2r+1)_{2r+1}$

Let $\mathcal{B}_b = \mathfrak{so}(2b+1)_{2b+1}$, where $b > 1$ is an odd integer. In [20], the Witt subgroup generated by an infinite sequence of \mathcal{B}_b 's, denoted by $G_{\mathbf{p}}$, was studied. Here, \mathbf{p} is a sequence of odd primes satisfying certain congruence conditions in [20, Section 6.2]. It is shown in [20, Theorem 6.7] that $G_{\mathbf{p}}$ contains an elementary 2-group of infinite rank, so it is natural to compare it with the Witt subgroups in this paper.

In this section, we prove there is an infinite subgroup of the group generated by $[\mathcal{D}_r]$ with $r \equiv 4 \pmod{8}$ that intersects trivially with the group $G_{\mathbf{p}}$. The tool we use is still the signature homomorphism. Thus, we start with the square root of the global dimension of \mathcal{B}_b (cf. [20, Prop. 5.3])

$$B_b := \sqrt{\dim(\mathcal{B}_b)} = W\sqrt{b} \left(\prod_{l=1}^b \left(\sin \frac{(2l-1)\pi}{8b} \right) \prod_{j=1}^{2b-2} \left(\sin \frac{j\pi}{4b} \right)^{c_b(j)} \right)^{-1}, \quad (5.20)$$

where $W = \frac{b^{\frac{b-1}{2}}}{2^{b^2-b-1}} \in \mathbb{Q}$ and $c_b(j) = b - \lceil \frac{j}{2} \rceil$ for $1 \leq j \leq 2b-2$.

Lemma 5.1. *We have*

- (i) $B_b \in \mathbb{Q}_{16b}$.
- (ii) Let k be any integer such that $k \equiv 1 \pmod{4}$ and $\gcd(k, b) = 1$. For any $x \in \mathbb{Z}$, if we denote $k' = 8xb + k$, then $\varepsilon_{\mathcal{B}_b}(\sigma_{k'}) = (-1)^x \varepsilon_{\mathcal{B}_b}(\sigma_k)$.

Proof. Since $\sqrt{b} \in \mathbb{Q}_{4b}$, $\sin\left(\frac{j\pi}{4b}\right) \in \mathbb{Q}_{8b}$ and $\sin\left(\frac{(2l-1)\pi}{8b}\right) \in \mathbb{Q}_{16b}$, so $B_b \in \mathbb{Q}_{16b}$.

By assumption, $k \equiv 1 \pmod{4}$ and k, k' are both coprime to $16b$, so the signatures are well defined. Moreover, by the similar argument as Proposition 4.3, together with [20, Lemma 6.1], we immediately have (note that b is odd)

$$\varepsilon_{\mathcal{B}_b}(\sigma_{k'}) = (-1)^{bx} \varepsilon_{\mathcal{B}_b}(\sigma_k) = (-1)^x \varepsilon_{\mathcal{B}_b}(\sigma_k).$$

Proposition 5.2. *Let $r \equiv 12 \pmod{80}$, $b = 2r - 1 \equiv 23 \pmod{160}$ and $x \in \mathbb{Z}$. We have*

$$\varepsilon_{\mathcal{D}_r}(\sigma_{r-3}) = 1, \quad \varepsilon_{\mathcal{B}_b}(\sigma_{8xb+r-3}) = (-1)^x.$$

Proof. Suppose $r = 80k + 12$ for some integers $k \geq 0$ and $b = 160k + 23$. Since $r - 3 \equiv 1 \pmod{8}$, $r - 3$ is coprime to both $8N_r$ and $16b$. We have seen in Proposition 4.8 that $\mathfrak{d}_r(j)$ is

odd when $j \in \{4m+2, 4m+3, 4n, 4n+1 \mid 0 \leq m \leq 20k+2, 20k+3 \leq n \leq 40k+5\}$, and it is straight forward to check $c_b(j)$ is odd when $j \in \{4m+3, 4(m+1) \mid 0 \leq m \leq 80k+10\}$. By (4.18), (5.20), [20, Lem. 6.2, 6.3] (as $r-3 \equiv 1 \pmod{8}$) and the quadratic reciprocity, we have

$$\varepsilon_{D_r}(\sigma_{r-3}) = (-1)^{\sum_{m=0}^{20k+2} \left(\left\lfloor \frac{(4m+2)(r-3)}{4r-2} \right\rfloor + \left\lfloor \frac{(4m+3)(r-3)}{4r-2} \right\rfloor \right) + \sum_{n=20k+4}^{40k+5} \left(\left\lfloor \frac{4n(r-3)}{4r-2} \right\rfloor + \left\lfloor \frac{(4n+1)(r-3)}{4r-2} \right\rfloor \right)}$$

and

$$\varepsilon_{B_b}(\sigma_{r-3}) = \left(\frac{r-3}{b} \right)_J (-1)^{\sum_{l=1}^b \left(\left\lfloor \frac{(2l-1)(r-3)}{8b} \right\rfloor + \sum_{m=0}^{80k+10} \left(\left\lfloor \frac{(4m+3)(r-3)}{4b} \right\rfloor + \left\lfloor \frac{(4m+1)(r-3)}{4b} \right\rfloor \right) \right)}.$$

Now we compute the exponents in the above equations term by term.

$$\begin{aligned} \left\lfloor \frac{(4m+2)(r-3)}{4r-2} \right\rfloor &= m + \left\lfloor \frac{2r-10m-6}{4r-2} \right\rfloor = \begin{cases} m & \text{if } 0 \leq m \leq \lfloor \frac{2r-6}{10} \rfloor = 16k+1, \\ m-1 & \text{if } 16k+2 \leq m \leq 20k+2, \end{cases} \\ \left\lfloor \frac{(4m+3)(r-3)}{4r-2} \right\rfloor &= m + \left\lfloor \frac{3r-10m-9}{4r-2} \right\rfloor = m, \\ \left\lfloor \frac{(4n)(r-3)}{4r-2} \right\rfloor &= n-1 + \left\lfloor \frac{10n-4r+2}{4r-2} \right\rfloor = \begin{cases} n-2 & \text{if } 20k+3 \leq m \leq 32k+4, \\ n-1 & \text{if } 32k+5 \leq m \leq 40k+5, \end{cases} \\ \left\lfloor \frac{(4n+1)(r-3)}{4r-2} \right\rfloor &= n-1 + \left\lfloor \frac{10n-5r+5}{4r-2} \right\rfloor = n-2. \end{aligned}$$

Therefore, we have

$$\varepsilon_{D_r}(\sigma_{r-3}) = (-1)^{\sum_{m=16k+2}^{20k+2} (m-1+m) + \sum_{n=32k+5}^{40k+5} (n-1+n-2)} = (-1)^{(4k+1)+(2k+1)} = 1.$$

To facilitate the various cases, write $m = 2m' + s$ for $s \in \{0, 1\}$, and write $l = 8l' + t$ for $t \in \{1, 2, 3, 4, 5, 6, 7, 8\}$, then we have (i) $0 \leq m' \leq 40k+5$ when $s=0$; (ii) $0 \leq m' \leq 40k+4$ when $s=1$; (iii) $0 \leq l' \leq 20k+2$ when $t \in \{1, 2, 3, 4, 5, 6, 7\}$ and (iv) $0 \leq l' \leq 20k+1$ when $t=8$. Therefore,

$$\begin{aligned} \left\lfloor \frac{(4m+3)(r-3)}{4b} \right\rfloor &= m' + \left\lfloor \frac{(240+320s)k-20m+27+36s}{640k+92} \right\rfloor \\ &= \begin{cases} m' & s \in \{0, 1\} \text{ and } 0 \leq m' \leq (12+16s)k+2s+1, \\ m'-1 & s \in \{0, 1\} \text{ and } (12+16s)k+2(s+1) \leq m' \leq 40k+5-s. \end{cases} \\ \left\lfloor \frac{4(m+1)(r-3)}{4b} \right\rfloor &= m' + \left\lfloor \frac{(320+320s)k-20m+36+36s}{640k+92} \right\rfloor \\ &= \begin{cases} m' & s \in \{0, 1\} \text{ and } 0 \leq m' \leq 16(1+s)k+2s+1, \\ m'-1 & s \in \{0, 1\} \text{ and } 16(1+s)k+2(1+s) \leq m' \leq 40k+5-s. \end{cases} \\ \left\lfloor \frac{(2l-1)(r-3)}{8b} \right\rfloor &= l' + \left\lfloor \frac{(160t-80)k+18t-9-40l'}{1280k+184} \right\rfloor \\ &= \begin{cases} l' & 1 \leq t \leq 5 \text{ and } 0 \leq l' \leq (4t-2)k + \lfloor \frac{t-1}{2} \rfloor, \\ l'-1 & 1 \leq t \leq 5 \text{ and } (2+4t)k + \lfloor \frac{t+1}{2} \rfloor \leq l' \leq 20k+2, \\ l' & t \in \{6, 7\} \text{ and } 0 \leq l' \leq 20k+2, \\ l' & t=8 \text{ and } 0 \leq l' \leq 20k+1. \end{cases} \end{aligned}$$

Therefore, we have

$$\begin{aligned}
\varepsilon_{\mathcal{B}_b}(\sigma_{r-3}) &= \left(\frac{80k+9}{160k+23} \right)_J (-1)^{\sum_{m'=12k+2}^{28k+3} (m'-1+m')+40k+5-1 + \sum_{m'=16k+2}^{32k+3} (m'-1+m')+40k+5-1} \\
&\quad \times (-1)^{\sum_{m'=6k}^{2k+1} (l'-1+l')+ \sum_{m'=10k+2}^{14k+1} (l'-1+l')+ \sum_{m'=18k+3}^{20k+2} (l'-1+l')+20k+2} \\
&= \left(\frac{5}{80k+9} \right)_J (-1)^{(16k+2)+40k+4+(16k+2)+40k+4+(4k)+(4k)+(2k)+20k+2} \\
&= \left(\frac{9}{5} \right)_J = 1.
\end{aligned}$$

From Lemma 5.1 ($r-3 \equiv 1 \pmod{8}$), we have

$$\varepsilon_{\mathcal{B}_b}(\sigma_{8x+(r-3)}) = (-1)^x \varepsilon_{\mathcal{B}_b}(\sigma_{r-3}) = (-1)^x.$$

□

Let $\{b_i\}_{i \geq 1}$ be a sequence of prime numbers such that $b_i \equiv 23 \pmod{160}$, which exists due to the Dirichlet prime number theorem. Let $r_i = \frac{b_i+1}{2} \equiv 12 \pmod{80}$, and we use $H_{\mathbf{r}}$ to denote the group generated by $\{[\mathcal{D}_{r_i}]\}_{i \geq 1}$. Let $G_{\mathbf{p}}$ be the Witt subgroup at the beginning of this section. Note that the set $\{b_i\}$ may intersect with \mathbf{p} .

Theorem 5.3. *With the above notations, we have $G_{\mathbf{p}} \cap H_{\mathbf{r}} = \{[\text{Vec}]\}$.*

Proof. It suffices to show that no finite product of distinct $[\mathcal{D}_{r_j}]$'s and elements in $G_{\mathbf{p}}$ yields $[\text{Vec}]$ (elements in $G_{\mathbf{p}}$ may have multiplicities in this product). To this end, we take an arbitrary finite subsequence of $\{r_i\}$ denoted by $\{r_{j_w} | 1 \leq w \leq m\}$. We also pick an arbitrary finite subsequence $\{p_l | 1 \leq l \leq n\}$ of \mathbf{p} such that $2r_{j_l} - 1 \neq p_l$ for any $1 \leq l \leq n$. In other words, $p_l \neq b_{j_l}$ for any $1 \leq l \leq n$.

Now for any $s, \gamma_l \in \mathbb{Z}$, we consider the finite product

$$\mathcal{F} := \left(\boxtimes_{w=1}^m \mathcal{D}_{r_{j_w}} \right) \boxtimes \left(\boxtimes_{l=1}^n \mathcal{B}_{p_l}^{\boxtimes \gamma_l} \right) \boxtimes \left(\mathcal{B}_{b_{j_1}}^{\boxtimes s} \right).$$

By the previous results, we have $\sqrt{\dim(\mathcal{D})} \in \mathbb{Q}_N$, where $N = \text{lcm}_{1 \leq w \leq m, 1 \leq l \leq n} \{32N_{r_{j_w}}, 32p_l\}$. Let $K = \text{lcm}_{2 \leq w \leq m, 1 \leq l \leq n} \{32b_{j_w}, 32p_l\}$, then $\gcd(b_{j_1}, K) = 1$ by construction. Hence, by Bezout's identity, there exist $x, y \in \mathbb{Z}$ such that

$$xb_{j_1} + yK = 1. \quad (5.21)$$

Define

$$t = \begin{cases} -(r_{j_1} - 4)xb_{j_1} + r_{j_1} - 3 & \text{if } s \text{ is odd,} \\ -(2r_{j_1})xb_{j_1} + 2r_{j_1} + 1 & \text{if } s \text{ is even.} \end{cases}$$

Since $r_{j_1} - 4 = 8(10k+1)$ and $4|2r_{j_1}$, we have

$$t \equiv 1 \pmod{K} \quad \text{and} \quad t \equiv \begin{cases} r_{j_1} - 3 \pmod{2b_{j_1}} & \text{if } s \text{ is odd,} \\ 2r_{j_1} + 1 \pmod{2b_{j_1}} & \text{if } s \text{ is even.} \end{cases}$$

Again by Lemma 3.5, we have $\gcd(t, N) = 1$. Moreover, we use Propositions 4.3, 4.8 and 5.2 and get the following two cases (note that x is odd by construction). To avoid too many subscripts in the expression of the signatures, we temporarily write $\varepsilon_w^{\mathcal{D}} := \varepsilon_{\mathcal{D}_{r_{j_w}}}$ for $1 \leq w \leq m$, $\varepsilon_l^{\mathcal{B}} := \varepsilon_{\mathcal{B}_{p_l}}$ for $1 \leq l \leq n$, and we write $\varepsilon_{j_1}^{\mathcal{B}} := \varepsilon_{\mathcal{B}_{j_1}}$ in this proof. Note that $\varepsilon_{\mathcal{B}_{b_{j_1}}}^{\boxtimes s} = (\varepsilon_{j_1}^{\mathcal{B}})^s$.

Firstly, when s is odd, there exists $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, such that $\sigma|_{\mathbb{Q}_N} = \sigma_t$, and

$$\begin{aligned}\varepsilon_w^{\mathcal{D}}(\sigma) &= \varepsilon_l^{\mathcal{B}}(\sigma) = 1 \quad \text{for } 1 \leq w \leq m, \quad 1 \leq l \leq n, \\ \varepsilon_{j_1}^{\mathcal{B}}(\sigma_{8(10k+1)xb_{j_1}+r_{j_1}-3})^s &= (-1)^{(10k+1)xs} = -1.\end{aligned}$$

Secondly, when s is even, there exists $\eta \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, such that $\eta|_{\mathbb{Q}_N} = \eta_t$, and

$$\varepsilon_w^{\mathcal{D}}(\eta) = \varepsilon_l^{\mathcal{B}}(\eta) = \varepsilon_{j_1}^{\mathcal{B}}(\eta)^s = 1 \quad \text{for } 2 \leq w \leq m, \quad 1 \leq l \leq n, \quad \text{and } \varepsilon_1^{\mathcal{D}}(\eta) = -1.$$

Therefore, in either case, $\varepsilon_{\mathcal{F}} = \prod_{w=1}^m \varepsilon_w^{\mathcal{D}} \cdot \prod_{l=1}^n (\varepsilon_l^{\mathcal{B}})^{\gamma_l} \cdot (\varepsilon_{j_1}^{\mathcal{B}})^s$ is not the constant function 1, then by [20, Thm. 3.5], $[\mathcal{E}] \neq [\text{Vec}]$. \square

6. An order two Witt class with property S

Recall that a non-degenerate braided fusion category \mathcal{C} has *property S* if it is completely anisotropic, simple and unpointed. The subgroup of \mathcal{W} generated by the categories with property S is denoted by \mathcal{W}_S . In this section, we prove that $[\mathcal{D}_4] \in \mathcal{W}_S$. Since \mathcal{D}_4 has order 2 in \mathcal{W} (see (3.15)), it gives a positive answer to the open question [5, Question 6.8]. From Theorem 4.10, $[\mathcal{D}_4] \notin \mathcal{W}_{\text{pt}}$, hence it suffices to prove \mathcal{D}_4 is simple and completely anisotropic.

Lemma 6.1. *For any positive integer $r \geq 3$, the category \mathcal{D}_r is simple.*

Proof. From Lemma 3.7 and [29, Lemma 1], we have $(\mathcal{D}_r)_{\text{pt}} \cong \text{Vec}$, and there is no nontrivial objects in \mathcal{D}_r of integer dimension. Hence if $\mathcal{R} \subset \mathcal{D}_r$ is a fusion subcategory, then by Deligne's Theorem [10, Section 9.9] and above discussion, we have $\mathcal{R}' \subset (\mathcal{D}_r)_{\text{pt}} \cong \text{Vec}$, which implies \mathcal{R} is non-degenerate. Now the Lemma follows from [29, Theorem 2]. \square

Now let $r=4$. Recall from Lemma 3.7 that in this case, $(\mathcal{C}_4)_{\text{pt}} \cong \text{Rep}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$, which contains the connected étale algebra $A_4 = \text{Fun}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. By definition, $\mathcal{D}_4 = (\mathcal{C}_4)_{A_4}^0$. We will show that \mathcal{D}_4 is completely anisotropic, i.e., it does not have any nontrivial connected étale algebra.

By [28, Lem. 2.24], all connected étale algebras in a pseudounitary braided fusion category have trivial twists. Therefore, it suffices to consider only objects with trivial twists in \mathcal{D}_4 . By [14, Thm. 1.17], such objects are images under the free module functor $F: \mathcal{C}_4 \rightarrow \mathcal{D}_4$ (see Lemma 3.7) of objects with trivial twists in \mathcal{C}_4 , which we describe as follows.

One can compute, by formulas (3.9), that in addition to the 4 invertible objects in \mathcal{C}_4 , there are 8 more objects with trivial twists, and they are grouped into the sets $X := \{2\omega_2, 2\omega_2 + 4\omega_1, 2\omega_2 + 4\omega_3, 2\omega_2 + 4\omega_4\}$ and $Y := \{2\omega_1 + \omega_2 + 2\omega_3, 2\omega_1 + \omega_2 + 2\omega_4, \omega_2 + 2\omega_3 + 2\omega_4, 2\omega_1 + \omega_2 + 2\omega_3 + 2\omega_4\}$. By [26, Lemma 2], the action of the algebra $A_4 \in \mathcal{C}_4$ on the objects in X and Y (by tensoring) is fixed-point free and transitive. In particular, this implies that all of the objects in $X \cup Y$ centralize A_4 . Therefore, there are only 2 nontrivial objects with trivial twists in \mathcal{D}_4 , which we denote by $Z_1 = F(\lambda)$ and $Z_2 = F(\mu)$ for an arbitrary choice of objects $\lambda \in X$ and $\mu \in Y$ (note that Z_1 and Z_2 do not depend on the choice of λ and μ).

Moreover, we have

$$d_1 := d_{Z_1} = 28(\zeta_7 + \zeta_7^6) + 14(\zeta_7^2 + \zeta_7^5) + 33 \approx 61.685$$

and

$$d_2 := d_{Z_2} = 126(\zeta_7 + \zeta_7^6) + 56(\zeta_7^2 + \zeta_7^5) + 157 \approx 289.197.$$

Therefore, any nontrivial connected étale algebra in \mathcal{D}_4 has to be of the form $L = \mathbb{1} + a_1 Z_1 + a_2 Z_2$ for some $a_1, a_2 \in \mathbb{Z}_{\geq 0}$. Moreover, by the local module construction, any connected étale algebra $L \in \mathcal{D}_4$ will give rise to a modular category $(\mathcal{D}_4)_L^0$ with the property (see [14, Thm. 4.5])

$$\dim(\mathcal{D}_4)_L^0 = \frac{\dim(\mathcal{D}_4)}{d_L^2},$$

where $\dim(\mathcal{D}_4) = -196[\zeta_7 + \zeta_7^6] + 873(\zeta_7^2 + \zeta_7^5) + 1357(\zeta_7^3 + \zeta_7^4) \approx 489669.5$.

Since the global dimensions of modular categories are ≥ 1 [11, Thm. 2.3], upper bounds for a_1, a_2 can be given by

$$\frac{\dim(\mathcal{D}_4)}{(1 + a_1 d_1)^2} \geq 1 \quad \Rightarrow \quad a_1 \leq 11; \quad \frac{\dim(\mathcal{D}_4)}{(1 + a_2 d_2)^2} \geq 1 \quad \Rightarrow \quad a_2 \leq 2.$$

Therefore, the set of connected algebras in \mathcal{D}_4 is a subset of the following set of objects

$$E := \{\mathbb{1} + a_1 Z_1 + a_2 Z_2 \mid 0 \leq a_1 \leq 11, 0 \leq a_2 \leq 2\},$$

with the tensor unit $\mathbb{1}$ corresponding to $a_1 = a_2 = 0$. From now on, we will focus on nontrivial objects, so we assume that a_1 and a_2 are not both 0.

According to [22, Lem. 5.3 (c)], the dimension of any connected étale algebra $L \in E$ is totally positive, i.e., all the Galois conjugates of d_L are positive real numbers. This gives more restrictions on a_1 and a_2 . Indeed, using SageMath [30], one can see that for any $L \in E$, the Galois conjugates of $d_L = 1 + a_1 d_1 + a_2 d_2$ are of the form $1 + a_1 d'_1 + a_2 d'_2$ and $1 + a_1 d''_1 + a_2 d''_2$. Here, d'_1, d''_1 are Galois conjugates of d_1 with $d'_1 \approx -4.688$ and $d''_1 \approx 0.003$; and d'_2, d''_2 are Galois conjugates of d_2 with $d'_2 \approx 0.016$ and $d''_2 \approx -0.213$. Therefore, by direct computation, the only nontrivial $L \in E$ with totally positive dimensions are $L = \mathbb{1} + Z_2$ and $L = \mathbb{1} + 2Z_2$. In other words, these are the only two candidates for nontrivial connected étale algebras in \mathcal{D}_4 .

Next observe that since $\dim(\mathcal{D}_4)_L^0$ is an algebraic integer [11, Rmk. 2.5]), the algebraic norm of $\frac{\dim(\mathcal{D}_4)}{d_L^2}$ has to be a (rational) integer. Again using SageMath, we can easily see that only for $L = \mathbb{1} + 2Z_2$, $\dim(\mathcal{D}_4)/d_L^2$ has integral norm.

Finally, since the local module construction preserves pseudounitariness [28, Lem. 2.24], $(\mathcal{D}_4)_L^0$ is pseudounitary for any connected étale algebra L . As the FP-dimension of objects are ≥ 1 [10, Prop. 3.3.4], we have either $\frac{\dim(\mathcal{D}_4)}{d_L^2} = 1$ or $\frac{\dim(\mathcal{D}_4)}{d_L^2} \geq 2$. By direct computation, we have

$$\frac{\dim(\mathcal{D}_4)}{d_L^2} \approx 1.459.$$

Therefore, $L = \mathbb{1} + 2Z_2$ cannot be a connected étale algebra.

Combining the above discussions, we have

Theorem 6.2. *The modular category \mathcal{D}_4 is completely anisotropic, hence $[\mathcal{D}_4] \in \mathcal{W}_s$.* □

Acknowledgments

The authors would like to thank Siu-Hung Ng and Andrew Schopieray for helpful discussions, especially for pointing out that the total positivity of connected étale algebras can be used to simplify arguments in Section 6. We thank Daniel Bump for the very useful FusionRing package in SageMath, used to test our results. We also thank the anonymous referee for helpful comments and constructive suggestions. E. C. R. was partially supported by NSF grant DMS-1664359 and a Presidential Impact Fellowship from Texas A&M University.

ORCID

Eric C. Rowell  <http://orcid.org/0000-0002-2338-9819>

Yuze Ruan  <http://orcid.org/0000-0002-9025-2804>

Yilong Wang  <http://orcid.org/0000-0003-4246-683X>

References

- [1] Bakalov, B., Kirillov, A. Jr. (2001). *Lectures on Tensor Categories and Modular Functors, Volume 21 of University Lecture Series*. Providence, RI: American Mathematical Society.
- [2] Bischoff, M., Jones, C., Lu, Y.-M., Penneys, D. (2019). Spontaneous symmetry breaking from anyon condensation. *J. High Energy Phys.* 2019(062):41 pp.
- [3] Burnell, F. (2018). Anyon condensation and its applications. *Annu. Rev. Condens. Matter Phys.* 9(1): 307–327. DOI: [10.1146/annurev-conmatphys-033117-054154](https://doi.org/10.1146/annurev-conmatphys-033117-054154).
- [4] Coquereaux, R. (2010). Global dimensions for Lie groups at level k and their conformally exceptional quantum subgroups. *Rev. Un. Mat. Argentina.* 51(2):17–42.
- [5] Davydov, A., Müger, M., Nikshych, D., Ostrik, V. (2013). The Witt group of non-degenerate braided fusion categories. *J. Reine Angew. Math.* 677:135–177.
- [6] Davydov, A., Nikshych, D., Ostrik, V. (2013). On the structure of the Witt group of braided fusion categories. *Sel. Math. New Ser.* 19(1):237–269. DOI: [10.1007/s00029-012-0093-3](https://doi.org/10.1007/s00029-012-0093-3).
- [7] Dong, C., Lin, X., Ng, S.-H. (2015). Congruence property in conformal field theory. *Algebra Number Theor.* 9(9):2121–2166. DOI: [10.2140/ant.2015.9.2121](https://doi.org/10.2140/ant.2015.9.2121).
- [8] Drinfeld, V., Gelaki, S., Nikshych, D., Ostrik, V. (2010). On braided fusion categories. I. *Sel. Math. New Ser.* 16(1):1–119. DOI: [10.1007/s00029-010-0017-z](https://doi.org/10.1007/s00029-010-0017-z).
- [9] Drinfel'd, V. G. (1987). Quantum groups. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986)*, p. 798–820. Amer. Math. Soc., Providence, RI.
- [10] Etingof, P., Gelaki, S., Nikshych, D., Ostrik, V. (2015). *Tensor Categories, Volume 205 of Mathematical Surveys and Monographs*. Providence, RI: American Mathematical Society.
- [11] Etingof, P., Nikshych, D., Ostrik, V. (2005). On fusion categories. *Ann. Math.* 162(2):581–642. DOI: [10.4007/annals.2005.162.581](https://doi.org/10.4007/annals.2005.162.581).
- [12] E. Humphreys, J. (1972). *Introduction to Lie Algebras and Representation Theory*. New York, Berlin: Springer-Verlag, Graduate Texts in Mathematics, Vol. 9.
- [13] Kassel, C. (1995). *Quantum Groups, Volume 155 of Graduate Texts in Mathematics*. New York: Springer-Verlag.
- [14] Kirillov, A., Jr., Ostrik, V. (2002). On a q -analogue of the McKay correspondence and the ADE classification of \mathfrak{sl}_2 conformal field theories. *Adv. Math.* 171(2):183–227.
- [15] Lusztig, G. (1993). *Introduction to Quantum Groups, Volume 110 of Progress in Mathematics*. Boston, MA: Birkhäuser Boston, Inc.
- [16] Moore, G., Seiberg, N. (1989). Classical and quantum conformal field theory. *Commun. Math. Phys.* 123(2): 177–254. DOI: [10.1007/BF01238857](https://doi.org/10.1007/BF01238857).
- [17] Müger, M. (2003). From subfactors to categories and topology. I. Frobenius algebras in and Morita equivalence of tensor categories. *J. Pure Appl. Algebra.* 180(1–2):81–157. DOI: [10.1016/S0022-4049\(02\)00247-5](https://doi.org/10.1016/S0022-4049(02)00247-5).
- [18] Müger, M. (2003). On the structure of modular categories. *Proc. London Math. Soc.* 87(2):291–308. DOI: [10.1112/S0024611503014187](https://doi.org/10.1112/S0024611503014187).
- [19] Nayak, C., Simon, S. H., Stern, A., Freedman, M., Sarma, S. D. (2008). Non-abelian anyons and topological quantum computation. *Rev. Mod. Phys.* 80(3):1083–1159. DOI: [10.1103/RevModPhys.80.1083](https://doi.org/10.1103/RevModPhys.80.1083).
- [20] Ng, S.-H., Rowell, E. C., Wang, Y., Zhang, Q. (2022). Higher central charges and Witt groups. *Adv. Math.* 404:108388.
- [21] Ng, S.-H., Schauenburg, P. (2007). Frobenius-Schur indicators and exponents of spherical categories. *Adv. Math.* 211(1):34–71. DOI: [10.1016/j.aim.2006.07.017](https://doi.org/10.1016/j.aim.2006.07.017).
- [22] Ng, S.-H., Schopieray, A., Wang, Y. (2019). Higher Gauss sums of modular categories. *Selecta Math.* 25(4): Paper No. 53, 32.
- [23] Pareigis, B. (1995). On braiding and dyslexia. *J. Algebra.* 171(2):413–425. DOI: [10.1006/jabr.1995.1019](https://doi.org/10.1006/jabr.1995.1019).
- [24] Rowell, E., Stong, R., Wang, Z. (2009). On classification of modular tensor categories. *Commun. Math. Phys.* 292(2):343–389. DOI: [10.1007/s00220-009-0908-z](https://doi.org/10.1007/s00220-009-0908-z).
- [25] Rowell, E. C. (2006). From quantum groups to unitary modular tensor categories. In *Representations of Algebraic Groups, Quantum Groups, and Lie Algebras, Volume 413 of Contemp. Math.*, p. 215–230. Amer. Math. Soc., Providence, RI.
- [26] Sawin, S. F. (2002). Jones-Witten invariants for nonsimply-connected Lie groups and the geometry of the Weyl alcove. *Adv. Math.* 165(1):1–34. DOI: [10.1006/aima.1999.1910](https://doi.org/10.1006/aima.1999.1910).
- [27] Sawin, S. F. (2006). Closed subsets of the Weyl alcove and TQFTs. *Pacific J. Math.* 228(2):305–324. DOI: [10.2140/pjm.2006.228.305](https://doi.org/10.2140/pjm.2006.228.305).
- [28] Schopieray, A. (2018). Level bounds for exceptional quantum subgroups in rank two. *Int. J. Math.* 29(5): 1850034. DOI: [10.1142/S0129167X18500349](https://doi.org/10.1142/S0129167X18500349).
- [29] Schopieray, A. (2020). Prime decomposition of modular tensor categories of local modules of type D. *Quantum Topol.* 11(3):489–524. DOI: [10.4171/QT/140](https://doi.org/10.4171/QT/140).

- [30] The Sage Developers. (2021). *SageMath, the Sage Mathematics Software System (Version 9.3)*, <https://www.sagemath.org>.
- [31] Turaev, V. G. (2010). *Quantum Invariants of Knots and 3-Manifolds, Volume 18 of De Gruyter Studies in Mathematics*. revised ed. Berlin: Walter de Gruyter & Co.
- [32] Vafa, C. (1988). Toward classification of conformal theories. *Phys. Lett. B.* 206(3):421–426. DOI: [10.1016/0370-2693\(88\)91603-6](https://doi.org/10.1016/0370-2693(88)91603-6).
- [33] Washington, L. C. (1982). *Introduction to Cyclotomic Fields, Volume 83 of Graduate Texts in Mathematics*. New York: Springer-Verlag.