Available online at www.sciencedirect.com
SciVerse ScienceDirect
Advances in Mathematics 230 (2012) 894–926
ADVANCES IN Mathematics
www.elsevier.com/locate/aim

The Weil representation in characteristic two

Shamgar Gurevich[a,*], Ronny Hadani[b]

[a] *Department of Mathematics, University of Wisconsin, Madison, WI 53706, USA*
[b] *Department of Mathematics, University of Texas, Austin, TX 78712, USA*

Received 13 August 2008; accepted 5 March 2012
Available online 21 April 2012

Communicated by David Ben-Zvi

Abstract

In this paper we construct a new variant of the Weil representation, associated with a symplectic vector space (V,ω) defined over a finite field of characteristic two. Our variant is a representation $\rho : AMp(V) \to GL(\mathcal{H})$, where the group $AMp(V)$ is the fourth cover of a group $ASp(V)$ which is a non-trivial extension of the symplectic group $Sp(V)$ by the dual group V^*. In particular, the group $ASp(V)$ contains Weil's pseudo-symplectic group as a strict subgroup. Along the way, we develop the formalism of canonical vector spaces which enables us to realize the group $AMp(V)$ and the Weil representation ρ in a transparent manner and also yields a conceptual explanation for these important objects of representation theory.

MSC: Primary 11F27

Keywords: Weil representation; Characteristic two; Strong Stone–von Neumann property; Weil Gerbe; Affine symplectic group; Affine metaplectic group; Canonical vector space

0. Introduction

In his celebrated 1964 Acta paper [5] André Weil constructed a distinguished unitary representation ρ_{Weil}, which is associated with a symplectic vector space (V,ω) over a local field $\mathbb{F}$, now referred to as the *Weil representation*. The Weil representation has many fascinating

* Corresponding author.
E-mail addresses: shamgar@math.wisc.edu (S. Gurevich), hadani@math.utexas.edu (R. Hadani).

0001-8708/$ - see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.aim.2012.03.008

properties which have gradually been brought to light over the past few decades. It now appears that this representation is a central object in mathematics: embedded in the fabric of the theory of harmonic analysis and bridging between various topics in mathematics, physics and also signal processing, including classical invariant theory, the theory of theta functions, automorphic forms, quantum mechanics and last (but probably not least) communication theory.

In his paper, André Weil constructs ρ_{Weil}, first, in the setup when $\mathbb{F}$ is a local field of characteristic zero or a local field of finite characteristic p where $p \neq 2$. In this set-up, ρ_{Weil} is a representation of a double cover of the symplectic group $Sp(V)$ (called the metaplectic cover). In his subsequent papers [1,5], Weil proceeds to construct ρ_{Weil} in the more intricate setup when $\mathbb{F}$ is a local field of characteristic 2. In this setup, ρ_{Weil} is a representation of (a double cover of) the *pseudo-symplectic group* $Ps(V)$, which is a non-trivial extension of an orthogonal group by the dual vector space V^* (at least in the case when the field $\mathbb{F}$ is perfect). In particular, the pseudo-symplectic group fits into a short exact sequence of groups

$$1 \to V^* \to Ps(V) \to O(Q) \to 1,$$

where, $Q : V \to \mathbb{F}$ is a quadratic form associated with a non-symmetric bilinear form $\beta : V \times V \to \mathbb{F}$ polarizing the symplectic form, namely, satisfying that $\beta(v,u) - \beta(u,v) = \omega(v,u)$ and $O(Q)$ is the associated orthogonal group.

A comparison between the construction of the Weil representation in the two setups suggests that the definition when $\mathbb{F}$ is a field of characteristic 2 is unsatisfactory for the reason that $Ps(V)$ does not surjects onto the symplectic group. Instead, it surjects only onto the subgroup $O(Q) \subsetneqq Sp(V)$ which (as an algebraic group) is of smaller dimension

$$\dim Sp(V) = \dim V(\dim V + 1)/2,$$
$$\dim O(Q) = \dim V(\dim V - 1)/2.$$

A natural question to pose is whether there exists an extension of ρ_{Weil} to a representation ρ (which acts on the same Hilbert space) of a larger group G containing the pseudo-symplectic group and mapping onto the symplectic group.

0.1. Main results

In this paper we give a positive answer to this question. Specifically, we construct a new variant of the Weil representation associated to a symplectic vector space (V, ω) defined over a finite field $\mathbb{F}$ of characteristic two. Our construction incorporates the following results.

0.1.1. Projective Weil representation

We describe a group $ASp(V)$ that we call the *affine symplectic group*, containing the pseudo-symplectic group $Ps(V)$ as a subgroup and constituting an extension of the symplectic group $Sp(V)$ by the dual abelian group V^*. Thus it fits into a short exact sequence of groups

$$1 \to V^* \to ASp(V) \to Sp(V) \to 1.$$

In addition, we describe a projective representation

$$\widetilde{\rho} : ASp(V) \to PGL(\mathcal{H}),$$

which extends, as a projective representation, the Weil's representation ρ_{Weil}.

0.1.2. Linear Weil representation

We describe a group $AMp(V)$, that we call the *affine metaplectic group*, which is a central extension of $ASp(V)$ by the group $\mu_4(\mathbb{C})$ of 4th roots of unity. In addition, we construct an honest representation

$$\rho : AMp(V) \to GL(\mathcal{H}),$$

linearizing the projective representation $\widetilde{\rho}$.

0.1.3. Splitting of the Weil representation

We describe a splitting homomorphism $s : Mp(\widetilde{V}) \to AMp(V)$ and a pull-back representation

$$\rho_{\widetilde{V}} = \rho \circ s : Mp(\widetilde{V}) \to GL(\mathcal{H}),$$

where $(\widetilde{V}, \widetilde{\omega})$ is a free symplectic module over the ring $W_2(\mathbb{F})$ of (level 2) truncated Witt vectors which specializes to (V, ω) modulo 2 and $Mp(\widetilde{V})$ is a central extension of the symplectic group $Sp(\widetilde{V})$ by the group $\mu_2(\mathbb{C}) = \{\pm 1\}$.

0.1.4. The formalism of canonical vector spaces

Along the way, we develop the formalism of canonical vector spaces in the characteristic two setup. Using this formalism we are able to give a transparent realization of the group $AMp(V)$, the representations ρ and the splitting homomorphism $s : Mp(\widetilde{V}) \to AMp(V)$. Moreover, this formalism serves as an appropriate conceptual framework for the study of these objects. The development of this formalism constitutes the main technical contribution of this paper.

We devote the reminder of the introduction to a more detailed account of the main constructions and results of this paper. For simplicity we assume that $\mathbb{F} = \mathbb{F}_2$ postponing the case when $\mathbb{F} = \mathbb{F}_{2^d}$ to the body of the paper.

0.2. The Heisenberg group

Considering the vector space V as an abelian group and equipping it with a bi-additive form $\beta : V \times V \to 2\mathbb{Z}/4\mathbb{Z}$ satisfying that $\beta(u, v) - \beta(v, u) = 2\omega(u, v) \in 2\mathbb{Z}/4\mathbb{Z}$, we can associate to the pair (V, β) a central extension group $H(V) = H_\beta(V)$

$$0 \to \mathbb{Z}/4\mathbb{Z} \to H(V) \to V \to 0,$$

called the *Heisenberg group*. The group of automorphisms of $H(V)$ acting trivially on the center is denoted by $ASp(V)$ and is referred to as the *affine symplectic group*. The affine symplectic group fits into a non-split exact sequence

$$0 \to V^* \to ASp(V) \to Sp(V) \to 1.$$

Concretely, elements of $ASp(V)$ can be presented as pairs (g, α) where $g \in Sp(V)$ and $\alpha : V \to \mathbb{Z}/4\mathbb{Z}$ is satisfying the following polarization condition:

$$\alpha(v_1 + v_2) - \alpha(v_1) - \alpha(v_2) = \beta(gv_1, gv_2) - \beta(v_1, v_2). \tag{0.1}$$

0.2.1. Weil's Heisenberg group

Our version of the Heisenberg group should be contrasted with Weil's version that appears in [5]. Weil's group $H_{\text{Weil}}(V)$ is a central extension of the vector space V by the field $\mathbb{F}$ associated with a non-symmetric bilinear form $\beta : V \times V \to \mathbb{F}$ satisfying $\beta(u,v) - \beta(v,u) = \omega(u,v)$. The group of automorphisms of $H_{\text{Weil}}(V)$ acting trivially on the center is the pseudo-symplectic group $Ps(V)$ whose elements can be presented as pairs (g, α) where $g \in Sp(V)$ and $\alpha : V \to \mathbb{F}$ is satisfying the condition:

$$\alpha(v_1 + v_2) - \alpha(v_1) - \alpha(v_2) = \beta(gv_1, gv_2) - \beta(v_1, v_2). \tag{0.2}$$

The reason why the pseudo-symplectic group $Ps(V)$ is strictly smaller than the affine symplectic group $ASp(V)$ is because Eq. (0.1) admits solutions with values in $\mathbb{Z}/4\mathbb{Z}$ for every $g \in Sp(V)$, while Eq. (0.2) admits solutions with values in $\mathbb{F}$ only when g lies in the orthogonal group $O(Q) \subset Sp(V)$ where $Q(v) = \beta(v,v)$.

This phenomena can be appreciated already in the following simplified situation: let $\beta : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ be the bilinear form given by

$$\beta(x,y) = xy.$$

It can be easily verified that there is no quadratic form $\alpha : \mathbb{F} \to \mathbb{F}$ which polarizes β, namely, satisfies the condition

$$\alpha(x+y) - \alpha(x) - \alpha(y) = \beta(x,y).$$

However, considering the quadratic form $\widetilde{\alpha} : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ given by $\widetilde{\alpha}(x) = x^2$, it can be easily verified that $\widetilde{\alpha}$ descends to a function $\alpha : \mathbb{F} \to \mathbb{Z}/4\mathbb{Z}$ which satisfies

$$\alpha(x+y) - \alpha(x) - \alpha(y) = 2\beta(x,y) \in \mathbb{Z}/4\mathbb{Z}.$$

0.3. The Heisenberg representation

Fixing a faithful character ψ of the center of $H(V)$, there exists a unique irreducible representation $\pi : H(V) \to GL(\mathcal{H})$ with a central character ψ—this is the *Stone–von Neumann property* (S–vN property for short). We refer to this representation as the *Heisenberg representation*.

0.4. Realizations of the Heisenberg representation

The Heisenberg representation admits a special family of models (realizations) associated with *enhanced Lagrangian* subspaces in V. An enhanced Lagrangian is a pair (L, τ) where $L \in Lag(V)$ is a Lagrangian subspace and $\tau : L \to H(V)$ is a homomorphism splitting of the natural projection $H(V) \to V$. To such a pair one can associate a model $(\pi_L, H(V), \mathcal{H}_L)$ of the Heisenberg representation (abusing the notation a bit), defined as follows. The vector space $\mathcal{H}_L$ consists of functions $f : H(V) \to \mathbb{C}$ satisfying

$$f(z \cdot \tau(l) \cdot h) = \psi(z) f(h),$$

with $l \in L$ and $z \in Z(H(V))$ a central element and the action π_L is given by right translations.

The collection of models $\{\mathcal{H}_L\}$ forms a vector bundle $\mathfrak{H}$ on the set $ELag(V)$ of enhanced Lagrangians, with fibers $\mathfrak{H}_L = \mathcal{H}_L$ for every $L \in ELag(V)$.

0.5. The strong Stone–von Neumann property

A fundamental technical result of this paper is a strong variant of the Stone–von Neumann property which asserts that the fourth tensor product Heisenberg bundle $\mathfrak{H}^{\otimes 4}$ admits a *natural* trivialization, that is, there is a canonical system of linear maps $T_{M,L} : \mathcal{H}_L^{\otimes 4} \to \mathcal{H}_M^{\otimes 4}$ satisfying the following multiplicativity condition:

$$T_{N,M} \circ T_{M,L} = T_{N,L},$$

for every triple $N, M, L \in ELag(V)$. We refer to this result as the strong Stone–von Neumann property (strong S–vN for short).

0.6. The Weil gerbe

The strong S–vN property is encoded in the structure of a groupoid category $\mathcal{W}$ defined as follows. An object in $\mathcal{W}$ is a triple $(\mathfrak{E}, \{E_{M,L}\}, \varphi)$, where $\mathfrak{E}$ is a vector bundle on $ELag(V)$, $\{E_{M,L} : M, L \in ELag(V)\}$ is a trivialization of $\mathfrak{E}$ and the map $\varphi : \mathfrak{E} \xrightarrow{\simeq} \mathfrak{H}$ is an isomorphism of vector bundles satisfying that

$$\varphi^{\otimes 4} : \mathfrak{E}^{\otimes 4} \xrightarrow{\simeq} \mathfrak{H}^{\otimes 4},$$

is an isomorphism of trivialized vector bundles. A morphism in $\mathcal{W}$ is an isomorphism $f : \mathfrak{E}_1 \xrightarrow{\simeq} \mathfrak{E}_2$ of trivialized vector bundles satisfying the condition

$$\varphi_2^{\otimes 4} \circ f^{\otimes 4} = \varphi_1^{\otimes 4}.$$

The groupoid $\mathcal{W}$ is a gerbe with band $\mu_4(\mathbb{C})$ which means that every two objects in $\mathcal{W}$ are isomorphic and $\mathrm{Mor}_{\mathcal{W}}(\mathfrak{E}, \mathfrak{E}) \simeq \mu_4(\mathbb{C})$, for every $\mathfrak{E} \in \mathcal{W}$. We remark that in this paper, a gerbe with band G is a groupoid category consisting of a single isomorphism class of objects such that the automorphism group of every object is isomorphic to G. We refer to $\mathcal{W}$ as the *Weil gerbe*.

Remark 0.1. We note that in the definition of an object in the Weil gerbe, the vector bundle is not equipped with an Heisenberg action.

0.7. Action of the affine symplectic group

The group $ASp(V)$ naturally acts on the Weil gerbe. The action of an element $g \in ASp(V)$ is given by the pull-back functor $g^* : \mathcal{W} \to \mathcal{W}$, sending a vector bundle $\mathfrak{E}$ to its pull-back $g^*\mathfrak{E}$. It follows from completely general considerations (see [2]) that there exists a central extension

$$1 \to \mu_4(\mathbb{C}) \to AMp(V) \to ASp(V) \to 1,$$

naturally associated with the action of $ASp(V)$ on the groupoid $\mathcal{W}$. Concretely, an element of $AMp(V)$ is a pair (g, ι) where $g \in ASp(V)$ and $\iota : g^* \xrightarrow{\simeq} Id$ is an isomorphism of functors.

0.8. Canonical realization of the Weil representation

The Weil representation is canonically realized as an action of the affine metaplectic group on a vector space twisted by the Weil gerbe. The construction proceeds as follows. We consider the fiber functor $\Gamma : \mathcal{W} \rightarrow \mathsf{Vect}$ where Vect denote the category of complex vector spaces, sending an object $\mathfrak{E} \in \mathcal{W}$ to the vector space of "horizontal sections" consisting of systems

$$(f_L \in \mathfrak{E}_L : L \in ELag\,(V))\,,$$

satisfying that $E_{M,L}\,(f_L) = f_M$, for every pair $M, L \in ELag\,(V)$. In addition, there exists a natural homomorphism

$$\rho : AMp\,(V) \rightarrow \operatorname{Aut}(\Gamma)\,.$$

After choosing an object $\mathfrak{E} \in \mathcal{W}$ we return to the more familiar setting of an action of a group on a vector space by specializing ρ to the object $\mathfrak{E}$, obtaining a homomorphism of groups

$$\rho_{\mathfrak{E}} : AMp\,(V) \rightarrow GL\,(\Gamma\,(\mathfrak{E}))\,.$$

This is of course our Weil representation in its more classical realization.

0.9. *Structure of the paper*

Apart from the introduction, this paper consists of five sections and an Appendix.

In Section 1, we introduce the Weil representation associated with a symplectic vector space (V, ω) defined over a finite field of characteristic 2. We begin by describing an appropriate Heisenberg group $H\,(V)$. Than we describe the Heisenberg representation and formulate the Stone–von Neumann property for this representation. Then we proceed to describe the group $ASp\,(V)$ of automorphisms of $H\,(V)$ acting trivially on the center. We end this section with the statements of two theorems: the first theorem (Theorem 1.3) asserts the existence of the Weil representation ρ of the affine metaplectic group $AMp\,(V)$. The second theorem (Theorem 1.4) asserts the existence of a splitting of ρ over the group $Sp(\widetilde{V})$ which amounts to a representation of the metaplectic group $Mp(\widetilde{V})$.

In Section 2, we develop the formalism of canonical vector spaces. We begin by describing a special family of models of the Heisenberg representation which are associated with enhanced Lagrangian subspaces in V. We explain how these models combine into the Heisenberg vector bundle $\mathfrak{H}$ on the set $ELag\,(V)$ of enhanced Lagrangians. We proceed to define the notion of a trivialization of an Heisenberg vector bundle. The main statement is Theorem 2.6 which asserts the existence of a canonical trivialization of the fourth tensor product $\mathfrak{H}^{\otimes 4}$. Using Theorem 2.6, we define the Weil gerbe $\mathcal{W}$, which is then used to construct the canonical model of the Weil representation, proving, in particular, Theorem 1.3.

In Section 3, we describe the construction of the canonical trivialization asserted in Theorem 2.6. Specifically, we describe the canonical intertwining morphisms between transversal models of the Heisenberg representation and give an explicit formula for the cocycle C which is associated with them. The main theorem of this section is Theorem 3.2 which asserts that $C^4 = 1$. The rest of the section is devoted to the proof of Theorem 3.2. Along the way, we obtain some results concerning inner product spaces over the ring $\mathbb{Z}/4\mathbb{Z}$.

In Section 4, the formalism of canonical vector spaces is further developed. We begin by introducing the notion of an oriented Lagrangian in $\widetilde{V}$. We then describe an Heisenberg vector bundle $\widetilde{\mathfrak{H}}$ on the set $OLag(\widetilde{V})$ of oriented Lagrangians in $\widetilde{V}$. The main statement is Theorem 4.2 asserting the existence of a natural trivialization of the vector bundle $\widetilde{\mathfrak{H}}^{\otimes 2}$. Using Theorem 4.2, we define the splitting of the Weil gerbe $S : \mathcal{W}^s \rightarrow \mathcal{W}$, which is then used to prove Theorem 1.4.

In Section 5, we describe the construction of the canonical trivialization asserted in Theorem 4.2, specifically, we describe a natural normalization of the canonical intertwining morphisms and the cocycle C which is associated with these normalized intertwining morphisms. The main theorem of this section is Theorem 5.1 which asserts that $C^2 = 1$.

In Appendix, we give the proofs of all technical statements which appear in the body of the paper.

1. The Heisenberg and the Weil representation

1.1. General setting

1.1.1. Fields and rings

Let K be an unramified extension of degree d of the 2-adic completion $\mathbb{Q}_2$. Let $\mathcal{O}_K \subset K$ be the ring of integers, $\mathfrak{m}_K \subset \mathcal{O}_K$ the unique maximal ideal with its standard generator $2 \in \mathfrak{m}_K$ and $k = \mathcal{O}_K/\mathfrak{m}_K$ the residue field, $k = \mathbb{F}_{2^d}$. Finally we denote by R the ring $\mathcal{O}_K/\mathfrak{m}_K^2$ and recall that we have the trace map

$$\mathrm{tr} : R \to \mathbb{Z}/4.$$

1.1.2. Symplectic module

Let $(\widetilde{V}, \widetilde{\omega})$ be a free symplectic module over R of rank $2n$. Let $V = \widetilde{V}/\mathfrak{m}_K$ be the quotient k-vector space. The form $\omega = 2\widetilde{\omega}$ factors to give a non-degenerate skew symmetric form on V with values in R. We denote by $Sp(\widetilde{V}) = Sp(\widetilde{V}, \widetilde{\omega})$ and by $Sp(V) = Sp(V, \omega)$ the corresponding groups of linear symplectomorphisms.

1.1.3. The cocycle associated with a Lagrangian splitting

Let $\widetilde{S}$ be a Lagrangian splitting $\widetilde{V} = \widetilde{L} \times \widetilde{M}$; we define a bilinear form $\widetilde{\beta} = \widetilde{\beta}_{\widetilde{S}} : \widetilde{V} \times \widetilde{V} \to R$, given by $\widetilde{\beta}((\widetilde{l}_1, \widetilde{m}_1), (\widetilde{l}_2, \widetilde{m}_2)) = \widetilde{\omega}(\widetilde{l}_1, \widetilde{m}_2)$, for $\widetilde{l}_i \in \widetilde{L}$ and $\widetilde{m}_i \in \widetilde{M}, i = 1, 2$. Since $\widetilde{\beta}$ is a bilinear form thus it is a cocycle, namely, we have that

$$0 = d\widetilde{\beta}(\widetilde{v}_1, \widetilde{v}_2, \widetilde{v}_3) = \widetilde{\beta}(\widetilde{v}_2, \widetilde{v}_3) - \widetilde{\beta}(\widetilde{v}_1 + \widetilde{v}_2, \widetilde{v}_3) + \widetilde{\beta}(\widetilde{v}_1, \widetilde{v}_2 + \widetilde{v}_3) - \widetilde{\beta}(\widetilde{v}_1, \widetilde{v}_2),$$

for every $\widetilde{v}_1, \widetilde{v}_2, \widetilde{v}_3 \in \widetilde{V}$. In addition, $\widetilde{\beta}(\widetilde{v}_1, \widetilde{v}_2) - \widetilde{\beta}(\widetilde{v}_2, \widetilde{v}_1) = \widetilde{\omega}(\widetilde{v}_1, \widetilde{v}_2)$, for every $\widetilde{v}_1, \widetilde{v}_2 \in \widetilde{V}$. Finally, we consider the form $\beta = 2\widetilde{\beta}$, which factors to give a cocycle on V with values in R, with the property that $\beta(v_1, v_2) - \beta(v_2, v_1) = \omega(v_1, v_2)$.

For the rest of this paper we fix a splitting $\widetilde{S}$ and denote by $\widetilde{\beta}$ and β the corresponding cocycles on $\widetilde{V}$ and V respectively.

1.2. The Heisenberg representation

1.2.1. The Heisenberg group

We consider V as an abelian group. To the pair (V, β) we associate a central extension

$$0 \to R \to H_\beta(V) \to V \to 0.$$

The group $H(V) = H_\beta(V)$ is called the *Heisenberg group* associated with the cocycle β. The Heisenberg group can be presented as $H(V) = V \times R$ with the multiplication given by

$$(v_1, z_1) \cdot (v_2, z_2) = (v_1 + v_2, z_1 + z_2 + \beta(v_1, v_2)).$$

The center of $H(V)$ is $Z = Z_{H(V)} = \{(0, z) : z \in R\}$.

1.2.2. The Heisenberg representation

One of the most important attributes of the group $H(V)$ is that it admits, principally, a unique irreducible representation. This is the Stone–von Neumann property (S–vN property for short). The precise statement goes as follows. Let $\psi : R \to \mathbb{C}^{\times}$ be a faithful character.

Theorem 1.1 (*Stone–von Neumann Property [4]*)**.** *There exists a unique (up to a non-unique isomorphism) irreducible representation* $(\pi, H(V), \mathcal{H})$, *with central character* ψ, *i.e.,* $\pi_{|Z} = \psi \cdot Id_{\mathcal{H}}$.

The representation π which appears in the above theorem will be called the *Heisenberg representation* associated with the central character ψ. For the rest of this paper we take $\psi(z) = e^{\frac{2\pi i}{4}\mathrm{tr}(z)}$.

1.3. The Weil representation

1.3.1. Automorphisms of the Heisenberg group

Let us denote by $ASp(V)$ the group of automorphisms of $H(V)$ acting trivially on the center. The group $ASp(V)$ can be presented as follows. Given an element $g \in Sp(V)$, we denote by Σ_g the set consisting of "quadratic functions" $\alpha : V \to R$ satisfying

$$\alpha(v_1 + v_2) - \alpha(v_1) - \alpha(v_2) = \beta(g(v_1), g(v_2)) - \beta(v_1, v_2),$$

for every $v_1, v_2 \in V$. We can write $ASp(V) = \left\{(g, \alpha) : g \in Sp(V), \alpha \in \Sigma_g\right\}$ with the multiplication rule

$$\left(g, \alpha_g\right) \cdot (h, \alpha_h) = \left(g \cdot h, Ad_{h^{-1}}\left(\alpha_g\right) + \alpha_h\right),$$

where $Ad_{h^{-1}}\left(\alpha_g\right)(v) = \alpha_g(h(v))$, for every $v \in V$. An element $(g, \alpha) \in ASp(V)$ defines the automorphism $(v, z) \longmapsto (g(v), z + \alpha(v))$ of $H(V)$. The group $ASp(V)$ fits into a non-split exact sequence

$$0 \to V^{\vee} \to ASp(V) \to Sp(V) \to 1,$$

where $V^{\vee}$ is the dual group $V^{\vee} = \mathrm{Hom}(V, R)$. We will refer to $ASp(V)$ as the *affine symplectic group*. Finally, we note that the action of $ASp(V)$ on the Heisenberg group, induces an action on the quotient vector space $V = H(V)/Z$, preserving the symplectic form.

It would be instructive to give an explicit description of an element in Σ_g. In order to specify such an element we choose a group element $\widetilde{g} \in Sp(\widetilde{V})$ lying over g. Using this choice, we define $\widetilde{\alpha}_g : \widetilde{V} \to R$ to be the quadratic form given by $\widetilde{\alpha}(\widetilde{v}) = \widetilde{\beta}(\widetilde{g}(\widetilde{v}), \widetilde{g}(\widetilde{v})) - \widetilde{\beta}(\widetilde{v}, \widetilde{v})$.

Lemma 1.2. *The quadratic form* $\widetilde{\alpha}$ *factors to a function* $\alpha_{\widetilde{g}} : V \to R$, *moreover* $\alpha_{\widetilde{g}} \in \Sigma_g$.

For a proof, see Appendix.

1.3.2. The Weil representation

A direct consequence of Theorem 1.1 is the existence of a projective representation $\widetilde{\rho} : ASp(V) \to PGL(\mathcal{H})$. The construction of $\widetilde{\rho}$ from the Heisenberg representation π is rather standard and it goes as follows. Considering the Heisenberg representation π and an element $g \in ASp(V)$, one can define a new representation π^g acting on the same Hilbert space via $\pi^g(h) = \pi(g(h))$. Clearly both π and π^g have the same central character ψ hence by Theorem 1.1 they are isomorphic. Since the space $\mathrm{Hom}_{H(V)}(\pi, \pi^g)$ is one-dimensional, choosing for every $g \in ASp(V)$ a non-zero representative $\widetilde{\rho}(g)$ in $\mathrm{Hom}_{H(V)}(\pi, \pi^g)$ gives a projective representation. The projective representation $\widetilde{\rho}$ is characterized by the relation

$$\widetilde{\rho}(g)\,\pi(h)\,\widetilde{\rho}\left(g^{-1}\right) = \pi(g(h)), \tag{1.1}$$

for every $g \in ASp(V)$ and $h \in H(V)$.

Our goal is to prove the following theorem.

Theorem 1.3 (*The Weil Representation*)**.** *There exists a group $AMp(V)$ which is a central extension of $ASp(V)$ by the group $\mu_4(\mathbb{C}) = \{\pm 1, \pm i\}$ and a linear representation $\rho : AMp(V) \to GL(\mathcal{H})$ lying over $\widetilde{\rho}$.*

For a proof, see Section 2.

1.3.3. Splitting of the Weil representation

We consider the homomorphism

$$Sp(\widetilde{V}) \to ASp(V),$$

sending an element $\widetilde{g} \in Sp(\widetilde{V})$ to the element $(g, \alpha_{\widetilde{g}}) \in ASp(V)$. Where $g \in Sp(V)$ is the reduction of $\widetilde{g}$ mod 2 and $\alpha_{\widetilde{g}} \in \Sigma_g$ is the "quadratic function" associated to the lift $\widetilde{g} \mapsto g$ (see Lemma 1.2). Our goal is to prove the following splitting theorem.

Theorem 1.4. *There exists a group $Mp(\widetilde{V})$ which is a central extension of $Sp(\widetilde{V})$ by the group $\mu_2(\mathbb{C}) = \{\pm 1\}$ and a homomorphism $s : Mp(\widetilde{V}) \to AMp(V)$.*

For a proof, see Section 4.

As a direct consequence of Theorem 1.4 we obtain the representation

$$\rho_{\widetilde{V}} = \rho \circ s : Mp(\widetilde{V}) \to GL(\mathcal{H}).$$

2. Canonical vector spaces

2.1. The canonical vector space

2.1.1. Models of the Heisenberg representation

Although, the representation π is unique, it admits a multitude of different models (realizations). In fact, this is one of its most interesting and powerful attributes. In this paper we will be interested in a particular family of such models associated with *enhanced Lagrangian* subspaces in V.

Definition 2.1. An *enhanced Lagrangian* is a pair (L, τ) where $L \in Lag(V)$ is a Lagrangian subspace and $\tau : L \to H(V)$ is a splitting of the canonical projection $H(V) \to V$. We denote by $ELag(V)$ the set of enhanced Lagrangians.

A concrete way to present an enhanced Lagrangian works as follows. Let $L \in Lag(V)$ and let Σ_L denote the set consisting of "quadratic functions" $\alpha : L \to R$ satisfying

$$\alpha(l_1 + l_2) - \alpha(l_1) - \alpha(l_2) = \beta(l_1, l_2). \tag{2.1}$$

A pair (L, α) yields a homomorphism section $\tau : L \to H(V)$ given by $\tau(l) = (l, \alpha(l))$. Indeed we verify

$$\begin{aligned}\tau(l_1 + l_2) &= (l_1 + l_2, \alpha(l_1 + l_2)) \\ &= (l_1 + l_2, \alpha(l_1) + \alpha(l_2) + \beta(l_1, l_2)) \\ &= \tau(l_1) \cdot \tau(l_2)\end{aligned}$$

where in the second equality we used the characteristic property of α (Eq. (2.1)). Thus, we can think of $ELag(V)$ as the set

$$ELag(V) = \{(L, \alpha) : L \in Lag(V) \text{ and } \alpha \in \Sigma_L\}.$$

To simplify notations, we will often denote an enhanced Lagrangian (L, α_L) simply by L. In situations where the quadratic form α_L is needed we will include it in the notation.

We conclude this discussion with an explicit construction of an element in Σ_L. The construction depends on a choice of a free Lagrangian submodule $\widetilde{L} \in Lag(\widetilde{V})$ in $\widetilde{V}$ laying over L in the sense that $\widetilde{L}/\mathfrak{m}_K\widetilde{L} = L$. Given such a choice, we consider the quadratic form $\widetilde{\beta}_{\widetilde{L}} : \widetilde{L} \to R$ given by $\widetilde{l} \mapsto \widetilde{\beta}(\widetilde{l}, \widetilde{l})$.

Lemma 2.2. *The quadratic form $\widetilde{\beta}_{\widetilde{L}}$ factors through L and yields a "quadratic function" $\alpha_{\widetilde{L}} \in \Sigma_L$.*

For a proof, see Appendix.

2.1.2. Models associated with enhanced Lagrangians

We associate with each enhanced Lagrangian L, a model $(\pi_L, H(V), \mathcal{H}_L)$ of the Heisenberg representation. The vector space $\mathcal{H}_L$ consists of functions $f : H(V) \to \mathbb{C}$ satisfying $f(z \cdot \tau(l) \cdot h) = \psi(z) f(h)$, for every $z \in Z$ and $l \in L$ and the action $\pi_L : H(V) \to GL(\mathcal{H}_L)$ is given by right translations, namely $\pi_L(h)[f](h') = f(h' \cdot h)$, for every $h, h' \in H(V)$.

The collection of models $\{\mathcal{H}_L\}$ forms a vector bundle $\mathfrak{H} \to ELag(V)$ with fiber $\mathfrak{H}_L = \mathcal{H}_L$. In addition, the vector bundle $\mathfrak{H}$ is equipped with a fiberwise action of the Heisenberg group given by $\pi_L : H(V) \to GL(\mathcal{H}_L)$. This suggests the following terminology.

Definition 2.3. Let $n \in \mathbb{N}$. An $H(V)^n$-vector bundle on $ELag(V)$ is a vector bundle $\mathfrak{E} \to ELag(V)$, equipped with a fiberwise action $\pi_L : H(V)^n \to GL(\mathfrak{E}_L)$, for every $L \in ELag(V)$.

2.1.3. The strong Stone–von Neumann property

We proceed to formulate a stronger form of the Stone–von Neumann property of the Heisenberg representation. First, we introduce the following terminology.

Definition 2.4. Let $\mathfrak{E} \to ELag(V)$ be a vector bundle. A *trivialization* of $\mathfrak{E}$ is a system of linear isomorphisms

$$E = \{E_{M,L} : \mathfrak{E}_L \to \mathfrak{E}_M : (M, L) \in ELag(V)^2\},$$

satisfying the multiplicativity condition $E_{N,M} \circ E_{M,L} = E_{N,L}$, for every $N, M, L \in ELag(V)$. In case $\mathfrak{E}$ is an $H(V)^n$-vector bundle, the system E is called an $H(V)^n$-trivialization if each linear map $E_{M,L}$ is an $H(V)^n$-intertwining morphism.

Remark 2.5. Another formal interpretation for a trivialization is the datum consisting of a vector space E and an isomorphism of the vector bundle $\mathfrak{E}$ with the trivial vector bundle with fiber E. Intuitively, a trivialization of a vector bundle $\mathfrak{E} \to ELag(V)$ might be thought of as a flat connection admitting a trivial monodromy.

Theorem 2.6 (*The Strong S–vN Property*)**.** *The $H(V)^4$-vector bundle $\mathfrak{H}^{\otimes 4}$ admits a natural trivialization $\{T_{M,L}\}$.*

For a proof, see Section 3.

2.1.4. The Weil gerbe

We proceed to describe a gerbe $\mathcal{W}$, canonically associated with the vector bundle $\mathfrak{H}$. An object of $\mathcal{W}$ is a triple $(\mathfrak{E}, \{E_{M,L}\}, \varphi)$, where $\mathfrak{E}$ is a vector bundle, $\{E_{M,L} : M, L \in ELag(V)\}$ is a trivialization of $\mathfrak{E}$ and $\varphi : \mathfrak{E} \xrightarrow{\simeq} \mathfrak{H}$ is an isomorphism of vector bundles satisfying that

$$\varphi^{\otimes 4} : \mathfrak{E}^{\otimes 4} \xrightarrow{\simeq} \mathfrak{H}^{\otimes 4}$$

is an isomorphism of trivialized vector bundles. A morphism $f : \mathfrak{E}_1 \to \mathfrak{E}_2$ is a morphism of vector bundles satisfying $\varphi_2^{\otimes 4} \circ f^{\otimes 4} = \varphi_1^{\otimes 4}$.

Proposition 2.7. *The category $\mathcal{W}$ is a gerbe with band $\mu_4(\mathbb{C})$.*

For a proof, see Appendix.

2.1.5. The canonical vector space

Let us denote by Vect the category of complex vector spaces. There is a natural fiber functor $\Gamma : \mathcal{W} \to \mathsf{Vect}$, sending an object $\mathfrak{E} \in \mathcal{W}$ to the vector space of "horizontal sections"

$$\Gamma(\mathfrak{E}) = \Gamma_{hor}(ELag(V), \mathfrak{E}),$$

consisting of compatible systems of vectors $(f_L \in \mathfrak{E}_L : L \in ELag(V))$ such that $E_{M,L}(f_L) = f_M$, for every $(M, L) \in ELag(V)^2$.

2.2. The canonical realization of the Weil representation

2.2.1. Action of the affine symplectic group on the set of enhanced Lagrangians

There is a natural action of the group $ASp(V)$ on the set $ELag(V)$ sending an element (L, τ) to the element $(gL, Ad_g\tau)$ where $Ad_g\tau : gL \to H(V)$ is the map given by $Ad_g\tau(l) = g\tau(g^{-1}(l))$. We note that the set Σ_L is a principal homogeneous set over the dual group $L^{\vee} = \mathrm{Hom}(L, R)$.

2.2.2. Action of the affine symplectic group on the vector bundle of Heisenberg models

The vector bundle $\mathfrak{H}$ is equipped with a natural $ASp(V)$-equivariant structure, defined as follows. For every $g \in ASp(V)$, let $g^*\mathfrak{H}$ be the $H(V)$-vector bundle with fibers $g^*\mathfrak{H}_L = \mathcal{H}_{gL}$ and the g-twisted Heisenberg action $\pi_L^g : H(V) \to GL(\mathcal{H}_{gL})$, given by $\pi_L^g(h) = \pi_{gL}(g(h))$. The equivariant structure is the isomorphisms of $H(V)$-vector bundles

$$\theta_g : g^*\mathfrak{H} \to \mathfrak{H}, \tag{2.2}$$

which on the level of fibers, sends $f \in \mathcal{H}_{gL}$ to $f \circ g \in \mathcal{H}_L$.

2.2.3. Action of the affine symplectic group on the Weil gerbe

We describe an action of the affine symplectic group $ASp(V)$ on the Weil gerbe. The action of an element $g \in ASp(V)$ is given by the pull-back functor $g^* : \mathcal{W} \to \mathcal{W}$, sending an object $(\mathfrak{E}, \{E_{M,L}\}, \varphi)$ to the object $(g^*\mathfrak{E}, \{g^*E_{M,L}\}, \varphi^g)$ where $g^*\mathfrak{E}$ is the pull-back vector bundle, $\{g^*E_{M,L} : M, L \in ELag(V)\}$ is the pull-back trivialization given by $g^*E_{M,L} = E_{gM,gL}$ and φ^g is the isomorphism given by

$$\varphi^g = \theta_g \circ g^*\varphi,$$

where $\theta_g : g^*\mathfrak{H} \to \mathfrak{H}$ is the equivariant structure on $\mathfrak{H}$ (see Eq. (2.2)). Furthermore, there is a central extension $AMp(V)$ of the group $ASp(V)$ naturally associated with the action of $ASp(V)$ on $\mathcal{W}$. This group consists of pairs (g, ι), where $g \in ASp(V)$ and ι is an isomorphism $\iota : g^* \xrightarrow{\simeq} Id$ between the pullback functor g^* and the identity functor.

The multiplication rule is defined as follows. Given a pair of elements $(g, \iota_g), (h, \iota_h) \in AMp(V)$, their multiplication is given by

$$(g, \iota_g) \cdot (h, \iota_h) = (g \cdot h, \iota),$$

where $\iota : (gh)^* \xrightarrow{\simeq} Id$ is the composition $\iota = \iota_h \circ h^*(\iota_g)$.

Proposition 2.8. *The group $AMp(V)$ is a central extension of the group $ASp(V)$ by $\mu_4(\mathbb{C})$, in particular it fits into an exact sequence of groups*

$$1 \to \mu_4(\mathbb{C}) \to AMp(V) \to ASp(V) \to 1.$$

For a proof, see Appendix.

2.2.4. The canonical realization of the Weil representation

We describe a natural homomorphism $\rho : AMp(V) \to Aut(\Gamma)$ defined as follows. Given an element $(g, \iota) \in ASp(V)$, the automorphism $\rho(g, \iota) : \Gamma \to \Gamma$ is given by the composition

$$\Gamma \xrightarrow{\simeq} \Gamma \circ g^* \xrightarrow{\Gamma(\iota)} \Gamma \circ Id = \Gamma,$$

where the first morphism is the tautological isomorphism. We refer to the homomorphism ρ as the canonical model of the Weil representation; in more scientific terms, ρ is an action of the group $AMp(V)$ on a vector space twisted by the gerbe $\mathcal{W}$. We obtain a more traditional realization of the Weil representation, after choosing a specific object $\mathfrak{E} \in \mathcal{W}$. Such a choice yields a homomorphism

$$\rho_{\mathfrak{E}} : AMp(V) \to GL(\Gamma(\mathfrak{E})).$$

As a consequence we proved Theorem 1.3.

3. The strong Stone–von Neumann property

In this section we describe the construction of the canonical trivialization of the vector bundle $\mathfrak{H}^{\otimes 4}$, asserted in Theorem 2.6.

3.1. Canonical intertwining morphisms

The vector bundle $\mathfrak{H}$ admits a partial "connective structure" which we proceed to describe. Let $U_2 \subset ELag(V)^2$ denote the subset consisting of pairs of enhanced Lagrangians (M, L)

in *general position*, namely, such that $M + L = V$. For every pair $(M, L) \in U_2$, there exists a canonical intertwining morphism $F_{M,L} \in \mathrm{Hom}_{H(V)}(\mathcal{H}_L, \mathcal{H}_M)$, given by the following averaging formula

$$F_{M,L}[f](h) = \sum_{m \in M} f(\tau(m) \cdot h),$$

for every $f \in \mathcal{H}_L$, where $\tau : M \to H(V)$ is the enhanced structure for M. Let $U_3 \subset ELag(V)^3$ denote the subset consisting of triples of enhanced Lagrangians (N, M, L) which are in general position pairwisely. For every $(N, M, L) \in U_3$, we can form two intertwining morphisms from $\mathcal{H}_L$ to $\mathcal{H}_N$. The first is $F_{N,L}$ and the second is the composition $F_{N,M} \circ F_{M,L}$. Since $\mathcal{H}_L$ and $\mathcal{H}_M$ are both isomorphic to the Heisenberg representation which is irreducible we conclude that $F_{N,L}$ and $F_{N,M} \circ F_{M,L}$ differ by a multiple of a non-zero complex number

$$F_{N,M} \circ F_{M,L} = C(N, M, L) \cdot F_{N,L}.$$

The function $C : U_3 \to \mathbb{C}$ is a cocycle with respect to an appropriately defined differential and, moreover, it can be described explicitly as a kind of "Gauss sum". To this end, we need to introduce some additional terminology. Let $r^L : M \to N$ denote the linear map characterized by the condition

$$r^L(m) - m \in L,$$

for every $m \in M$. Equivalent characterization of r^L is the condition

$$\omega\left(r^L(m), l\right) = \omega(m, l),$$

for every $m \in M$ and $l \in L$. Let us fix a triple of enhanced Lagrangians $N = (N, \alpha_N)$, $M = (M, \alpha_M)$ and $L = (L, \alpha_L)$ and let $Q_{(N,M,L)} : M \to R$ denote the "quadratic function"

$$Q_{(N,M,L)}(m) = \alpha_M(m) + \alpha_N\left(-r^L(m)\right) - \alpha_L\left(m - r^L(m)\right) - \beta\left(m, r^L(m)\right). \quad (3.1)$$

Proposition 3.1. *We have*

$$C(N, M, L) = \sum_{m \in M} \psi\left(Q_{(N,M,L)}(m)\right).$$

For a proof, see Appendix.

Based on the analysis of inner product spaces over the ring $\mathbb{Z}/4$ which will be done in sequel, we will prove the following important technical result.

Theorem 3.2. *For every $(N, M, L) \in U_3$, we have*

$$C(N, M, L)^4 = (-1)^{d \cdot n} \cdot |M|^2$$

where d is the degree $[k : \mathbb{F}_2]$ and $2n$ is the dimension of the symplectic vector space V over the field k.

Specifically, Theorem 3.2 will follow from Theorem 3.4, which appears below. Using Theorem 3.2 we exhibit the canonical trivialization of the vector bundle $\mathfrak{H}^{\otimes 4}$. We define the normalized intertwining morphism

$$T_{M,L} = A_{M,L} \cdot F_{M,L}^{\otimes 4},$$

for every $(M, L) \in U_2$. The normalization coefficient $A_{M,L}$ is given $A_{M,L} = \frac{(-1)^{d \cdot n}}{|M|^2}$. It can be easily checked that the normalization coefficients satisfy the condition

$$A_{N,M} \cdot A_{M,L} = \frac{(-1)^{d \cdot n}}{|M|^2} A_{N,L},$$

for every $(N, M, L) \in U_3$. Thus, based on Theorem 3.2, we have the multiplicativity condition

$$T_{N,M} \circ T_{M,L} = T_{N,L}, \tag{3.2}$$

for every $(N, M, L) \in U_3$. This condition enables to extend the definition of T to every pair of enhanced Lagrangians (including such pairs that are not in general position).

Theorem 3.3. *The partial trivialization $\left\{T_{M,L} : (M, L) \in U_2\right\}$ extends, in a unique manner, to a trivialization of $\mathfrak{H}^{\otimes 4}$.*

For a proof, see Appendix.

The rest of this section is devoted to the proof of Theorem 3.2. The proof consists of two main steps. In the first step we massage the formula of the cocycle $C(N, M, L)$ to fit in the setting of inner product spaces over the ring $\mathbb{Z}/4\mathbb{Z}$. In the second step we develop the structure theory of inner product spaces over $\mathbb{Z}/4\mathbb{Z}$ which is then applied to prove the theorem.

3.2. Simplification of the cocycle

We proceed to introduce a simplification of the cocycle formula (3.1) which depends on a choice of a free Lagrangian submodules $\widetilde{N}, \widetilde{M}, \widetilde{L}$ in $\widetilde{V}$ lying over N, M and L respectively. Given such a choice, we can write

$$\alpha_N = \alpha_{\widetilde{N}} + \sigma_N,$$
$$\alpha_M = \alpha_{\widetilde{M}} + \sigma_M,$$
$$\alpha_L = \alpha_{\widetilde{L}} + \sigma_L,$$

where $\alpha_{\widetilde{N}} \in \Sigma_N, \alpha_{\widetilde{M}} \in \Sigma_M$ and $\alpha_{\widetilde{L}} \in \Sigma_L$ are the enhanced structures associated with the liftings (see Lemma 2.2) and $\sigma_N \in N^\vee, \sigma_M \in M^\vee$ and $\sigma_L \in L^\vee$ are characters (taking values in R). Let us denote $Q = Q_{(N,M,L)}$ and let $\widetilde{m}$ be an element in $\widetilde{M}$ lying over $m \in M$. Simple verification reveals that

$$Q(m) = \widetilde{\omega}(r^{\widetilde{L}}(\widetilde{m}), \widetilde{m}) + \sigma(m), \tag{3.3}$$

where σ is the character in $M^\vee$ given by

$$\sigma(m) = \sigma_M(m) + \sigma_N\left(-r^L(m)\right) - \sigma_L\left(m - r^L(m)\right).$$

Here $r^{\widetilde{L}} : \widetilde{M} \to \widetilde{N}$ is the linear map characterized by the condition $r^{\widetilde{L}}(\widetilde{m}) - \widetilde{m} \in \widetilde{L}$, for every $\widetilde{m} \in \widetilde{M}$. We introduce the following notations. Let $\widetilde{\omega}_{\widetilde{L}} : \widetilde{M} \times \widetilde{M} \to R$ denote the bilinear form $\widetilde{\omega}(r^{\widetilde{L}}(\cdot), \cdot)$ and $\omega_L : M \times M \to R$ denote the bilinear form $\omega(r^L(\cdot), \cdot)$.

Evidently, the form $2\widetilde{\omega}_{\widetilde{L}}$ reduces to the form ω_L. Since ω_L is non-degenerate, there exists a unique element $m_\sigma \in M$ such that $\omega_L(m_\sigma, \cdot) = \sigma(\cdot)$. Choosing an element $\widetilde{m}_\sigma \in \widetilde{M}$ lying over m_σ, we can write

$$Q(m) = \widetilde{\omega}_{\widetilde{L}}(\widetilde{m} + \widetilde{m}_\sigma, \widetilde{m} + \widetilde{m}_\sigma) - \widetilde{\omega}_{\widetilde{L}}(\widetilde{m}_\sigma, \widetilde{m}_\sigma).$$

Hence

$$C(N,M,L) = \psi\left(-\widetilde{\omega}_{\widetilde{L}}(\widetilde{m}_\sigma,\widetilde{m}_\sigma)\right)\sum_{m\in M}\psi\left(\widetilde{\omega}_{\widetilde{L}}(\widetilde{m},\widetilde{m})\right). \tag{3.4}$$

Let $G([\widetilde{M},\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})])$ denote the "Gauss sum"

$$\begin{aligned} G([\widetilde{M},\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})]) &= \sum_{m\in M}\psi\left(\widetilde{\omega}_{\widetilde{L}}(\widetilde{m},\widetilde{m})\right) \\ &= \sum_{m\in M} e^{\frac{2\pi i}{4}\mathrm{tr}\left(\widetilde{\omega}_{\widetilde{L}}(\widetilde{m},\widetilde{m})\right)}. \end{aligned}$$

Since $\psi\left(-\widetilde{\omega}_{\widetilde{L}}(\widetilde{m}_\sigma,\widetilde{m}_\sigma)\right) \in \mu_4(\mathbb{C})$, the assertion that $C(N,M,L)^4 = (-1)^{d\cdot n}\cdot|M|^2$ will follow from the following statement.

Theorem 3.4. *We have*

$$G([\widetilde{M},\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})])^4 = (-1)^{d\cdot n}\cdot|M|^2.$$

The proof of Theorem 3.4, will appear in Section 3.5 after we develop some appropriate formalism.

3.3. Inner product spaces

Let A be a ring and let $\mathcal{B}(A)$ denote the category of *inner product spaces* over A. An object in $\mathcal{B}(A)$ is a pair (V,B), where V is a free module over A and $B : V\times V\to A$ is a non-degenerate symmetric bilinear form on V. A morphism $f \in \mathrm{Mor}_{\mathcal{B}(A)}((V_1,B_1),(V_2,B_2))$ is a map of A-modules $f : V_1\to V_2$, such that $B_2(f(v_1),f(v_2)) = B_1(v_1,v_2)$, for every $v_1,v_2\in V$. The category $\mathcal{B}(A)$ has a monoidal structure given by the operation of direct-sum of inner product spaces.

Let us denote by $\mathrm{W}(A) = (\mathrm{Iso}(\mathcal{B}(A)),+)$ the associated commutative monoid, whose elements are isomorphism classes of objects in $\mathcal{B}(A)$ and $+$ is the binary operation induced from the monoidal structure in $\mathcal{B}(A)$. Given an object $(V,B)\in\mathcal{B}(A)$ we will denote by $[V,B]$ its isomorphism class in $\mathrm{W}(A)$. More concretely, given a symmetric matrix $M\in\mathrm{Mat}_{n\times n}(A)$, we will denote by $[M]$ the isomorphism class of (A^n,B_M), where

$$B_M\left(\overrightarrow{x},\overrightarrow{y}\right) = \overrightarrow{x}^t\cdot M\cdot\overrightarrow{y}.$$

3.3.1. The discriminant

We now describe an important morphism of monoids $d : \mathrm{W}(A)\to A^\times/A^{\times 2}$ called the *discriminant*. Given an element $[V,B]\in\mathrm{W}(A)$, the discriminant $d([V,B])$ can be defined as follows. Choose an isomorphism $f : V\simeq A^n$, $n = rk(V)$; let B_0 denote the standard symmetric form on A^n given by

$$B_0\left(\overrightarrow{x},\overrightarrow{y}\right) = x_1\cdot y_1+\cdots+x_n\cdot y_n.$$

Define $d([V,B]) = \det(B/f^*(B_0))$. This procedure yields a well defined element in $A^\times/A^{\times 2}$ (and element which does not depend on the choice of the isomorphism f). We denote $\mathcal{B} = \mathcal{B}(\mathbb{Z}/4\mathbb{Z})$ and $\mathrm{W} = \mathrm{W}(\mathbb{Z}/4\mathbb{Z})$ and refer to W as the *Witt–Grothendieck monoid*.

3.3.2. The structure of the Witt–Grothendieck monoid

The fine structure of the Witt–Grothendieck monoid is specified in the following two propositions. The first proposition asserts that every element in W can be written in a standard form as a combination of four types of generators. The second proposition specifies some basic relations satisfied by these generators.

Proposition 3.5 (*Witt Generators*)**.** *Let* $[V, B] \in \mathrm{W}$ *then*

$$[V, B] = n_1 \cdot [1] + n_2 \cdot [-1] + n_3 \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + n_4 \cdot \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix},$$

where $n_i \in \mathbb{N}$, $i = 1, 2, 3, 4$.

For a proof, see Appendix.

Proposition 3.6 (*Witt Relations*)**.** *The following relations hold in* W

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{3.5}$$

$$3 \cdot [1] = [-1] + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \tag{3.6}$$

$$3 \cdot [-1] = [1] + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}. \tag{3.7}$$

For a proof, see Appendix.

3.4. The Gauss character and the Witt group

We proceed to describe a morphism of monoids $G = G_\psi : \mathrm{W} \to \mathbb{C}^\times$, which we call the *Gauss character*. It is defined as follows. To an isomorphism class $[V, B] \in \mathrm{W}$, we associate the following complex number

$$G([V, B]) = \sum_{v \in V/2V} \psi(B(v, v)).$$

The number $G([V, B])$ does not depend on the representative $(V, B) \in \mathcal{B}$ and summing over the quotient $V/2V$ makes sense since the quadratic function $B(v, v)$ factors through $V/2V$. The rule $G : \mathrm{W} \to \mathbb{C}^\times$ establishes a homomorphism of monoids, namely

$$G([V_1, B_1] + [V_2, B_2]) = G([V_1, B_1]) \cdot G([V_2, B_2]),$$

for every $[V_1, B_1], [V_2, B_2] \in \mathrm{W}$. Using Proposition 3.5 about the generators of the Weil monoid we obtain the first fundamental statement about Gauss sums in the $\mathbb{Z}/4$ setting.

Theorem 3.7 (*Purity Theorem*)**.** *For every* $[V, B] \in \mathrm{W}$

$$|G([V, B])| = 2^{rk(V)/2} = |V/2V|^{1/2}.$$

For a proof, see Appendix.

Furthermore, let $I \subset \mathrm{W}$ be the submonoid consisting of elements $[V, B] \in \mathrm{W}$ such that $G([V, B]) \in 2^{\mathbb{Z}}$. Using both Propositions 3.5 and 3.6, we obtain the second fundamental statement about Gauss sums in the $\mathbb{Z}/4$ setting.

Theorem 3.8. *The submonoid I is generated by the elements*

$$[1]+[-1]\,,\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}.$$

Moreover, the quotient monoid W/I *is a group, isomorphic to* $\mathbb{Z}/8\mathbb{Z}$.

For a proof, see Appendix.

We denote $\mathrm{GW}=\mathrm{W}/I$ and refer to it as the *Witt group*.

3.5. Proof of Theorem 3.4

We are now ready to prove Theorem 3.4. Since $\widetilde{\omega}_{\widetilde{L}}:\widetilde{M}\times\widetilde{M}\rightarrow R$ is a non-degenerate symmetric form over the ring R, it implies that $\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}}):\widetilde{M}\times\widetilde{M}\rightarrow\mathbb{Z}/4\mathbb{Z}$ is a non-degenerate symmetric form over $\mathbb{Z}/4\mathbb{Z}$. We consider $(\widetilde{M},\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}}))$ as an object in $\mathcal{B}$ and denote by $[\widetilde{M},\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})]$ its class in W. Let $\mathbf{4}\in\mathrm{GW}$ denote the unique non-trivial element of order 2.

Proposition 3.9. *For every* $[V,B]\in\mathrm{GW}$*, we have*

$$4\cdot[V,B]=rk\,(V)\cdot\mathbf{4}.$$

For a proof, see Appendix.

The purity theorem (Theorem 3.7) and Proposition 3.9 imply that

Corollary 3.10. *For every* $[V,B]\in\mathrm{W}$*, we have*

$$G\,(4\cdot[V,B])=(-1)^{rk(V)}\cdot|V/2V|^2\,.$$

Combining all of the above we obtain

$$\begin{aligned}G([\widetilde{M},\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})])^4&=G(4\cdot[\widetilde{M},\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})])\\&=(-1)^{rk(\widetilde{M})}\cdot|M|^2=(-1)^{d\cdot n}\cdot|M|^2\,,\end{aligned}$$

where, in the first equality we used the fact that G is a morphism of monoids, in the second equality we used Corollary 3.10 and in the third equality we used the fact that the rank of $\widetilde{M}$ considered as a module over $\mathbb{Z}/4\mathbb{Z}$ is $d\cdot n$ where $d=[k:\mathbb{F}_2]$ and $\dim V=2n$.

This concludes the proof of the theorem.

4. Splitting of the canonical vector space

4.1. Splitting of the Weil gerbe

4.1.1. The pull-back vector bundle

We consider the symplectic module $(\widetilde{V},\widetilde{\omega})$.

Definition 4.1. An *oriented Lagrangian* in $\widetilde{V}$ is a pair $(\widetilde{L},o)$, where $\widetilde{L}\in Lag(\widetilde{V})$ is a free Lagrangian sub-module of $\widetilde{V}$ and $o\in\wedge^n\widetilde{L}$ is an element such that $R\cdot o=\wedge^n\widetilde{L}$.

Let us denote by $OLag(\widetilde{V})$ the set of oriented Lagrangians in $\widetilde{V}$. To simplify notations, we will often denote an oriented Lagrangian $(\widetilde{L}, o)$ simply by $\widetilde{L}$. We define the map

$$\pi : OLag(\widetilde{V}) \to ELag\,(V)\,,$$

sending an oriented Lagrangian $(\widetilde{L}, o)$ to the enhanced Lagrangian $(L, \alpha_{\widetilde{L}})$, where $L = \widetilde{L}/2\widetilde{L}$ and $\alpha_{\widetilde{L}} \in \Sigma_L$ is the enhanced structure associated with the lift $\widetilde{L} \to L$ (see Lemma 2.2). Let us denote by $\widetilde{\mathfrak{H}}$ the $H(V)$-vector bundle given by the pull-back $\widetilde{\mathfrak{H}} = \pi^*\mathfrak{H}$. The $H(V)^4$-vector bundle $\widetilde{\mathfrak{H}}^{\otimes 4}$ admits a trivialization $\{T_{\widetilde{M},\widetilde{L}}\}$ which is induced from the trivialization of $\mathfrak{H}^{\otimes 4}$ (see Theorem 2.6).

4.1.2. Square root of the canonical trivialization

The following statements concerns the existence of a natural square root of the trivialized $H(V)^4$-vector bundle $\widetilde{\mathfrak{H}}^{\otimes 4}$.

Theorem 4.2 (*The Strong S–vN Property—Split Form*)**.** *The $H(V)^2$-vector bundle $\widetilde{\mathfrak{H}}^{\otimes 2}$ admits a natural trivialization $\{S_{\widetilde{M},\widetilde{L}}\}$ which satisfies*

$$S^{\otimes 2}_{\widetilde{M},\widetilde{L}} = T_{\widetilde{M},\widetilde{L}},$$

for every $(\widetilde{M}, \widetilde{L}) \in OLag(\widetilde{V})^2$.

For a proof, see Section 5.

4.1.3. Splitting of the Weil gerbe

We proceed to describe a natural splitting of the Weil gerbe $\mathcal{W}$. In more precise terms, we construct a gerbe $\mathcal{W}^s$, with band $\mu_2(\mathbb{C})$ and a faithful functor $S : \mathcal{W}^s \to \mathcal{W}$. The definition of the gerbe $\mathcal{W}^s$ proceeds as follows. There are two gerbes which are naturally associated with the vector bundle $\widetilde{\mathfrak{H}}$. The first gerbe, denoted by $\widetilde{\mathcal{W}}$, has band $\mu_4(\mathbb{C})$ and is associated with the trivialization of $\widetilde{\mathfrak{H}}^{\otimes 4}$. The second gerbe, denoted by $\widetilde{\mathcal{W}}^s$, has band $\mu_2(\mathbb{C})$ and is associated with the trivialization of $\widetilde{\mathfrak{H}}^{\otimes 2}$ (see Theorem 4.2). The definition of these gerbes is in complete analogy to the definition of the Weil gerbe $\mathcal{W}$ (see Section 2.1.4).

In addition, there are two evident functors. The first functor is a fully faithful functor $\pi^* : \mathcal{W} \to \widetilde{\mathcal{W}}$, sending an object $\mathfrak{E} \in \mathcal{W}$ to its pull-back $\pi^*\mathfrak{E} \in \widetilde{\mathcal{W}}$. The second functor is the obvious faithful functor $\widetilde{S} : \widetilde{\mathcal{W}}^s \to \widetilde{\mathcal{W}}$ acting as identity on objects and morphisms. We define the gerbe $\mathcal{W}^s$ to be the fiber product category

$$\mathcal{W}^s = \widetilde{\mathcal{W}}^s \times_{\widetilde{\mathcal{W}}} \mathcal{W}.$$

In more concrete terms, an object of $\mathcal{W}^s$ is a triple $(\widetilde{\mathfrak{E}}, \mathfrak{E}, \alpha)$, where $\widetilde{\mathfrak{E}} \in \widetilde{\mathcal{W}}^s$, $\mathfrak{E} \in \mathcal{W}$ and $\alpha \in \mathrm{Mor}_{\widetilde{\mathcal{W}}}(\widetilde{S}(\widetilde{\mathfrak{E}}), \pi^*(\mathfrak{E}))$; and a morphism in $\mathrm{Mor}_{\mathcal{W}^s}((\widetilde{\mathfrak{E}}_1, \mathfrak{E}_1, \alpha_1), (\widetilde{\mathfrak{E}}_2, \mathfrak{E}_2, \alpha_2))$ is a pair of morphisms $(\widetilde{f}, f)$, with $\widetilde{f} \in \mathrm{Mor}_{\widetilde{\mathcal{W}}^s}(\widetilde{\mathfrak{E}}_1, \widetilde{\mathfrak{E}}_2)$ and $f \in \mathrm{Mor}_{\mathcal{W}}(\mathfrak{E}_1, \mathfrak{E}_2)$ so that the following compatibility condition is satisfied

$$\alpha_2 \circ \widetilde{S}(\widetilde{f}) = \pi^*(f) \circ \alpha_1.$$

Proposition 4.3. *The category $\mathcal{W}^s$ is a gerbe with band $\mu_2(\mathbb{C})$.*

For a proof, see Appendix.

Finally, we define the splitting functor $S : \mathcal{W}^s \to \mathcal{W}$ to be the functor which sends an object $(\widetilde{\mathfrak{E}}, \mathfrak{E}, \alpha) \in \mathcal{W}^s$ to the object $\mathfrak{E} \in \mathcal{W}$.

4.2. *Splitting of the Weil representation*

4.2.1. *Action of the symplectic group*

The symplectic group $Sp(\widetilde{V})$ naturally acts on the gerbes $\mathcal{W}$, $\widetilde{\mathcal{W}}$, $\widetilde{\mathcal{W}}^s$ and $\mathcal{W}^s$. The definition of these actions is in complete analogy to the definition of the action of the affine symplectic group $ASp\,(V)$ on the Weil gerbe $\mathcal{W}$ (see Section 2.1.4). Moreover, the functors π^*, $\widetilde{S}$ and S are compatible with the above actions.

In complete analogy to the definition of the central extension $AMp\,(V)$ (see Section 2.1.4), there is a central extension

$$1 \to \mu_2\,(\mathbb{C}) \to Mp(\widetilde{V}) \to Sp(\widetilde{V}) \to 1,$$

naturally associated with the action of $Sp(\widetilde{V})$ on the of gerbe $\mathcal{W}^s$. An element of the group $Mp(\widetilde{V})$ is a pair $(\widetilde{g},\widetilde{\iota})$ where $\widetilde{g} \in Sp(\widetilde{V})$ and $\widetilde{\iota}$ is an isomorphism of functors $\iota : \widetilde{g}^* \xrightarrow{\simeq} Id$.

4.2.2. *The splitting homomorphism*

The splitting functor $S : \mathcal{W}^s \to \mathcal{W}$ induces a homomorphism

$$s : Mp(\widetilde{V}) \to AMp\,(V)\,,$$

sending an element $(\widetilde{g},\widetilde{\iota}) \in Mp(\widetilde{V})$ to the element $(g,\iota) \in ASp(V)$ where $g = \left(\widetilde{g}, \alpha_{\widetilde{g}}\right)$ and $\iota : g^* \to Id$ is the composition

$$g^*\,(S\,(\mathfrak{E})) \xrightarrow{\simeq} S\left(g^*\,(\mathfrak{E})\right) \xrightarrow{S(\widetilde{\iota})} S\,(\mathfrak{E})\,,$$

for every $\mathfrak{E} \in \mathcal{W}^s$. This proves, in particular, Theorem 1.4.

5. The strong S–vN property—split form

In this section we describe the construction of the trivialization of the vector bundle $\widetilde{\mathfrak{H}}^{\otimes 2}$, which is asserted in Theorem 4.2.

5.1. *Canonical intertwining morphisms*

We proceed along similar lines as in Section 3.1. Let $\widetilde{U}_2 \subset OLag(\widetilde{V})^2$ denote the subset consisting of pairs of oriented Lagrangians $(\widetilde{M}, \widetilde{L})$ which are in general position, namely, such that $\widetilde{M} + \widetilde{L} = \widetilde{V}$. For every $(\widetilde{M}, \widetilde{L}) \in \widetilde{U}_2$, there is a canonical intertwining morphism $F_{\widetilde{M},\widetilde{L}}$ from $\mathcal{H}_L$ to $\mathcal{H}_M$ given by

$$F_{\widetilde{M},\widetilde{L}}\,[f]\,(h) = \sum_{m\in M} f\,(\tau\,(m)\cdot h)\,,$$

for every $f \in \mathcal{H}_L$, where $\tau : M \to H\,(V)$ is the enhanced Lagrangian $\pi(\widetilde{M})$. Let $\widetilde{U}_3 \subset OLag(\widetilde{V})^3$ denote the subset consisting of triples of oriented Lagrangians $(\widetilde{N}, \widetilde{M}, \widetilde{L})$ which are in general position pairwisely. For every $(\widetilde{N}, \widetilde{M}, \widetilde{L}) \in \widetilde{U}_3$ the intertwining morphisms $F_{\widetilde{N},\widetilde{L}}$ and $F_{\widetilde{N},\widetilde{M}} \circ F_{\widetilde{M},\widetilde{L}}$ differ by multiplicative complex number

$$F_{\widetilde{N},\widetilde{M}} \circ F_{\widetilde{M},\widetilde{L}} = C(\widetilde{N}, \widetilde{M}, \widetilde{L}) \cdot F_{\widetilde{N},\widetilde{L}}.$$

As a particular case of Formula (3.4) is an expression of the function $C : \widetilde{U}_3 \to \mathbb{C}$ as a Gauss sum on the Lagrangian $\widetilde{M}$ given by

$$C(\widetilde{N}, \widetilde{M}, \widetilde{L}) = G([\widetilde{M}, \mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})]). \tag{5.1}$$

5.2. Normalization coefficients

For every $(\widetilde{M}, \widetilde{L}) \in \widetilde{U}_2$ define the normalization coefficient

$$A_{\widetilde{M},\widetilde{L}} = G(2[R^n, \mathrm{tr}(B_{\widetilde{M},\widetilde{L}})]),$$

where $B_{\widetilde{M},\widetilde{L}} : R^n \times R^n \to R$ denote the symmetric bilinear form

$$B_{\widetilde{M},\widetilde{L}}(\overrightarrow{x}, \overrightarrow{y}) = x_1 \cdot y_1 + \cdots + x_{n-1} \cdot y_{n-1} + \widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{M}}) x_n \cdot y_n,$$

where $\widetilde{\omega}_\wedge : \wedge^n \widetilde{L} \times \wedge^n \widetilde{M} \to R$ is the pairing induced from the symplectic form $\widetilde{\omega}$. The normalization coefficients satisfy the following relation.

Theorem 5.1. *For every $(\widetilde{N}, \widetilde{M}, \widetilde{L}) \in \widetilde{U}_3$, we have*

$$A_{\widetilde{N},\widetilde{M}} \cdot A_{\widetilde{M},\widetilde{L}} = G(2[\widetilde{M}, -\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})]) \cdot A_{\widetilde{N},\widetilde{L}}.$$

The proof of Theorem 5.1 appears in Section 5.4.

5.3. Normalized intertwining morphisms

We are now ready to exhibit the trivialization of the vector bundle $\widetilde{\mathfrak{H}}^{\otimes 2}$. First we define a partial trivialization as follows. Let $S_{\widetilde{M},\widetilde{L}}$ be the normalized intertwining morphism

$$S_{\widetilde{M},\widetilde{L}} = \frac{A_{\widetilde{M},\widetilde{L}}}{|M|^2} \cdot F^{\otimes 2}_{\widetilde{M},\widetilde{L}}.$$

For every $(\widetilde{M}, \widetilde{L}) \in \widetilde{U}_2$. We have for every $(\widetilde{N}, \widetilde{M}, \widetilde{L}) \in \widetilde{U}_3$

$$\begin{aligned} S_{\widetilde{N},\widetilde{M}} \circ S_{\widetilde{M},\widetilde{L}} &= \frac{A_{\widetilde{N},\widetilde{M}} \cdot A_{\widetilde{M},\widetilde{L}}}{|M|^4} F^{\otimes 2}_{\widetilde{N},\widetilde{L}} \circ F^{\otimes 2}_{\widetilde{M},\widetilde{L}} \\ &= \frac{G(2[\widetilde{M}, -\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})]) \cdot A_{\widetilde{N},\widetilde{L}}}{|M|^4} G(2[\widetilde{M}, \mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})]) \cdot F^{\otimes 2}_{\widetilde{N},\widetilde{L}} \\ &= \frac{G(2[\widetilde{M}, -\mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})] + 2[\widetilde{M}, \mathrm{tr}(\widetilde{\omega}_{\widetilde{L}})])}{|M|^2} S_{\widetilde{N},\widetilde{L}} = S_{\widetilde{N},\widetilde{L}}, \end{aligned}$$

where in the second equality we used Formula (5.1) and Theorem 5.1 and in the third equality we used the purity theorem (Theorem 3.7) for the Gauss character and the fact that $G([V, B]) = \overline{G([V, -B])}$, for every $(V, B) \in \mathcal{B}$. Follows similar lines as the proof of Theorem 3.3 we conclude that:

Theorem 5.2. *The partial trivialization $\{S_{\widetilde{M},\widetilde{L}} : (\widetilde{M}, \widetilde{L}) \in \widetilde{U}_2\}$ extends, in a unique manner, to a trivialization of $\widetilde{\mathfrak{H}}^{\otimes 2}$.*

We are left to show that for every $(\widetilde{M}, \widetilde{L}) \in OLag(\widetilde{V})^2$, we have that

$$S^{\otimes 2}_{\widetilde{M},\widetilde{L}} = T_{\widetilde{M},\widetilde{L}}.$$

It is enough to verify this in the case $(\widetilde{M}, \widetilde{L}) \in \widetilde{U}_2$, which can be done by direct computation

$$\begin{aligned} S^{\otimes 2}_{\widetilde{M},\widetilde{L}} &= \frac{G(2[R^n, \operatorname{tr}(B_{\widetilde{M},\widetilde{L}})])^2}{|M|^4} F^{\otimes 2}_{\widetilde{M},\widetilde{L}} \\ &= \frac{G(4[R^n, \operatorname{tr}(B_{\widetilde{M},\widetilde{L}})])}{|M|^4} F^{\otimes 2}_{\widetilde{M},\widetilde{L}} \\ &= \frac{(-1)^{rk(R^n)} \cdot |M|^2}{|M|^4} F^{\otimes 2}_{\widetilde{M},\widetilde{L}} = \frac{(-1)^{d\cdot n}}{|M|^2} F^{\otimes 2}_{\widetilde{M},\widetilde{L}} = T_{\widetilde{M},\widetilde{L}}, \end{aligned}$$

where in the second equality we used the fact that G is a morphism of monoids, in the third equality we used Corollary 3.10 and in the fourth equality we used the fact that the rank of R^n as a module over $\mathbb{Z}/4\mathbb{Z}$ is $d \cdot n$.

5.4. *Proof of Theorem 5.1*

First we note that by the purity theorem (Theorem 3.7) it is enough to show that in GW the following relation holds

$$2[\widetilde{M}, \operatorname{tr}(\widetilde{\omega}_{\widetilde{L}})] + 2[\operatorname{tr}(B_{\widetilde{N},\widetilde{M}})] + 2[\operatorname{tr}(B_{\widetilde{M},\widetilde{L}})] + 2[-\operatorname{tr}(B_{\widetilde{N},\widetilde{L}})] = \mathbf{0},$$

where we use the abbreviated notation $[\operatorname{tr}(B)]$ for $[R^n, \operatorname{tr}(B)]$. Let us denote by X the following element in W

$$X = [\widetilde{M}, \operatorname{tr}(\widetilde{\omega}_{\widetilde{L}})] + [\operatorname{tr}(B_{\widetilde{N},\widetilde{M}})] + [\operatorname{tr}(B_{\widetilde{M},\widetilde{L}})] + [-\operatorname{tr}(B_{\widetilde{N},\widetilde{L}})].$$

As an element in W we have that $rk\,(X) = 4n$, in particular, $4|rk\,(X)$. Moreover

Proposition 5.3. *The discriminant* $d\,(X) = 1$.

For a proof, see Appendix.

The theorem now follows from

Proposition 5.4. *Let* $X \in \mathrm{W}$ *such that* $4|rk\,(X)$ *and* $d\,(X) = 1$ *then* $2X = \mathbf{0}$ *in* GW.

For a proof, see Appendix.

This concludes the proof of the theorem.

Acknowledgments

We would like to thank our teacher J. Bernstein for his interest and guidance. It is a pleasure to thank D. Kazhdan for sharing with us his thoughts about the nature of canonical Hilbert spaces. We are also thankful to P. Etingof for telling us about the peculiarities of the Weil representation in even characteristic [3], a remark which initiated this direction of research. We thank M. Nori for explaining to us several useful ideas from algebraic number theory. We thank T. Schedler for many stimulating discussions about Heisenberg groups, Weil representations and commutative rings with even number of elements. Finally, we are grateful to the anonymous referees who raised many important corrections and improvements to the original manuscript.

Appendix. Proof of statements

A.1. Proof of Lemma 1.2

First we show that the map $\widetilde{\alpha}$ factors to a function $\alpha_{\widetilde{g}} : V \to R$. Let $\widetilde{v}, \widetilde{x} \in \widetilde{V}$. Write

$$\begin{aligned}\alpha_{\widetilde{g}}(\widetilde{v}+2\widetilde{x}) &= \alpha_{\widetilde{g}}(\widetilde{v}) + \beta(\widetilde{g}(\widetilde{x}), \widetilde{g}(\widetilde{v})) + \beta(\widetilde{g}(\widetilde{v}), \widetilde{g}(\widetilde{x})) - \beta(\widetilde{x}, \widetilde{v}) - \beta(\widetilde{v}, \widetilde{x}) \\ &= \alpha_{\widetilde{g}}(\widetilde{v}) + \omega(\widetilde{g}(\widetilde{v}), \widetilde{g}(\widetilde{x})) - \omega(\widetilde{v}, \widetilde{x}) = \alpha_{\widetilde{g}}(\widetilde{v})\end{aligned}$$

where in the second equality we added $\beta(\widetilde{g}(\widetilde{x}), \widetilde{g}(\widetilde{v})) - \beta(\widetilde{g}(\widetilde{x}), \widetilde{g}(\widetilde{v}))$ and also $\beta(\widetilde{x}, \widetilde{v}) - \beta(\widetilde{x}, \widetilde{v})$ and used the fact that $2\beta = 0$.

We are left to show that $\alpha_{\widetilde{g}} \in \Sigma_g$. Write

$$\begin{aligned}\alpha_{\widetilde{g}}(v_1+v_2) &= \widetilde{\beta}(\widetilde{g}(\widetilde{v}_1+\widetilde{v}_2), \widetilde{g}(\widetilde{v}_1+\widetilde{v}_2)) - \widetilde{\beta}(\widetilde{v}_1+\widetilde{v}_2, \widetilde{v}_1+\widetilde{v}_2) \\ &= \alpha_{\widetilde{g}}(v_1) + \alpha_{\widetilde{g}}(v_2) + \widetilde{\beta}(\widetilde{g}(\widetilde{v}_1), \widetilde{g}(\widetilde{v}_2)) + \widetilde{\beta}(\widetilde{g}(\widetilde{v}_2), \widetilde{g}(\widetilde{v}_1)) \\ &\quad - \widetilde{\beta}(\widetilde{v}_1, \widetilde{v}_2) - \widetilde{\beta}(\widetilde{v}_2, \widetilde{v}_1) \\ &= \alpha_{\widetilde{g}}(v_1) + \alpha_{\widetilde{g}}(v_2) + \beta(g(v_1), g(v_2)) + \widetilde{\omega}(\widetilde{g}(\widetilde{v}_2), \widetilde{g}(\widetilde{v}_1)) \\ &\quad - \beta(v_1, v_2) - \widetilde{\omega}(\widetilde{v}_2, \widetilde{v}_1) \\ &= \alpha_{\widetilde{g}}(v_1) + \alpha_{\widetilde{g}}(v_2) + \beta(g(v_1), g(v_2)) - \beta(v_1, v_2),\end{aligned}$$

where, in the third equality we added $\widetilde{\beta}(\widetilde{g}(\widetilde{v}_1), \widetilde{g}(\widetilde{v}_2)) - \widetilde{\beta}(\widetilde{g}(\widetilde{v}_1), \widetilde{g}(\widetilde{v}_2))$ and also $\widetilde{\beta}(\widetilde{v}_1, \widetilde{v}_2) - \widetilde{\beta}(\widetilde{v}_1, \widetilde{v}_2)$ and used that

$$\begin{aligned}&\widetilde{\beta}(\widetilde{g}(\widetilde{v}_2), \widetilde{g}(\widetilde{v}_1)) - \widetilde{\beta}(\widetilde{g}(\widetilde{v}_1), \widetilde{g}(\widetilde{v}_2)) = \widetilde{\omega}(\widetilde{g}(\widetilde{v}_2), \widetilde{g}(\widetilde{v}_1)), \\ &\widetilde{\beta}(\widetilde{v}_2, \widetilde{v}_1) - \widetilde{\beta}(\widetilde{v}_1, \widetilde{v}_2) = \widetilde{\omega}(\widetilde{v}_2, \widetilde{v}_1).\end{aligned}$$

This concludes the proof of the lemma.

A.2. Proof of Lemma 2.2

First we show that $\widetilde{\beta}$ factors to a function $\alpha_{\widetilde{L}} : L \to R$. Let $\widetilde{l}, \widetilde{x} \in \widetilde{L}$. Write

$$\begin{aligned}\widetilde{\beta}(\widetilde{l}+2\widetilde{x}, \widetilde{l}+2\widetilde{x}) &= \widetilde{\beta}(\widetilde{l}, \widetilde{l}) + 2\widetilde{\beta}(\widetilde{x}, \widetilde{l}) + 2\widetilde{\beta}(\widetilde{l}, \widetilde{x}) \\ &= \widetilde{\beta}(\widetilde{l}, \widetilde{l}) + 4\widetilde{\beta}(\widetilde{x}, \widetilde{l}),\end{aligned}$$

where, in the second equality we used the fact that $\widetilde{\beta} : \widetilde{L} \times \widetilde{L} \to R$ is symmetric, since $\widetilde{L}$ is a Lagrangian sub-module.

We are left to show that $\alpha_{\widetilde{L}} \in \Sigma_L$. Write

$$\begin{aligned}\alpha_{\widetilde{L}}(l_1+l_2) - \alpha_{\widetilde{L}}(l_1) - \alpha_{\widetilde{L}}(l_2) &= \widetilde{\beta}(\widetilde{l}_1+\widetilde{l}_2, \widetilde{l}_1+\widetilde{l}_2) - \widetilde{\beta}(\widetilde{l}_1, \widetilde{l}_1) - \widetilde{\beta}(\widetilde{l}_2, \widetilde{l}_2) \\ &= \widetilde{\beta}(\widetilde{l}_1, \widetilde{l}_2) + \widetilde{\beta}(\widetilde{l}_2, \widetilde{l}_1) = 2\widetilde{\beta}(\widetilde{l}_1, \widetilde{l}_2) \\ &= \beta(l_1, l_2),\end{aligned}$$

where in the third equality we, again, used the fact that $\widetilde{\beta} : \widetilde{L} \times \widetilde{L} \to R$ is symmetric. This concludes the proof of the lemma.

A.3. *Proof of* Proposition 2.7

First we show that $\mathcal{W}$ is a groupoid. Let $f : \mathfrak{E}_1 \to \mathfrak{E}_2$, where $\mathfrak{E}_1, \mathfrak{E}_2 \in \mathcal{W}$. Since $\varphi_2^{\otimes 4} \circ f^{\otimes 4} = \varphi_1^{\otimes 4}$ and $\varphi_2^{\otimes 4}, \varphi_1^{\otimes 4}$ are isomorphisms, this implies that $f^{\otimes 4}$ is an isomorphism, which, in turns, implies that f is an isomorphism.

Second, we show that every two objects in $\mathcal{W}$ are isomorphic. Let $\mathfrak{E}_1, \mathfrak{E}_2 \in \mathcal{W}$, in order to specify an isomorphism between $\mathfrak{E}_1$ and $\mathfrak{E}_2$ as trivialized vector bundles, it is enough to specify an isomorphism of a single fiber. Let $L \in ELag(V)$, and choose $f_L \in \mathfrak{E}_{1,L} \to \mathfrak{E}_{2,L}$ to be a non-zero isomorphism which satisfies $\varphi_{2,L}^{\otimes 4} \circ f_L^{\otimes 4} = \varphi_{1,L}^{\otimes 4}$ (this can be always done). This implies that the isomorphism $f : \mathfrak{E}_1 \to \mathfrak{E}_2$ which is determined by f_L satisfies $\varphi_2^{\otimes 4} \circ f^{\otimes 4} = \varphi_1^{\otimes 4}$ which means that $f \in \mathrm{Mor}_{\mathcal{W}}(\mathfrak{E}_1, \mathfrak{E}_2)$.

Finally, we show that, $\mathrm{Mor}(\mathfrak{E}, \mathfrak{E}) \simeq \mu_4(\mathbb{C})$, for every $\mathfrak{E} \in \mathcal{W}$. Let $\mathfrak{E} \in \mathcal{W}$. It is easy to see that any two morphisms $f_1, f_2 \in \mathrm{Mor}(\mathfrak{E}, \mathfrak{E})$ are proportional, namely $f_2 = \lambda \cdot f_1$, for some $\lambda \in \mathbb{C}^\times$. Now since both satisfies the condition $\varphi^{\otimes 4} \circ f_i^{\otimes 4} = \varphi^{\otimes 4}$, this implies that $\lambda^4 = 1$.

This concludes the proof of the proposition.

A.4. *Proof of* Proposition 2.8

First we show that $AMp(V)$ fits into an exact sequence

$$1 \to \mu_4(\mathbb{C}) \to AMp(V) \xrightarrow{p} ASp(V) \to 1$$

where the morphism $p : AMp(V) \to ASp(V)$ is the canonical projection. The kernel of p consists of pairs of the form $(1, \iota)$, where $\iota : Id \xrightarrow{\simeq} Id$. An isomorphism $\iota : Id \xrightarrow{\simeq} Id$ is determined by $\iota_{\mathfrak{E}} : \mathfrak{E} \xrightarrow{\simeq} \mathfrak{E}$, for any $\mathfrak{E} \in \mathcal{W}$, but by Proposition 2.7 we know that $\mathrm{Mor}(\mathfrak{E}, \mathfrak{E}) \simeq \mu_4(\mathbb{C})$.

Second we show that $p : AMp(V) \to ASp(V)$ is a central extension. We have to show that

$$(g, \iota_g)^{-1} \cdot (1, \iota) \cdot (g, \iota_g) = (1, \iota),$$

for every $(g, \iota_g) \in AMp(V)$. Explicit calculation reveals that

$$(g, \iota_g)^{-1} = \left(g^{-1}, \left(g^{-1}\right)^* \left(\iota_g^{-1}\right)\right),$$

which implies that

$$(g, \iota_g)^{-1} \cdot (1, \iota) \cdot (g, \iota_g) = \left(1, \iota_g \circ \iota \circ \iota_g^{-1}\right).$$

Now, verify that $\iota_g \circ \iota \circ \iota_g^{-1} = \iota$. This concludes the proof of the proposition.

A.5. *Proof of* Proposition 3.1

Let $\delta \in \mathcal{H}_L$ be the unique function on $H(V)$, supported on $Z \cdot L \subset H(V)$ and normalized such that $\delta(0) = 1$.

On the one hand, explicit computation reveals that $F_{N,L}[\delta](0) = 1$. This implies that

$$C(N, M, L) = F_{N,M} \circ F_{M,L}[\delta](0). \tag{A.1}$$

On the other hand

$$F_{N,M} \circ F_{M,L}[\delta](0) = \sum_{m \in M} \sum_{n \in N} \delta(\tau_M(m) \cdot \tau_N(n)),$$

where $\tau_M : M \to H(V)$ and $\tau_N : N \to H(V)$ are the associated injective homomorphisms. The multiplication rule in $H(V)$ implies that for every $m \in M$ and $n \in N$ we have that

$$\tau_M(m) \cdot \tau_N(n) = (m+n, \alpha_M(m) + \alpha_N(n) + \beta(m,n)).$$

Since $\delta(\tau_M(m) \cdot \tau_N(n)) = 0$ unless $m + n \in L$ we obtain that for every $m \in M$, the only non-zero contribution to the sum $\sum_{n \in N} \delta(\tau_M(m) \cdot \tau_N(n))$ comes from $n = -r^L(m)$.

Therefore, we obtain that

$$\begin{aligned} F_{N,M} \circ F_{M,L}[\delta](0) &= \sum_{m \in M} \delta\left(\tau_M(m) \cdot \tau_N\left(-r^L(m)\right)\right) \\ &= \sum_{m \in M} \delta\left(m - r^L(m), \alpha_L\left(m - r^L(m)\right) + Q_{(N,M,L)}(m)\right) \\ &= \sum_{m \in M} \psi\left(Q_{(N,M,L)}(m)\right). \end{aligned}$$

Combining with (A.1) we get

$$C(N, M, L) = \sum_{m \in M} \psi\left(Q_{(N,M,L)}(m)\right).$$

This concludes the proof of the proposition.

A.6. *Proof of Theorem 3.3*

We will use the following technical result:

Lemma A.1. *Let $(N, L) \in ELag(V)^2$, then there exists $M \in ELag(V)$ such that (N, M), $(M, L) \in U_2$.*

We prove the lemma below.

The trivialization of the vector bundle $\mathfrak{H}^{\otimes 4}$ is constructed as follows: Let $(N, L) \in ELag(V)^2$, choose a third $M \in ELag(V)$ such that $(N, M), (M, L) \in U_2$. Define

$$T_{N,L} = T_{N,M} \circ T_{M,L}.$$

Noting that both operators in the left hand side are defined. We are left to show that the operator $T_{N,L}$ does not depends on the choice of M.

Let $M_i \in ELag(V), i = 1, 2$, such that $(N, M_i), (M_i, L) \in U_2$. We want to show that $T_{N,M_1} \circ T_{M_1,L} = T_{N,M_2} \circ T_{M_2,L}$.

Choose $M_3 \in ELag(V)$ such that $(M_3, M_i) \in U_2$ and $(M_3, L), (M_3, N) \in U_2$. We have

$$\begin{aligned} T_{N,M_1} \circ T_{M_1,L} &= T_{N,M_1} \circ T_{M_1,M_3} \circ T_{M_3,L} \\ &= T_{N,M_3} \circ T_{M_3,L}, \end{aligned}$$

where the first and second equalities are the multiplicativity property for triples which are in general position pairwisely (Formula (3.2)). In the same fashion, we show that $T_{N,M_1} \circ T_{M_1,L} = T_{N,M_3} \circ T_{M_3,L}$.

The fact the full system $\left\{T_{M,L} : (M, L) \in ELag(V)^2\right\}$ is a trivialization can be easily proved along the same lines as above. This concludes the proof of the theorem.

A.6.1. Proof of Lemma A.1

Let $A = L \cap N$, and write $L = A \oplus B$, $N = A \oplus C$. Then the assumptions imply that ω induces a perfect pairing between B and C, and the direct sum $B \oplus C$ is symplectic, hence so is its orthogonal complement $W = (B \oplus C)^{\perp}$, which is seen to have dimension $2\dim(A)$, so A is Lagrangian in W. So we can find a symplectic basis (e's and f's) of W such that A is spanned by the e's, and let D be the space spanned by the f's. Let v_i, $i = 1, \ldots, r$ be a basis of B and v_i^* the dual basis of C. Take $M = D \oplus \operatorname{span}\{v_i + v_i^*; i = 1, \ldots, r\}$.

This concludes the proof of the lemma.

A.7. Proof of Proposition 3.5

The proof is by induction on the rank of V.

If $rk\,(V) = 1$ then, since B is non-degenerate, either $[V, B] = [1]$ or $[V, B] = [-1]$ (1 and -1 are the invertible elements in $\mathbb{Z}/4\mathbb{Z}$) and we are done.

Assume $rk\,(V) > 1$.

A.7.1. Case 1

We are in the situation where there exists $v \in V$ such that $B\,(v, v) = \pm 1$, then the module V decomposes into a direct sum

$$V = \mathbb{Z}/4\mathbb{Z} \cdot v \oplus (\mathbb{Z}/4\mathbb{Z} \cdot v)^{\perp},$$

therefore $[V, B] = [\pm 1] + [V_1, B_1]$, with $rk\,(V_1) < rk\,(V)$ and the statement follows by induction.

A.7.2. Case 2

We are in the situation where $B\,(v, v) \in 2 \cdot \mathbb{Z}/4\mathbb{Z}$, for every $v \in V$. Always there exists a pair $e, f \in V$ such that $B\,(e, f) = 1$. Let us denote by U the sub-module $\mathbb{Z}/4\mathbb{Z} \cdot e + \mathbb{Z}/4\mathbb{Z} \cdot f$. First we show that V decomposes into a direct sum

$$V = U \oplus V_1.$$

We verify the last assertion in three different cases.

Case 1. Assume $B\,(e, e) = B\,(f, f) = 0$. Let $P : V \to V$ be the operator defined by

$$P\,(v) = v - \langle v, e\rangle \cdot f - \langle v, f\rangle \cdot e.$$

Direct verification reveals that P is an idempotent and $P\,(U) = 0$, hence $V = U \oplus PV$.

Case 2. Assume $B\,(e, e) = B\,(f, f) = 2$. Let $P : V \to V$ be the operator defined by

$$P\,(v) = v - \langle v, e\rangle \cdot f - \langle v, f\rangle \cdot e + 2\,\langle v, e\rangle \cdot e + 2\,\langle v, f\rangle \cdot f.$$

Direct verification reveals that P is an idempotent and $P\,(U) = 0$, hence $V = U \oplus PV$.

Case 3. Without loss of generality, assume $B\,(e, e) = 2$ and $B\,(f, f) = 0$. Let $P : V \to V$ be the operator defined by

$$P\,(v) = v - \langle v, e\rangle \cdot f - \langle v, f\rangle \cdot e + 2\,\langle v, f\rangle \cdot f.$$

Direct verification reveals that P is an idempotent and $P\,(U) = 0$, hence $V = U \oplus PV$.

Now, in case 1

$$\left[U, B_{|U}\right] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

in case 2

$$\left[U, B_{|U}\right] = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix},$$

and in case 3

$$\left[U, B_{|U}\right] = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}.$$

Finally, considering case 3, we claim that

$$\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

via the isomorphism sending $e \mapsto e + f$ and $f \mapsto f$.

This concludes the proof of the proposition.

A.8. *Proof of Proposition 3.6*

First we show that

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Denote

$$M = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \qquad N = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Let $V_i = (\mathbb{Z}/4\mathbb{Z} \cdot e_i \oplus \mathbb{Z}/4\mathbb{Z} \cdot f_i, B_M)$, $i = 1, 2$ be two copies of the inner product space associated to the matrix M.

Let $\phi : V_1 \oplus V_2 \to V_1 \oplus V_2$ be the isomorphism given by

$$\phi(e_1) = -e_1 - f_1 - 2e_2 - f_2,$$
$$\phi(f_1) = 2e_1 + f_1 + 2e_2 - f_2,$$
$$\phi(e_2) = e_1 + e_2,$$
$$\phi(f_2) = -e_1 - e_2 + f_2.$$

Direct verification reveals that $\phi^*(B_M \oplus B_M) = B_N \oplus B_N$, which is what we wanted to show.

Second, we show that

$$3 \cdot [1] = [-1] + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Let $V_i = \left(\mathbb{Z}/4\mathbb{Z} \cdot e_i, B_{[1]}\right)$, $i = 1, 2, 3$ be three copies of the inner product space associated to the matrix (1). Let $\phi : V_1 \oplus V_2 \oplus V_3 \to V_1 \oplus V_2 \oplus V_3$ be the isomorphism given by

$$\phi(e_1) = e_1 + e_2 + e_3,$$
$$\phi(e_2) = e_1 + 2e_2 + e_3,$$
$$\phi(e_3) = e_1 + e_2 + 2e_3.$$

Direct verification reveals that $\phi^*\left(B_{[1]} \oplus B_{[1]} \oplus B_{[1]}\right) = B_{[-1]} \oplus B_M$, which is what we wanted to show.

In the same fashion one shows that

$$3 \cdot [-1] = [1] + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

This concludes the proof of the proposition.

A.9. *Proof of Proposition 3.9*

Let $[V, B] \in \mathrm{GW}$. Using Proposition 3.5, we can write

$$[V, B] = n_1 \cdot [1] + n_2 \cdot [-1] + n_3 \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + n_4 \cdot \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Therefore

$$\begin{aligned} 4 \cdot [V, B] &= 4n_1 \cdot [1] + 4n_2 \cdot [-1] + 4n_3 \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} + 4n_4 \cdot \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \\ &= n_1 \cdot \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} + n_2 \cdot \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} + 4n_3 \cdot \mathbf{0} + 2n_4 \cdot \mathbf{0} \\ &= (n_1 + n_2) \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} = rk\,(V) \cdot \mathbf{4}. \end{aligned}$$

We have to explain the second and the fourth equalities.

The second equality. In the second equality we used the following. First, in GW

$$\begin{aligned} &\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \mathbf{0}, \\ &\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} = \mathbf{0}, \end{aligned}$$

where in the second equality we used Proposition 3.6, relation (3.5). Second, in W

$$\begin{aligned} 4 \cdot [1] &= [1] + 3 \cdot [1] = [1] + [-1] + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \\ 4 \cdot [-1] &= [-1] + 3 \cdot [-1] = [-1] + [1] + \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \end{aligned}$$

where, here, we used Proposition 3.6, relations (3.6) and (3.7) respectively. Hence in GW

$$\begin{aligned} 4 \cdot [1] &= \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}, \\ 4 \cdot [-1] &= \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}. \end{aligned}$$

The fourth equality. First, we note that the unique element in GW of order 2, which we denoted by **4** can be represented

$$\mathbf{4} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Second, since $rk\,(V) = n_1 + n_2 + 2n_3 + 2n_4$ we have that $rk\,(V) = n_1 + n_2 (\mathrm{mod}\ 2)$.

This concludes the proof of the proposition.

A.10. Proof of Theorem 3.7

Since $G : \mathrm{W} \to \mathbb{C}^{\times}$ is a morphism of monoids, it is enough to prove the assertion for the generators $[1]$, $[-1]$, $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$, that is, we need to show

$$|G([1])| = \sqrt{2},$$
$$|G([-1])| = \sqrt{2},$$
$$\left| G\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right) \right| = 2,$$
$$\left| G\left(\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \right) \right| = 2.$$

We calculate

$$G([1]) = \sum_{x \in \mathbb{F}_2} e^{\frac{2\pi i}{4} x^2} = 1 + i = e^{\frac{2\pi i}{8}} \sqrt{2},$$

therefore, we get that $|G([1])| = \sqrt{2}$. Since $G([-1]) = \overline{G([1])}$, the assertion follows for $G([-1])$ as well.

Now, we calculate

$$G\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right) = \sum_{x,y \in \mathbb{F}_2} e^{\frac{2\pi i}{2} xy} = 2.$$

Using the above equality and Proposition 3.5, we can write

$$G\left(\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \right)^2 = G\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right)^2 = 4,$$

which implies that $\left| G\left(\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \right) \right| = 2$.

This concludes the proof of the theorem.

A.11. Proof of Theorem 3.8

Denote

$$A = [1] + [-1],$$
$$B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

First, we show that $A, B \in I$. For this it is enough to show that $G(A) = 2$ and $G(B) = 2$. The first equality is clear since $G([-1]) = \overline{G([1])}$. The second equality is obtained by direct calculation

$$G(B) = \sum_{x,y \in \mathbb{F}_2} e^{\frac{2\pi i}{2} xy} = 2.$$

Let us denote by $I' \subset \mathrm{W}$ the submonoid generated by A, B.

Second, we show that W/I' is a group, isomorphic to $\mathbb{Z}/8\mathbb{Z}$. First, note that Propositions 3.5 and 3.6 imply that the element $[1]$ generates the group W/I' and, in addition, $8 \cdot [1] = \mathbf{0}$ in W/I'.

This implies that the morphism of monoids $\mathbb{Z}/8\mathbb{Z} \to \mathrm{GW}$, sending 1 to [1] is a surjection, which in particular implies that W/I' is a group—a quotient group of $\mathbb{Z}/8\mathbb{Z}$.

In order to show that W/I' is isomorphic to $\mathbb{Z}/8\mathbb{Z}$ it will be enough to show that $G([1]) = \mu\sqrt{2}$, where μ is a primitive element in $\mu_8(\mathbb{C})$. We calculate

$$G([1]) = \sum_{x \in \mathbb{F}_2} e^{\frac{2\pi i}{4} x^2} = 1 + i = e^{\frac{2\pi i}{8}} \sqrt{2}. \tag{A.2}$$

Finally, we show that the canonical morphism $\mathrm{W}/I' \to \mathrm{GW} = \mathrm{W}/I$ is an isomorphism. This follows from the fact that $G : \mathrm{W}/I' \to \mathbb{C}^{\times}/2^{\mathbb{Z}}$ is an injection, which, in turns, follows from A.2.

This concludes the proof of the theorem.

A.12. Proof of Proposition 4.3

We need to show that the category $\mathcal{W}^s$ is a gerbe with band $\mu_2(\mathbb{C})$.

Clearly $\mathcal{W}^s$ is a groupoid. We need to show that every two objects in $\mathcal{W}^s$ are isomorphic.

Consider two objects $\mathfrak{E}_1^s, \mathfrak{E}_2^s \in \mathcal{W}^s$, that is

$$\mathfrak{E}_1^s = (\widetilde{\mathfrak{E}}_1, \mathfrak{E}_1, \alpha_1),$$
$$\mathfrak{E}_2^s = (\widetilde{\mathfrak{E}}_2, \mathfrak{E}_2, \alpha_2),$$

where $\widetilde{\mathfrak{E}}_i \in \widetilde{\mathcal{W}}^s$, $\mathfrak{E}_i \in \mathcal{W}$ and $\alpha_i \in \mathrm{Mor}_{\widetilde{\mathcal{W}}}(\widetilde{S}(\widetilde{\mathfrak{E}}_i), \pi^*(\mathfrak{E}_i))$, for $i = 1, 2$.

Since $\widetilde{\mathcal{W}}^s$ is a gerbe, there exists an morphism $\widetilde{f} \in \mathrm{Mor}_{\widetilde{\mathcal{W}}^s}(\widetilde{\mathfrak{E}}_1, \widetilde{\mathfrak{E}}_2)$. Since π^* is full, there exists a morphism $f \in \mathrm{Mor}_{\mathcal{W}}(\mathfrak{E}_1, \mathfrak{E}_2)$ such that $\pi^*(f) = \alpha_2 \circ \widetilde{S}(\widetilde{f}) \circ \alpha_1^{-1}$. The pair $(\widetilde{f}, f)$ is a morphism in $\mathrm{Mor}_{\mathcal{W}^s}(\mathfrak{E}_1^s, \mathfrak{E}_2^s)$.

We are left to show that $\mathrm{Mor}_{\mathcal{W}^s}(\mathfrak{E}^s, \mathfrak{E}^s) \simeq \mu_2(\mathbb{C})$, for every $\mathfrak{E}^s \in \mathcal{W}^s$. Write $\mathfrak{E}^s = (\widetilde{\mathfrak{E}}, \mathfrak{E}, \alpha)$. A morphism $(\widetilde{f}, f) \in \mathrm{Mor}_{\mathcal{W}^s}(\mathfrak{E}^s, \mathfrak{E}^s)$ satisfies $\pi^*(f) = \alpha \circ \widetilde{S}(\widetilde{f}) \circ \alpha^{-1}$, therefore, $\pi^*(f)$ is determined by $\widetilde{S}(\widetilde{f})$. Since $\widetilde{S}$ is faithful, $\pi^*(f)$ is, in fact, determined by $\widetilde{f}$. Finally, since π^* is faithful, we obtain that f is determined by $\widetilde{f}$. Therefore, we get that

$$\mathrm{Mor}_{\mathcal{W}^s}(\mathfrak{E}^s, \mathfrak{E}^s) \simeq \mathrm{Mor}_{\widetilde{\mathcal{W}}^s}(\widetilde{\mathfrak{E}}, \widetilde{\mathfrak{E}}) \simeq \mu_2(\mathbb{C}).$$

This concludes the proof of the proposition.

A.13. Proof of Proposition 5.3

Let us first consider the element $X' \in \mathrm{W}(R)$

$$X' = [\widetilde{M}, \widetilde{\omega}_{\widetilde{L}}] + [B_{\widetilde{N},\widetilde{M}}] + [B_{\widetilde{M},\widetilde{L}}] + [-B_{\widetilde{N},\widetilde{L}}],$$

where we use the abbreviated notation $[B]$ for $\left[R^n, B\right]$.

Lemma A.2. *The discriminant $d\left(X'\right) = 1$.*

The proposition now follows from

Lemma A.3. *Let $[V, B] \in \mathrm{W}(R)$ be such that $d([V, B]) = 1$ then $d([V, \mathrm{tr}(B)]) = 1$.*

This concludes the proof of the proposition.

A.13.1. Proof of Lemma A.2

Write

$$d\left(X'\right) = d([\widetilde{M}, \widetilde{\omega}_{\widetilde{L}}]) \cdot d([B_{\widetilde{N},\widetilde{M}}]) \cdot d([B_{\widetilde{M},\widetilde{L}}]) \cdot d([-B_{\widetilde{N},\widetilde{L}}])$$
$$= (-1)^n\, d([\widetilde{M}, \widetilde{\omega}_{\widetilde{L}}]) \cdot \widetilde{\omega}_\wedge(o_{\widetilde{M}}, o_{\widetilde{N}}) \cdot \widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{M}}) \cdot \widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{N}}), \tag{A.3}$$

where, by construction, $d([B_{\widetilde{M},\widetilde{L}}]) = \widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{M}})$ for every $(\widetilde{M}, \widetilde{L}) \in \widetilde{U}_2$. We proceed to compute $d([\widetilde{M}, \widetilde{\omega}_{\widetilde{L}}])$.

First, we note

$$d([\widetilde{M}, \widetilde{\omega}_{\widetilde{L}}]) = \widetilde{\omega}_\wedge(r_\wedge^{\widetilde{L}}(o_{\widetilde{M}}), o_{\widetilde{M}}),$$

where $r_\wedge^{\widetilde{L}} : \wedge^n \widetilde{M} \to \wedge^n \widetilde{N}$ is the map induced from $r^{\widetilde{L}} : \widetilde{M} \to \widetilde{N}$.

Lemma A.4. *We have*

$$\widetilde{\omega}_\wedge(r_\wedge^{\widetilde{L}}(o_{\widetilde{M}}), o_{\widetilde{M}}) = (-1)^n \frac{\widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{M}}) \cdot \widetilde{\omega}_\wedge(o_{\widetilde{M}}, o_{\widetilde{N}})}{\widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{N}})}. \tag{A.4}$$

Substituting (A.4) in (A.3) we get

$$d\left(X'\right) = \widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{M}})^2 \cdot \widetilde{\omega}_\wedge(o_{\widetilde{M}}, o_{\widetilde{N}})^2.$$

This concludes the proof of the lemma.

Proof of Lemma A.4. We know that $r_\wedge^{\widetilde{L}}(o_{\widetilde{M}}) \in \wedge^n \widetilde{N}$ is proportional to $o_{\widetilde{N}}$ since $\wedge^n \widetilde{N} = R \cdot o_{\widetilde{N}}$, so we can write $r_\wedge^{\widetilde{L}}(o_{\widetilde{M}}) = a \cdot o_{\widetilde{N}}$, for some $a \in R^\times$.

On the one hand, since $r^{\widetilde{L}}(\widetilde{m}) - \widetilde{m} \in \widetilde{L}$, we have

$$\widetilde{\omega}_\wedge(r_\wedge^{\widetilde{L}}(o_{\widetilde{M}}), o_{\widetilde{L}}) = \widetilde{\omega}_\wedge(o_{\widetilde{M}}, o_{\widetilde{L}}).$$

On the other hand, since $r_\wedge^{\widetilde{L}}(o_{\widetilde{M}}) = a \cdot o_{\widetilde{N}}$, we have

$$\widetilde{\omega}_\wedge(r_\wedge^{\widetilde{L}}(o_{\widetilde{M}}), o_{\widetilde{L}}) = a \cdot \widetilde{\omega}_\wedge(o_{\widetilde{N}}, o_{\widetilde{L}}).$$

Combining the above two equations we get

$$a = \frac{\widetilde{\omega}_\wedge(o_{\widetilde{M}}, o_{\widetilde{L}})}{\widetilde{\omega}_\wedge(o_{\widetilde{N}}, o_{\widetilde{L}})} = \frac{\widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{M}})}{\widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{N}})}.$$

Finally, write

$$\widetilde{\omega}_\wedge(r_\wedge^{\widetilde{L}}(o_{\widetilde{M}}), o_{\widetilde{M}}) = a \cdot \widetilde{\omega}_\wedge(o_{\widetilde{N}}, o_{\widetilde{M}})$$
$$= \frac{\widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{M}})}{\widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{N}})} \cdot \widetilde{\omega}_\wedge(o_{\widetilde{N}}, o_{\widetilde{M}})$$
$$= (-1)^n \frac{\widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{M}}) \cdot \widetilde{\omega}_\wedge(o_{\widetilde{M}}, o_{\widetilde{N}})}{\widetilde{\omega}_\wedge(o_{\widetilde{L}}, o_{\widetilde{N}})}.$$

This concludes the proof of the lemma.

A.13.2. Proof of Lemma A.3

It is easy to verify that the discriminants $d([V, \mathrm{tr}(B)])$ and $d([V, B])$ are related as follows

$$d([V, \mathrm{tr}(B)]) = N(d([V, B])) \cdot d([R, \mathrm{tr}])^{rk_R(V)}$$

where $N : R^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ is the norm map. Since we assume that $d([V, B])$ is a square in $R^\times$ this implies that $N(d([V, B]))$ is a square in $(\mathbb{Z}/4\mathbb{Z})^\times$ therefore it is enough to prove that

$$d([R, \mathrm{tr}]) = 1,$$

where $\mathrm{tr} : R \times R \to \mathbb{Z}/4\mathbb{Z}$ denote the trace form $\mathrm{tr}(x, y) = \mathrm{tr}(x \cdot y)$.

We prove a more general assertion. Let K/F be an unramified extension of local fields lying over $\mathbb{Q}_2$. Denote $R_K = \mathcal{O}_K/\mathfrak{m}_K^2$ and $R_F = \mathcal{O}_F/\mathfrak{m}_F^2$. We claim that

$$d\left(\left[R_K, \mathrm{tr}_{K/F}\right]\right) = 1$$

where $\mathrm{tr}_{K/F} : R_K \times R_K \to R_F$ denote the relative trace map. First, we prove the above in two particular cases. The first case is when $[K : F]$ is odd; the second case is when $[K : F] = 2^l$, for some $l \in \mathbb{N}$.

Case 1. Assume $d = [K : F]$ is odd. In this case we claim that already $d\left(\left[\mathcal{O}_K, \mathrm{tr}_{K/F}\right]\right) = 1$ in $\mathcal{O}_F^\times/\mathcal{O}_F^{\times 2}$.

We can present K in the form $K = F(\alpha)$ such that $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ is a basis of $\mathcal{O}_K$ over $\mathcal{O}_F$. Explicit computation reveals that

$$\begin{aligned} d\left(\left[\mathcal{O}_K, \mathrm{tr}_{K/F}\right]\right) &= \Delta\left(1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\right) \\ &= \prod_{0 \le i < j \le d-1} \left(\mathrm{Fr}^j \alpha - \mathrm{Fr}^i \alpha\right)^2, \end{aligned} \tag{A.5}$$

where $\mathrm{Fr} \in G = \mathrm{Gal}(K/F)$ is the Frobenius automorphism. Denote

$$D = \prod_{0 \le i < j \le d-1} \left(\mathrm{Fr}^j \alpha - \mathrm{Fr}^i \alpha\right).$$

We claim that $D \in \mathcal{O}_F^\times$. Clearly, $D \in \mathcal{O}_K^\times$. In addition, for every $g \in G$, we have that $gD = \sigma(g) D$, where $\sigma : \Sigma_d \to \{\pm 1\}$ is the sign homomorphism of the permutation group and we use the injection $G \hookrightarrow \Sigma_d$. Since K/F is an unramified extension this implies that G is cyclic and since by assumption $|G|$ is odd, it must be that $\sigma_{|G} = 1$. Hence, D is invariant under the action of G therefore $D \in \mathcal{O}_F^\times$.

Combining this with (A.5) we get that $d\left(\left[\mathcal{O}_K, \mathrm{tr}_{K/F}\right]\right) = 1$. This concludes the proof of the assertion in this case.

Case 2. Assume $d = [K : F] = 2^l$, for some $l \in \mathbb{N}$. Consider a series of intermediate extensions interpolating between K and F

$$K = K_l - K_{l-1} - \cdots - K_1 - K_0 = F,$$

where $\left[K_i : K_{i-1}\right] = 2$, for every $i = 1, \ldots, l$.

Denote $R_i = \mathcal{O}_{K_i}/\mathfrak{m}_{K_i}^2$, let $\mathrm{tr}_{i/i-1} : R_i \to R_{i-1}$ and $\mathrm{tr}_i : R_i \to R_0 = R_F$ denote the corresponding trace maps and finally, let $N_i : R_i^\times \to R_0^\times = R_F^\times$ denote the norm map.

It is easy to verify that the discriminants $d([R_i, \mathrm{tr}_i])$ and $d([R_{i-1}, \mathrm{tr}_{i-1}])$ are related as follows

$$d([R_i, \mathrm{tr}_i]) = N_{i-1}\left(d\left(\left[R_i, \mathrm{tr}_{i/i-1}\right]\right)\right) \cdot d\left(\left[R_{i-1}, \mathrm{tr}_{i-1}\right]\right).$$

It is enough to prove that $d\left(\left[R_i, \mathrm{tr}_{i/i-1}\right]\right) = 1$ in $R_{i-1}^{\times}/R_{i-1}^{\times 2}$.

We can assume that $K_i = K_{i-1}(\alpha)$ where $\alpha^2 + \alpha + a = 0$, for some $a \in \mathcal{O}_{K_{i-1}}$. Now, we have

$$d\left(\left[\mathcal{O}_{K_i}, \mathrm{tr}_{i/i-1}\right]\right) = \Delta(1, \alpha) = (\alpha_1 - \alpha_2)^2,$$

where α_1, α_2 are the two roots of the polynomial $x^2 + x + a$. Explicit computation reveals that $\Delta(1, \alpha) = 1 - 4a$ which implies that $d\left(\left[R_i, \mathrm{tr}_{i/i-1}\right]\right) = 1$.

This concludes the proof of the assertion in this case.

The statement for a general extension K/F now follows easily: Let E be an intermediate extension $K - E - F$ such that $[K : E]$ is odd and $[E : F] = 2^l$ and use

$$d\left(\left[R_K, \mathrm{tr}_{K/F}\right]\right) = N_{E/F}\left(d\left(\left[R_K, \mathrm{tr}_{K/E}\right]\right)\right) \cdot d\left(\left[R_F, \mathrm{tr}_{E/F}\right]\right).$$

This concludes the proof of the lemma.

A.14. *Proof of Proposition 5.4*

Write $X \in \mathrm{W}$ in the form

$$X = n_1[1] + n_2[-1] + n_3\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} + n_4\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}.$$

We have $rk(X) = n_1 + n_2 + 2n_3 + 2n_4$. On the one hand, since $4|rk(X)$ we have

$$n_1 + n_2 + 2n_3 + 2n_4 \equiv 0 \bmod 4. \tag{A.6}$$

On the other hand, $d(X) = (-1)^{n_1+n_2+n_3}$, where we use here the facts that

$$d\left(\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\right) = d\left(\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix}\right) = -1.$$

Therefore, since $d(X) = 1$ we have $n_2 + n_3 + n_4 \equiv 0 \bmod 2$, which implies that

$$2n_2 + 2n_3 + 2n_4 \equiv 0 \bmod 4. \tag{A.7}$$

Subtracting (A.7) from (A.6) we get that $n_1 \equiv n_2 \bmod 4$ which implies that

$$2n_1 \equiv 2n_2 \bmod 8. \tag{A.8}$$

Finally, in GW, we can write

$$\begin{aligned} 2X &= 2n_1[1] + 2n_2[-1] + 2n_3\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} + 2n_4\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix} \\ &= 2n_1[1] + 2n_2[-1] = \mathbf{0}, \end{aligned}$$

where the second equality follows from the facts that $2\begin{bmatrix}2 & 1\\ 1 & 2\end{bmatrix} = 2\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ in W (Theorem 3.8) and $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix} = \mathbf{0}$ in GW (Theorem 3.8) and the third equality follows from (A.8), the relation $[1] + [-1] = \mathbf{0}$ (Theorem 3.8) and the fact that for every $X \in \mathrm{GW}$, $8X = \mathbf{0}$ (Theorem 3.8).

This concludes the proof of the proposition.

References

[1] L. Blasco, Paires duales réductives en caractéristique 2, Mém. Soc. Math. Fr. Ser. 2e 52 (1993) 1–73.
[2] J.-L. Brylinski, Central extensions and reciprocity laws, Cah. Topol. Géom. Différ. Catég. 38 (3) (1997) 193–215.
[3] P. Etingof, S. Gelaki, Isocategorical groups, Int. Math. Res. Not. (2) (2001) 59–76.
[4] D. Mumford, Tata Lectures on Theta. III. With the Collaboration of Madhav Nori and Peter Norman, in: Progress in Mathematics, vol. 97, Birkhäuser Boston, Inc., Boston, MA, 1991.
[5] A. Weil, Sur certains groupes d'operateurs unitaires, Acta Math. 111 (1964) 143–211.