

Finite quotients of symplectic groups vs mapping class groups

Louis Funar*

Institut Fourier BP 74, UMR 5582
University of Grenoble I
38402 Saint-Martin-d'Hères cedex, France
e-mail: funar@fourier.ujf-grenoble.fr

Wolfgang Pitsch†

Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra (Cerdanyola del Vallès), Espana
e-mail: pitsch@mat.uab.es

May 31, 2013

Abstract

We show that the Schur multiplier of $Sp(2g, \mathbb{Z}/D\mathbb{Z})$ is $\mathbb{Z}/2\mathbb{Z}$, when D is divisible by 4. We give several proofs of this statement, a first one using Deligne's non-residual finiteness theorem and recent results of Putman, a second one using K-theory arguments based on the work of Barge and Lannes and a third one based on the Weil representations of symplectic groups arising in abelian Chern-Simons theory. We can also retrieve this way Deligne's non-residual finiteness of the universal central extension $\widetilde{Sp}(2g, \mathbb{Z})$ and a sharp result since $\widetilde{Sp}(2g, \mathbb{Z})$ surjects on the non-trivial central extension of $Sp(2g, \mathbb{Z}/D\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$, when $g \geq 3$. We prove then that the essential second homology of finite quotients of symplectic groups over a Dedekind domain of arithmetic type are torsion groups of uniformly bounded size. In contrast, quantum representations produce for every prime p , finite quotients of the mapping class group of genus $g \geq 3$ whose essential second homology has p -torsion. We further derive that all central extensions of the mapping class group are residually finite and deduce that mapping class groups have Serre's property A_2 for trivial modules, contrary to symplectic groups. Eventually we compute the module of coinvariants $H_2(\mathfrak{sp}_{2g}(2))_{Sp(2g, \mathbb{Z}/2^k\mathbb{Z})} = \mathbb{Z}/2\mathbb{Z}$.

2000 MSC Classification: 57 M 50, 55 N 25, 19 C 09, 20 F 38.

Keywords: Symplectic groups, group homology, mapping class group, central extension, quantum representation, residually finite.

1 Introduction and statements

Let $\Sigma_{g,k}$ denote a connected oriented surface of genus g with k boundary components and $M_{g,k}$ be its mapping class group, namely the group of isotopy classes of orientation preserving homeomorphisms that fix pointwise the boundary components. If $k = 0$, we simply write M_g for $M_{g,0}$. The action of M_g on the integral homology of Σ_g equipped with some symplectic basis gives a surjective homomorphism $M_g \rightarrow Sp(2g, \mathbb{Z})$, and it is a natural and classical problem to compare the properties of these two groups. The present paper is concerned with the central extensions and 2-homology groups of these two groups and their finite quotients.

Our first result is:

Theorem 1.1. *The second homology group of finite principal congruence quotients of $Sp(2g, \mathbb{Z})$, $g \geq 3$ is*

$$H_2(Sp(2g, \mathbb{Z}/D\mathbb{Z})) = \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } D \equiv 0 \pmod{4}, \\ 0, & \text{otherwise.} \end{cases}$$

This result when D is not divisible by 4 is an old theorem of Stein (see [65], Thm. 2.13 and Prop. 3.3.a) while the case $D \equiv 0 \pmod{4}$ remained open since then; this is explicitly mentioned in ([58], Remarks after Thm. 3.8), as the condition $D \not\equiv 0 \pmod{4}$ seemed essential for all results in there.

*Supported by the ANR 2011 BS 01 020 01 ModGroup.

†Supported by the FEDER/MEC grant MTM2010-20692.

The equality $H_2(SL(2, \mathbb{Z}/D\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}$, for $D \equiv 0 \pmod{4}$ was proved by Beyl (see [4]) and for large n Dennis and Stein proved using K-theoretic methods that $H_2(SL(n, \mathbb{Z}/D\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}$, for $D \equiv 0 \pmod{4}$, while $H_2(SL(n, \mathbb{Z}/D\mathbb{Z})) = 0$, otherwise (see [13], Cor. 10.2 and [52], section 12).

Our main motivation for carrying the computation of Theorem 1.1 was to better understand the (non-)residual finiteness of central extensions. The second result of this paper is the following:

Theorem 1.2. *The universal central extension $\widetilde{Sp(2g, \mathbb{Z})}$ is not residually finite when $g \geq 2$ since the image of the center under any homomorphism into a finite group has order at most two when $g \geq 3$. Moreover, the image of the center has order two under the natural homomorphism of $\widetilde{Sp(2g, \mathbb{Z})}$ into the universal central extension of $Sp(2g, \mathbb{Z}/D\mathbb{Z})$, where D is a multiple of 4.*

The first part of this result is the statement of Deligne's non-residual finiteness theorem from [12]. In what concerns the sharpness statement, Putman in ([58], Thm.F) has previously obtained the existence of finite index subgroups of $\widetilde{Sp(2g, \mathbb{Z})}$ which contain $2\mathbb{Z}$ but not \mathbb{Z} . We provide an explicit construction of such finite index normal subgroups derived from his computations. The relation between Theorems 1.1 and 1.2 is somewhat intricate. For instance, the statement $H_2(\widetilde{Sp(2g, \mathbb{Z}/D\mathbb{Z})}) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$, for $g \geq 3$ is a consequence of Deligne's theorem. This statement and the second part of Theorem 1.2 actually imply Theorem 1.1 and this is our first proof of the later. However, we can reverse all implications and using now a different proof of Theorem 1.1 we derive from it another proof of Theorem 1.2. In particular, this provides a new proof of Deligne's theorem, independent on Moore's theory of topological central extensions from [54].

Remark 1.1. Deligne proved that the image of twice the generator of the center under any homomorphism into a finite group is trivial, for any $g \geq 2$. We believe that this is sharp also when $g = 2$.

The theorem stated in [12] is much more general and covers higher rank Chevalley groups over number fields. The proof of Theorem 1.2 also shows that the residual finiteness of central extensions is directly related to the torsion of the second homology of finite quotients of the group. Then the general form of Deligne's theorem can be used to obtain bounds for the torsion arising in the second homology of finite quotients of symplectic groups over more general rings. To make our statement precise we introduce the notion of *essential homology* of a finite quotient of a discrete group G :

Definition 1.1. *Let G be a discrete group and F a finite group. We define the essential second homology group $EH_2(F, G)$ of F relative to G as the union:*

$$EH_2(F, G) = \bigcup_{p:G \rightarrow F} p_*(H_2(G)) \subset H_2(F) \quad (1)$$

over all surjective homomorphisms $p : G \rightarrow F$, where $p_* : H_2(M_g) \rightarrow H_2(F)$ denotes the map induced in homology and all homology groups are considered with (trivial) integral coefficients.

Notice that by definition $EH_2(F, G)$ is a torsion group. In the case G is either a mapping class group or a symplectic group we have two very different situations. First, we have:

Theorem 1.3. *Let \mathfrak{A} be the ring of S -integers of a number field which is not totally imaginary and $g \geq 3$ an integer. Then there is a uniform bound (independent on g) for the order of the torsion group $EH_2(F, Sp(2g, \mathfrak{A}))$.*

The result is a rather immediate consequence of the general Deligne theorem from [12], along with classical results of Borel and Serre ([6]) and Bass, Milnor and Serre ([3]) on the congruence subgroup problem.

Remark 1.2. With slightly more effort we can show that this holds also when the number field is totally imaginary due to the finiteness of the congruence kernel. Furthermore, the result holds for any Chevalley group instead of the symplectic group, with a similar proof. More generally it holds under the conditions of [12], namely for every absolutely simple simply connected algebraic group \mathbb{G} over a number field \mathbb{K} , S a finite set of places of \mathbb{K} containing all archimedean ones and such that $\sum_{v \in S} \text{rank } \mathbb{G}(\mathbb{K}_v) \geq 2$ and \mathfrak{A} the associated ring of S -integers. The quasi-split assumption in [12] was removed in [59]. However, for the sake of simplicity we will only consider symplectic groups in the sequel.

Theorem 1.3 contrasts with the abundance of finite quotients of mapping class groups:

Theorem 1.4. *For any prime p there exist finite quotients F of M_g , $g \geq 3$, such that $EH_2(F, M_g)$ has p -torsion.*

We prove this result by exhibiting explicit finite quotients of the universal central extension of a mapping class group that arise from the so-called quantum representations. We refine here the approach in [18] where the first author proved that central extensions of M_g by \mathbb{Z} are residually finite. In the meantime, it was proved in [19, 45] by more sophisticated tools that the set of quotients of mapping class groups contains arbitrarily large rank finite groups of Lie type. Notice however that the family of quotients obtained in Theorem 1.4 are of different nature than those obtained in [19, 47], although their source is the same (see Proposition 4.1 for details).

Theorem 1.4 shows that in the case of non-abelian quantum representations of mapping class groups there is no finite central extension for which all projective representations could be lifted to linear representations, when the genus is $g \geq 2$ (see Corollary 4.1 for the precise statement).

When G is a discrete group we denote by \widehat{G} its *profinite completion*, i.e. the projective limit of the directed system of all its finite quotients. There is a natural homomorphism $i : G \rightarrow \widehat{G}$ which is injective if and only if G is residually finite. A *discrete \widehat{G} -module* is an abelian group endowed with a continuous action of \widehat{G} . We will simply call them \widehat{G} -modules in the sequel. Recall, following ([63], I.2.6) that:

Definition 1.2. *A discrete group G has property A_n for the finite \widehat{G} -module M if the homomorphism $H^k(\widehat{G}, M) \rightarrow H^k(G, M)$ is an isomorphism for $k \leq n$ and injective for $k = n + 1$. Furthermore G is called good if it has property A_n for all n and for all finite \widehat{G} -modules.*

It is known, for instance, that all groups have property A_1 .

Now, Deligne's theorem on the non-residual finiteness of the universal central extension of $Sp(2g, \mathbb{Z})$ actually is equivalent to the fact that $Sp(2g, \mathbb{Z})$ has not property A_2 for the trivial $Sp(2g, \mathbb{Z})$ -modules (see also [25]).

Our next result is:

Theorem 1.5. *For $g \geq 4$ the mapping class group M_g has property A_2 for the trivial \widehat{M}_g -modules.*

The last part of this article is devoted to a partial extension of the method used by Putman in [58] to compute $H_2(Sp(2g, \mathbb{Z}/D\mathbb{Z})$, when $D \equiv 0 \pmod{4}$, using induction. One key point is to show that there is a potential $\mathbb{Z}/2\mathbb{Z}$ factor that appears for $H_2(Sp(2g, \mathbb{Z}/4\mathbb{Z}))$. Although we couldn't complete the proof of Theorem 1.1 this way, our main result in this direction may be of independent interest:

Theorem 1.6. *For any integers $g \geq 3$, $k \geq 1$ and prime p , we have:*

$$H_2(\mathfrak{sp}_{2g}(p))_{Sp(2g, \mathbb{Z}/p^k\mathbb{Z})} = \begin{cases} 0, & \text{if } p \text{ is odd,} \\ \mathbb{Z}/2\mathbb{Z}, & \text{if } p = 2. \end{cases}$$

An useful consequence of this result is the alternative $H_2(Sp(2g, \mathbb{Z}/4\mathbb{Z})) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$.

The plan of this article is the following.

In Section 2 we prove Theorem 1.1. Although it is easy to show from the results of Section 3.4 that the groups $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ are cyclic, their non-triviality is much more involved. That this group is trivial for $k = 1$ is a known fact, for instance by Stein results [67]. We give three different proofs of the non-triviality, each one of them having its advantages and disadvantages in terms of bounds for detections or sophistication. The first proof relies on deep results of Putman in [58], and shows that we can detect this $\mathbb{Z}/2\mathbb{Z}$ factor on $H_2(Sp(2g, \mathbb{Z}/8\mathbb{Z}))$ for $g \geq 4$, providing even an explicit extension that detects this homology class. The second proof uses mapping class groups. We show that there is a perfect candidate to detect this $\mathbb{Z}/2\mathbb{Z}$ that comes from a Weil representation of the symplectic group. This is, by construction, a representation of $Sp(2g, \mathbb{Z})$ into a projective unitary group that factors through $Sp(2g, \mathbb{Z}/4n\mathbb{Z})$. To show that it detects the factor $\mathbb{Z}/2\mathbb{Z}$ it is enough to show that this representation does not lift to a linear representation. We will show that the pull-back of the representation on the mapping class group M_g does not linearize. This proof relies on deep results of Gervais [21]. The projective representation that we use is related to the theory of theta functions on symplectic groups, this relation is explained in an appendix to this article. The third proof is K -theoretical in nature and uses a generalization of Sharpe's exact sequence relating K -theory to symplectic K -theory due to Barge and Lannes [2]. Indeed, by the stability results, this $\mathbb{Z}/2\mathbb{Z}$ should correspond to a

class in $KSp_2(\mathbb{Z}/4\mathbb{Z})$. There is a natural map from this group to a Witt group of symmetric non-degenerate bilinear forms on free $\mathbb{Z}/4\mathbb{Z}$ -modules, and it turns out that the class is detected by the class of the bilinear map of matrix $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

In Section 3 we first state the relation between the essential homology of a perfect group and residual finiteness of its universal central extension. We then prove Theorem 1.3 for Dedekind domains by analyzing Deligne's central extension. We then specify our discussion to the group $Sp(2g, \mathbb{Z})$, and show how the result stated in Theorem 1.1 allows to show that Deligne's result is sharp.

In Section 3.4 we discuss some general facts about the first and second homology groups of principal congruence subgroups of symplectic groups over Dedekind domains, again with an emphasis on the ring of integers.

Finally in Section 4 we discuss the case of the mapping class groups and prove Theorem 1.4 and Theorem 1.5 using the quantum representations that arise from the $SU(2)$ -TQFT's. These representations are the non-abelian counterpart of the Weil representations of symplectic groups, which might be described as the quantum representations that arise from the $U(1)$ -TQFT.

Finally, in appendix A we give a small overview of the relation between Weil representations and extensions of the symplectic group.

In all this work, unless otherwise specified, all (co)homology groups are with coefficients in \mathbb{Z} , and we drop it from the notation so that for a group G , $H_*(G) = H_*(G; \mathbb{Z})$ and $H^*(G) = H^*(G; \mathbb{Z})$.

Acknowledgements. We are thankful to Jean Barge, Nicolas Bergeron, Will Cavendish, Florian Deloup, Philippe Elbaz-Vincent, Richard Hain, Greg McShane, Ivan Marin, Gregor Masbaum, Alexander Rahm and Alan Reid for helpful discussions and suggestions. We are greatly indebted to an anonymous referee for pointing out a contradiction in the first version of this paper, which lead us to correcting an error in the initial statement of Theorem 1.2. We are grateful to Pierre Lochak and Andy Putman for their help in clarifying a number of technical points and improving the presentation.

2 Proof of Theorem 1.1

2.1 Preliminaries

Let $D = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ be the prime decomposition of an integer D . Then, according to ([56, Thm. 5]) we have $Sp(2g, \mathbb{Z}/D\mathbb{Z}) = \bigoplus_{i=1}^s Sp(2g, \mathbb{Z}/p_i^{n_i}\mathbb{Z})$. Since symplectic groups are perfect for $g \geq 3$ (see e.g. [58], Thm. 5.1), from the Künneth formula, we derive:

$$H_2(Sp(2g, \mathbb{Z}/D\mathbb{Z})) = \bigoplus_{i=1}^s H_2(Sp(2g, \mathbb{Z}/p_i^{n_i}\mathbb{Z})).$$

Then, from Stein's computations for $D \not\equiv 0 \pmod{4}$ (see [65, 67]), Theorem 1.1 is equivalent to the statement:

$$H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}, \text{ for all } g \geq 3, k \geq 2.$$

We will freely use in the sequel two classical results due to Stein. *Stein's isomorphism theorem* (see [65], Thm. 2.13 and Prop. 3.3.(a)), states that there is an isomorphism:

$$H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) \simeq H_2(Sp(2g, \mathbb{Z}/2^{k+1}\mathbb{Z})), \text{ for all } g \geq 3, k \geq 2.$$

Further, *Stein's stability theorem* (see [65]) states that the stabilization homomorphism $Sp(2g, \mathbb{Z}/2^k\mathbb{Z}) \hookrightarrow Sp(2g+2, \mathbb{Z}/2^k\mathbb{Z})$ induces an isomorphism:

$$H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) \simeq H_2(Sp(2g+2, \mathbb{Z}/2^k\mathbb{Z})), \text{ for all } g \geq 3, k \geq 1.$$

Therefore, to prove Theorem 1.1 it suffices to show that:

$$H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}, \text{ for some } g \geq 3, k \geq 2.$$

We provide hereafter three different proofs of this statement, each having its own advantage. For the first and the second proofs, the starting point is the intermediary result $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$, for

$g \geq 4$. This will be derived from Deligne's theorem ([12]). An alternative way is to derive it from Theorem 1.6 as it is explained in section 5.1, and more precisely in Corollary 5.2. Then it will be enough to find a non-trivial extension of $Sp(2g, \mathbb{Z}/2^k\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$ for some $g \geq 3, k \geq 2$.

In section 2.3 we show then that Putman's computations from ([58], Thm. F) provide us with a *non-trivial* central extension of $Sp(2g, \mathbb{Z}/8\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$. The second proof seems more elementary and it provides a non-trivial central extension of $Sp(2g, \mathbb{Z}/4n\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$, for all integers $n \geq 1$. Moreover, it does not use Stein's isomorphism theorem and relies instead on the study of the Weil representations of symplectic groups, or equivalently abelian quantum representations of mapping class groups. Since these representations come from theta functions this approach is deeply connected to Putman's approach. In fact the proof of the Theorem F in ([58]) is based on his Lemma 5.5 whose proof needed the transformation formulas for the classical theta nulls. The third proof, based on an extension of Sharpe's sequence in symplectic K -theory due to Barge and Lannes (see [2]), uses more sophisticated techniques but works already for $Sp(2g, \mathbb{Z}/4\mathbb{Z})$. Moreover, this last proof does not rely on Deligne's theorem.

2.2 An alternative for the order of $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$

Proposition 2.1. *We have $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$, when $g \geq 4$.*

An independent proof of the fact that $H_2(Sp(2g, \mathbb{Z}/4\mathbb{Z})) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$, when $g \geq 4$ will be given in section 5.1, under the form of Corollary 5.2 of Theorem 1.6. The claim holds when $g = 3$ as well, by Stein's stability theorem.

We prove here that Proposition 2.1 is a rather immediate consequence of Deligne's theorem. Let $p : Sp(2g, \mathbb{Z}) \rightarrow Sp(2g, \mathbb{Z}/2^k\mathbb{Z})$ be the reduction mod 2^k and $p_* : H_2(Sp(2g, \mathbb{Z})) \rightarrow H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ the induced homomorphism. The first ingredient in the proof is the following result which seems well-known:

Lemma 2.1. *The homomorphism $p_* : H_2(Sp(2g, \mathbb{Z})) \rightarrow H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ is surjective.*

This is a direct consequence of the more general Proposition 3.3, which will be proved in section 3.4. Here we use this lemma only to obtain that $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ is cyclic, and this was already shown by Stein in [65].

Now, it is a classical result that $H_1(Sp(2g, \mathbb{Z})) = 0$, for $g \geq 3$ and $H_2(Sp(2g, \mathbb{Z})) = \mathbb{Z}$, for $g \geq 4$ (see e.g. [58], Thm. 5.1). This implies that $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ is cyclic, when $g \geq 4$ and we only have to bound its order. Notice in contrast that $H_2(Sp(6, \mathbb{Z})) = \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ according to [66]. Further we have the following general statement:

Lemma 2.2. *Let Γ and F be perfect groups, $\tilde{\Gamma}$ and \tilde{F} their universal central extensions and $p : \Gamma \rightarrow F$ be a group homomorphism. Then there exists a unique homomorphism $\tilde{p} : \tilde{\Gamma} \rightarrow \tilde{F}$ lifting p such that the following diagram is commutative:*

$$\begin{array}{ccccccc} 1 & \rightarrow & H_2(\Gamma) & \rightarrow & \tilde{\Gamma} & \rightarrow & \Gamma \\ & & p_* \downarrow & & \tilde{p} \downarrow & & \downarrow p \\ 1 & \rightarrow & H_2(F) & \rightarrow & \tilde{F} & \rightarrow & F \\ & & & & & & \rightarrow 1 \end{array}$$

Proof of Lemma 2.2. For any perfect group G , by the universal coefficients theorem there is a natural isomorphism $H^2(G, H_2(G)) = \text{Hom}(H_2(G), H_2(G))$, and the universal central extension corresponds under this isomorphism to the identity homomorphism $\mathbf{1}_{H_2(G)}$. The existence of the map \tilde{p} is then equivalent to the trivial fact that $p_* \circ \mathbf{1}_{H_2(F)} = \mathbf{1}_{H_2(\Gamma)} \circ p_*$. The set of such homomorphisms \tilde{p} if not empty, is in one-to-one correspondence with the set

$$H^1(\Gamma, H_2(F)) = \text{Hom}(H_1(\Gamma), H_2(F)) = 0$$

and this settles the uniqueness statement. \square

Proof Proposition 2.1. Lemma 2.2 provides a lift between the universal central extensions $\tilde{p} : \widetilde{Sp(2g, \mathbb{Z})} \rightarrow \widetilde{Sp(2g, \mathbb{Z}/2^k\mathbb{Z})}$ of the mod 2^k reduction map, such that the restriction of \tilde{p} to the center $H_2(Sp(2g, \mathbb{Z}))$ of $Sp(2g, \mathbb{Z})$ is the homomorphism $p_* : H_2(Sp(2g, \mathbb{Z})) \rightarrow H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$.

Assume now that Deligne's theorem holds, namely that every finite index subgroup of the universal central extension $\widetilde{Sp(2g, \mathbb{Z})}$, for $g \geq 4$, contains $2\mathbb{Z}$, where \mathbb{Z} is the central kernel $\ker(\widetilde{Sp(2g, \mathbb{Z})} \rightarrow Sp(2g, \mathbb{Z}))$. Let

c be a generator of \mathbb{Z} . This implies that $2p_*(c) = \tilde{p}(2c) = 0$. According to Lemma 2.1 p_* is surjective and thus $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ is a quotient of $\mathbb{Z}/2\mathbb{Z}$, as claimed. \square

2.3 First proof: an explicit extension detecting $H_2(Sp(2g, \mathbb{Z}/8\mathbb{Z})) = \mathbb{Z}/2$

According to Proposition 2.1, in order to prove Theorem 1.1 it is enough to provide a non-trivial central extension of $Sp(2g, \mathbb{Z}/2^k\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$, for some $g \geq 3$ and $k \geq 2$.

As ingredients of our proof we use the following results of Putman (see [58], Lemma 5.5 and Thm. F), which we state here in a unified way:

Proposition 2.2. *The pull-back $\widetilde{Sp(2g, 2)}$ of the universal central extension $\widetilde{Sp(2g, \mathbb{Z})}$ under the inclusion homomorphism $Sp(2g, 2) \rightarrow Sp(2g, \mathbb{Z})$ is a central extension of $Sp(2g, 2)$ by \mathbb{Z} whose extension class in $H^2(Sp(2g, 2))$ is even.*

Let $\widetilde{G} \subset \widetilde{Sp(2g, 2)}$ be the central extension of $Sp(2g, 2)$ by \mathbb{Z} whose extension class is half the extension class of $Sp(2g, 2)$. We have then a commutative diagram:

$$\begin{array}{ccccccc} 1 \rightarrow & \mathbb{Z} & \rightarrow & \widetilde{G} & \rightarrow & Sp(2g, 2) & \rightarrow 1 \\ & \downarrow \times 2 & & \downarrow & & \downarrow \cong & \\ 1 \rightarrow & \mathbb{Z} & \rightarrow & \widetilde{Sp(2g, 2)} & \rightarrow & Sp(2g, 2) & \rightarrow 1 \\ & \downarrow \cong & & \downarrow & & \downarrow & \\ 1 \rightarrow & \mathbb{Z} & \rightarrow & \widetilde{Sp(2g, \mathbb{Z})} & \rightarrow & Sp(2g, \mathbb{Z}) & \rightarrow 1. \end{array} \quad (2)$$

In this section we will denote by $i : \mathbb{Z} \rightarrow \widetilde{Sp(2g, \mathbb{Z})}$ the inclusion of the center and by $p : \widetilde{Sp(2g, \mathbb{Z})} \rightarrow Sp(2g, \mathbb{Z})$ the projection killing $i(\mathbb{Z})$. Now \widetilde{G} is a subgroup of index 2 of $\widetilde{Sp(2g, 2)}$ and hence a normal subgroup of the form $\ker f$, where $f : \widetilde{Sp(2g, 2)} \rightarrow \mathbb{Z}/2\mathbb{Z}$ is some group homomorphism. In particular, f factors through the abelianization homomorphism $F : \widetilde{Sp(2g, 2)} \rightarrow H_1(\widetilde{Sp(2g, 2)})$. We denote by \widetilde{K} the kernel $\ker F$. Then $\widetilde{K} \subset \widetilde{G}$.

Lemma 2.3. *The image $K = p(\widetilde{K})$ under the projection $p : \widetilde{Sp(2g, \mathbb{Z})} \rightarrow Sp(2g, \mathbb{Z})$ is the kernel of the abelianization homomorphism $Sp(2g, 2) \rightarrow H_1(Sp(2g, 2))$. In particular K is the Igusa subgroup $Sp(2g, 4, 8)$ of $Sp(2g, 4)$ consisting of those symplectic matrices $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ with the property that the diagonal entries of AB^\top and CD^\top are multiples of 8.*

Proof of lemma 2.3. Let $\phi : Sp(2g, 2) \rightarrow H_1(Sp(2g, 2))/F(i(\mathbb{Z}))$ be the map defined by:

$$\phi(x) = F(\tilde{x}),$$

where \tilde{x} is an arbitrary lift of x to $\widetilde{Sp(2g, 2)}$. Then ϕ is a well-defined homomorphism. Moreover, $p(\widetilde{K})$ is $\ker \phi$.

The 5-term exact sequence associated to the central extension $\widetilde{Sp(2g, 2)}$ is:

$$H_2(Sp(2g, 2)) \rightarrow (H_1(\mathbb{Z}))_{Sp(2g, 2)} \rightarrow H_1(\widetilde{Sp(2g, 2)}) \rightarrow H_1(Sp(2g, 2)) \rightarrow 0.$$

The image of $(H_1(\mathbb{Z}))_{Sp(2g, 2)} \cong \mathbb{Z}$ into $H_1(\widetilde{Sp(2g, 2)})$ in the sequence above is the subgroup $F(i(\mathbb{Z}))$. Therefore p induces an isomorphism between $H_1(Sp(2g, 2))/F(\mathbb{Z})$ and $H_1(Sp(2g, 2))$. This proves the first claim.

The second claim follows from Sato's computation of $H_1(Sp(2g, 2))$, (see [62], Proposition 2.1) where he identifies the commutator subgroup $[Sp(2g, 2), Sp(2g, 2)]$ with $Sp(2g, 4, 8)$. \square

Lemma 2.4. *The subgroups \widetilde{K} and K are normal subgroups of $\widetilde{Sp(2g, \mathbb{Z})}$ and $Sp(2g, \mathbb{Z})$, respectively.*

Proof of lemma 2.4. For any group G the subgroup $\ker(G \rightarrow H_1(G))$ is characteristic. Now the group $\widetilde{Sp(2g, \mathbb{Z})}$ acts by conjugation on its normal subgroup $\widetilde{Sp(2g, 2)}$ and since \widetilde{K} is a characteristic subgroup of $\widetilde{Sp(2g, 2)}$ it is therefore preserved by the conjugacy action of $\widetilde{Sp(2g, \mathbb{Z})}$ and hence a normal subgroup. The proof of the other statement is similar. The fact that $Sp(2g, 4, 8)$ is a normal subgroup of $Sp(2g, \mathbb{Z})$ was proved by Igusa (see [36], Lemma 1.(i)). \square

Lemma 2.5. *If $\widetilde{H} \subset \widetilde{G}$ is a normal finite index subgroup of $\widetilde{Sp(2g, \mathbb{Z})}$, then $\widetilde{H} \cap i(\mathbb{Z}) = 2 \cdot i(\mathbb{Z})$.*

Proof of lemma 2.5. We have $\widetilde{H} \cap i(\mathbb{Z}) \subset \widetilde{G} \cap i(\mathbb{Z}) = 2 \cdot i(\mathbb{Z})$ so that $\widetilde{H} \cap i(\mathbb{Z}) = m \cdot i(\mathbb{Z})$, with $m \geq 2$ or $m = 0$. Then $m \neq 0$ since \widetilde{H} was supposed to be of finite index in $\widetilde{Sp(2g, \mathbb{Z})}$. If $m > 2$ then the projection homomorphism $\widetilde{Sp(2g, \mathbb{Z})} \rightarrow \widetilde{Sp(2g, \mathbb{Z})}/\widetilde{H}$ would send the center $i(\mathbb{Z})$ into $\mathbb{Z}/m\mathbb{Z}$, contradicting Deligne's theorem ([12]). Thus $m = 2$. \square

Lemma 2.6. *The subgroup \widetilde{K} is of finite index in $\widetilde{Sp(2g, \mathbb{Z})}$.*

Proof of lemma 2.6. By definition of \widetilde{K} it is equivalent to prove that $H_1(\widetilde{Sp(2g, 2)})$ is a finite abelian group. From the 5-term exact sequence above, and since the group $H_1(\widetilde{Sp(2g, 2)})$ is finite, it is enough to show that the image of $H_1(\mathbb{Z})_{Sp(2g, 2)}$ is finite in $H_1(\widetilde{Sp(2g, 2)})$ and this is precisely the image of the center of $\widetilde{Sp(2g, \mathbb{Z})}$. If this image is infinite in $H_1(\widetilde{Sp(2g, 2)})$, then we could find finite abelian quotients of $\widetilde{Sp(2g, 2)}$ for which the center is sent into $\mathbb{Z}/m\mathbb{Z}$, for arbitrary large m . Using induction we obtain finite representations of $\widetilde{Sp(2g, \mathbb{Z})}$ with the same property, contradicting Deligne's theorem. \square

Proposition 2.3. *If $H \subset Sp(2g, 4, 8)$ is a principal congruence subgroup of $Sp(2g, \mathbb{Z})$ and $g \geq 3$ then $H_2(Sp(2g, \mathbb{Z})/H) = \mathbb{Z}/2\mathbb{Z}$. In particular for all $k \geq 3$, we have $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z})) \simeq H_2(Sp(2g, \mathbb{Z}/8\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}$.*

Proof. Let $\widetilde{H} \subset \widetilde{K}$ be the pull-back of the central extension $\widetilde{Sp(2g, \mathbb{Z})}$ under the inclusion homomorphism $H \subset Sp(2g, \mathbb{Z})$, which is a normal finite index subgroup of $Sp(2g, \mathbb{Z})$. Then the image of the center $i(\mathbb{Z})$ by the projection homomorphism $\widetilde{Sp(2g, \mathbb{Z})} \rightarrow \widetilde{Sp(2g, \mathbb{Z})}/\widetilde{H}$ is of order two. Therefore we have a central extension:

$$0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \widetilde{Sp(2g, \mathbb{Z})}/\widetilde{H} \rightarrow Sp(2g, \mathbb{Z})/H \rightarrow 0.$$

If the extension $\widetilde{Sp(2g, \mathbb{Z})}/\widetilde{H}$ were trivial then we would obtain a surjective homomorphism $\widetilde{Sp(2g, \mathbb{Z})} \rightarrow \mathbb{Z}/2\mathbb{Z}$. But $H_1(\widetilde{Sp(2g, \mathbb{Z})}) = 0$ by universality. Therefore $H^2(Sp(2g, \mathbb{Z})/H; \mathbb{Z}/2\mathbb{Z}) \neq 0$. By Deligne's theorem $H_2(Sp(2g, \mathbb{Z})/H) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$ and hence $H_2(Sp(2g, \mathbb{Z})/H) = \mathbb{Z}/2\mathbb{Z}$. \square

2.4 Second proof: detecting the non-trivial class via Weil representations

2.4.1 Preliminaries on Weil representations

The projective representation that we use is related to the theory of theta functions on symplectic groups, this relation being briefly explained in an appendix to this article. Although the Weil representations of symplectic groups over finite fields of characteristic different from 2 is a classical subject present in many textbooks, the slightly more general Weil representations associated to finite rings of the form $\mathbb{Z}/k\mathbb{Z}$ received less consideration until recently. They first appeared in print as representations associated to finite abelian groups in [38] for genus $g = 1$ and were extended to locally compact abelian groups in ([70], Chapter I) and independently in the work of Igusa and Shimura on theta functions (see [35, 64, 34]) and in physics literature ([28]). They were rediscovered as monodromies of generalized theta functions arising in the $U(1)$ Chern-Simons theory in [16, 23, 17] and then in finite-time frequency analysis (see [37] and references from there). In [16, 17, 23] these are projective representations of the symplectic group factorizing through the finite congruence quotients $Sp(2g, \mathbb{Z}/2k\mathbb{Z})$, which are only defined for even $k \geq 2$. However, for odd k the monodromy of theta functions lead to representations of the theta subgroup of $Sp(2g, \mathbb{Z})$. These also factor through the image of the theta group into the finite congruence quotients $Sp(2g, \mathbb{Z}/2k\mathbb{Z})$. Notice however that the original Weil construction works as well for $\mathbb{Z}/k\mathbb{Z}$ with odd k (see e.g. [27, 37]).

It is well-known (see [70] sections 43, 44 or [60], Prop. 5.8) that these projective Weil representations lift to linear representations of the integral metaplectic group, which is the pull-back of the symplectic group in a double cover of $Sp(2g, \mathbb{R})$. The usual way to resolve the projective ambiguities is to use the Maslov cocycle (see e.g. [69]). Moreover, it is known that the Weil representations over finite fields of odd characteristic and over \mathbb{C} actually are linear representations. In fact the vanishing of the second power of the augmentation ideal of the Witt ring of such fields (see e.g. [68, 42]) implies that the corresponding metaplectic extension splits. This contrasts with the fact that Weil representations over \mathbb{R} (or any local field different from \mathbb{C}) are true representations of the real metaplectic group and cannot be linearized (see e.g. [42]). The Weil representations over local fields of characteristic 2 is subtler as they are rather representations of a double cover of the so-called pseudo-symplectic group (see [70] and [26] for recent work).

Let $k \geq 2$ be an integer, and denote by \langle , \rangle the standard bilinear form on $(\mathbb{Z}/k\mathbb{Z})^g \times (\mathbb{Z}/k\mathbb{Z})^g \rightarrow \mathbb{Z}/k\mathbb{Z}$. The Weil representation we consider is a representation in the unitary group of the complex vector space $\mathbb{C}^{(\mathbb{Z}/k\mathbb{Z})^g}$ endowed with its standard Hermitian form. Notice that the canonical basis of this vector space is canonically labeled by elements in $\mathbb{Z}/k\mathbb{Z}$.

It is well-known (see e.g. [36]) that $Sp(2g, \mathbb{Z})$ is generated by the matrices having one of the following forms: $\begin{pmatrix} \mathbf{1}_g & B \\ 0 & \mathbf{1}_g \end{pmatrix}$ where $B = B^\top$ has integer entries, $\begin{pmatrix} A & 0 \\ 0 & (A^\top)^{-1} \end{pmatrix}$ where $A \in GL(g, \mathbb{Z})$ and $\begin{pmatrix} 0 & -\mathbf{1}_g \\ \mathbf{1}_g & 0 \end{pmatrix}$.

We can now define the Weil representations (see the Appendix for more details) on these generating matrices as follows:

$$\rho_{g,k} \begin{pmatrix} \mathbf{1}_g & B \\ 0 & \mathbf{1}_g \end{pmatrix} = \text{diag} \left(\exp \left(\frac{\pi\sqrt{-1}}{k} \langle m, Bm \rangle \right) \right)_{m \in (\mathbb{Z}/k\mathbb{Z})^g}, \quad (3)$$

where diag stands for diagonal matrix with given entries;

$$\rho_{g,k} \begin{pmatrix} A & 0 \\ 0 & (A^\top)^{-1} \end{pmatrix} = (\delta_{A^\top m, n})_{m, n \in (\mathbb{Z}/k\mathbb{Z})^g}, \quad (4)$$

where δ stands for the Kronecker symbol;

$$\rho_{g,k} \begin{pmatrix} 0 & -\mathbf{1}_g \\ \mathbf{1}_g & 0 \end{pmatrix} = k^{-g/2} \exp \left(-\frac{2\pi\sqrt{-1}\langle m, n \rangle}{k} \right)_{m, n \in (\mathbb{Z}/k\mathbb{Z})^g}. \quad (5)$$

It is proved in [17, 23], that for even k these formulas define a unitary representation $\rho_{g,k}$ of $Sp(2g, \mathbb{Z})$ in $U(\mathbb{C}^{(\mathbb{Z}/k\mathbb{Z})^g})/R_8$. Here $U(\mathbb{C}^N) = U(N)$ denotes the unitary group of dimension N and $R_8 \subset U(1) \subset U(\mathbb{C}^N)$ is the subgroup of scalar matrices whose entries are roots of unity of order 8. For odd k the same formulas define representations of the theta subgroup $Sp(2g, 1, 2)$ (see [36, 35, 17]). Notice that by construction $\rho_{g,k}$ factors through $Sp(2g, \mathbb{Z}/2k\mathbb{Z})$ for even k and through the image of the theta subgroup in $Sp(2g, \mathbb{Z}/k\mathbb{Z})$ for odd k .

The terminology "Weil representation" is misleading since it is not properly a representation, but only a projective one. However our definition gives us a map (say for even k) $\rho_{g,k} : Sp(2g, \mathbb{Z}) \rightarrow U(\mathbb{C}^{(\mathbb{Z}/k\mathbb{Z})^g})$ satisfying the cocycle condition:

$$\rho_{g,k}(AB) = \eta(A, B)\rho_{g,k}(A)\rho_{g,k}(B)$$

for all $A, B \in Sp(2g, \mathbb{Z})$ and some $\eta(A, B) \in R_8$.

Proposition 2.4. *The projective Weil representation $\rho_{g,k}$ of $Sp(2g, \mathbb{Z})$, for $g \geq 3$ and even k does not lift to linear representations of $Sp(2g, \mathbb{Z})$, namely it determines a generator of $H^2(Sp(2g, \mathbb{Z}/2k\mathbb{Z}); \mathbb{Z}/2\mathbb{Z})$.*

Remark 2.1. For odd k it was already known that Weil representations did not detect any non-trivial element, i.e. that the projective representation $\rho_{g,k}$ lifts to a linear representation [1], we will give a very short outline of this at the end of the Appendix.

The element $\rho_{g,k} \begin{pmatrix} 0 & -\mathbf{1}_g \\ \mathbf{1}_g & 0 \end{pmatrix}$ will be central in our argument, we will denote it by S .

The rest of this section is devoted to the proof of Proposition 2.4.

2.4.2 Outline of the proof

We use again, as in the first proof, Proposition 2.1.

The projective Weil representation $\rho_{g,k}$ determines a central extension of $Sp(2g, \mathbb{Z}/2k\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$, since it factors through the metaplectic central extension, by [70]. We will prove that this central extension is non-trivial thereby proving the claim. The pull-back of this central extension by the homomorphism $Sp(2g, \mathbb{Z}) \rightarrow Sp(2g, \mathbb{Z}/2k\mathbb{Z})$ is a central extension of $Sp(2g, \mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$ and it is enough to prove that this last extension is non-trivial. It turns out to be easier to describe the pull-back of this central extension over the mapping class group M_g of the genus g closed orientable surface. Denote by \tilde{M}_g the pull-back of the central extension above under the homomorphism $M_g \rightarrow Sp(2g, \mathbb{Z})$. By the stability results of Harer for $g \geq 5$, and the low dimensional computations in [57] and [40] for $g \geq 4$, the natural homomorphism $M_g \rightarrow Sp(2g, \mathbb{Z})$, obtained by choosing a symplectic basis in the surface homology induces isomorphisms $H_2(M_g; \mathbb{Z}) \rightarrow H_2(Sp(2g, \mathbb{Z}); \mathbb{Z})$ and $H^2(Sp(2g, \mathbb{Z}); \mathbb{Z}) \rightarrow H^2(M_g; \mathbb{Z})$ for $g \geq 4$. In particular in this range the class of the central extension \tilde{M}_g is a generator of $H^2(M_g; \mathbb{Z}/2\mathbb{Z})$. In contrast for $g = 3$, there is an element of infinite order in $H^2(M_3; \mathbb{Z})$ such that its reduction mod 2 is the class of the central extension \tilde{M}_g , but it is only known that $H^2(M_3; \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z} + A$ where A is either $\mathbb{Z}/2$ or 0. Therefore, we can reformulate Proposition 2.4 at least for $g \geq 4$ in equivalent form in terms of the mapping class group:

Proposition 2.5. *If $g \geq 4$ then the class of the central extension \tilde{M}_g is a generator of $H^2(M_g; \mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$.*

The proof reduces to a computation which is also valid when $g = 3$. This proves that the central extension coming from the Weil representation (and hence its cohomology class with $\mathbb{Z}/2\mathbb{Z}$ coefficients) for $g = 3$ is non-trivial. We won't need Stein stability results unless we want to identify this class with some mod 2 reduction of the universal central extension of $Sp(6, \mathbb{Z})$.

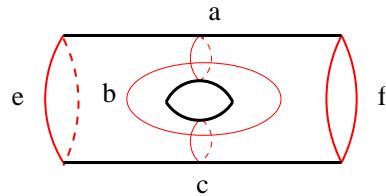
2.4.3 A presentation of \tilde{M}_g

The method we use is due to Gervais (see [21]) and was already used in [20] for computing central extensions arising in quantum Teichmüller space. We start with a number of notations and definitions. Recall that $\Sigma_{g,r}$ denotes the orientable surface of genus g with r boundary components. If γ is a curve on a surface then D_γ denotes the right Dehn twist along the curve γ .

Definition 2.1. *A chain relation C on the surface $\Sigma_{g,r}$ is given by an embedding $\Sigma_{1,2} \subset \Sigma_{g,r}$ and the standard chain relation on this 2-holed torus, namely*

$$(D_a D_b D_c)^4 = D_e D_d,$$

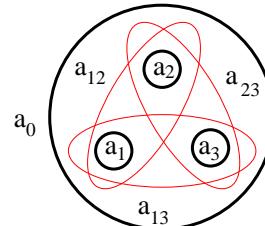
where a, b, c, d, e, f are the following curves of the embedded 2-holed torus:



Definition 2.2. *A lantern relation L on the surface $\Sigma_{g,r}$ is given by an embedding $\Sigma_{0,4} \subset \Sigma_{g,r}$ and the standard lantern relation on this 4-holed sphere, namely*

$$D_{a_{12}} D_{a_{13}} D_{a_{23}} D_{a_0}^{-1} D_{a_1}^{-1} D_{a_2}^{-1} D_{a_3}^{-1} = 1, \quad (6)$$

where $a_0, a_1, a_2, a_3, a_{12}, a_{13}, a_{23}$ are the following curves of the embedded 4-holed sphere:



The following lemma is a simple consequence of a deep result of Gervais from ([21]):

Lemma 2.7. *Let $g \geq 3$. Then the group M_g is presented as follows:*

1. Generators are all Dehn twists D_a along the non-separating simple closed curves a on Σ_g .

2. Relations:

(a) Braid-type 0 relations:

$$D_a D_b = D_b D_a,$$

for each pair of disjoint non-separating simple closed curves a and b ;

(b) Braid type 1 relations:

$$D_a D_b D_a = D_b D_a D_b,$$

for each pair of non-separating simple closed curves a and b which intersect transversely in one point;

(c) One lantern relation for a 4-holed sphere embedded in Σ_g so that all boundary curves are non-separating;

(d) One chain relation for a 2-holed torus embedded in Σ_g so that all boundary curves are non-separating;

The key step in proving Proposition 2.5 and hence Proposition 2.4 is to find an explicit presentation for the central extension \widetilde{M}_g . By definition, if we choose arbitrary lifts $\widetilde{D}_a \in \widetilde{M}_g$ for each of Dehn twists $D_a \in M_g$, then \widetilde{M}_g is generated by the elements \widetilde{D}_a plus a central element z of order at most 2. Specifically, as a consequence of Gervais' presentation [21] of the universal central extension of the mapping class group, the group \widetilde{M}_g in the next proposition determines canonically a non-trivial central extension of M_g by $\mathbb{Z}/2\mathbb{Z}$.

Proposition 2.6. *Suppose that $g \geq 3$. Then the group \widetilde{M}_g has the following presentation.*

1. Generators:

(a) With each non-separating simple closed curve a in Σ_g is associated a generator \widetilde{D}_a ;

(b) One (central) element z .

2. Relations:

(a) Centrality:

$$z \widetilde{D}_a = \widetilde{D}_a z, \quad (7)$$

for any non-separating simple closed curve a on Σ_g ;

(b) Braid type 0-relations:

$$\widetilde{D}_a \widetilde{D}_b = \widetilde{D}_b \widetilde{D}_a, \quad (8)$$

for each pair of disjoint non-separating simple closed curves a and b ;

(c) Braid type 1-relations:

$$\widetilde{D}_a \widetilde{D}_b \widetilde{D}_a = \widetilde{D}_b \widetilde{D}_a \widetilde{D}_b, \quad (9)$$

for each pair of non-separating simple closed curves a and b which intersect transversely at one point;

(d) One lantern relation on a 4-holed sphere subsurface with non-separating boundary curves:

$$\widetilde{D}_{a_0} \widetilde{D}_{a_1} \widetilde{D}_{a_2} \widetilde{D}_{a_3} = \widetilde{D}_{a_{12}} \widetilde{D}_{a_{13}} \widetilde{D}_{a_{23}}, \quad (10)$$

(e) One chain relation on a 2-holed torus subsurface with non-separating boundary curves:

$$(\widetilde{D}_a \widetilde{D}_b \widetilde{D}_c)^4 = z \widetilde{D}_e \widetilde{D}_d. \quad (11)$$

(f) Scalar equation:

$$z^2 = 1. \quad (12)$$

Moreover $z \neq 1$.

2.4.4 Proof of Proposition 2.6

By definition \widetilde{M}_g fits into a commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \widetilde{M}_g & \longrightarrow & M_g \longrightarrow 1 \\ & & \parallel & & \downarrow & & \downarrow \rho_{g,k} \\ 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \widetilde{\rho_{g,k}(M_g)} & \longrightarrow & \rho_{g,k}(M_g) \longrightarrow 1, \end{array}$$

where $\widetilde{\rho_{g,k}(M_g)} \subset U(\mathbb{C}^{(\mathbb{Z}/k\mathbb{Z})^g})$. This presents \widetilde{M}_g as a pull-back and therefore the relations claimed in Proposition 2.6 will be satisfied if and only if they are satisfied when we project them into M_g and $\widetilde{\rho_{g,k}(M_g)} \subset U(\mathbb{C}^{(\mathbb{Z}/k\mathbb{Z})^g})$. If this is the case then \widetilde{M}_g will be a quotient of the group obtained from the universal central extension by reducing mod 2 the center and that surjects onto M_g . But, as the mapping class group is Hopfian there are only two such groups: first, $M_g \times \mathbb{Z}/2\mathbb{Z}$ with the obvious projection on M_g and second, the mod 2 reduction of the universal central extension. Then relation (e) shows that we are in the latter case.

The projection on M_g is obtained by killing the center z , and by construction the projected relations are satisfied in M_g and we only need to check them in the unitary group.

Lemma 2.8. *For any lifts \tilde{D}_a of the Dehn twists D_a we have $\tilde{D}_a \tilde{D}_b = \tilde{D}_b \tilde{D}_a$ and thus relations (2) are satisfied.*

Proof. The commutativity relations are satisfied for particular lifts and hence for arbitrary lifts. \square

Lemma 2.9. *There are lifts \tilde{D}_a of the Dehn twists D_a , for each non-separating simple closed curve a such that we have*

$$\tilde{D}_a \tilde{D}_b \tilde{D}_a = \tilde{D}_b \tilde{D}_a \tilde{D}_b$$

for any simple closed curves a, b with one intersection point and thus the braid type 1-relations (3) are satisfied.

Proof. Consider an arbitrary lift of one braid type 1-relation (to be called the fundamental one), which has the form $\tilde{D}_a \tilde{D}_b \tilde{D}_a = z^k \tilde{D}_b \tilde{D}_a \tilde{D}_b$. Change then the lift \tilde{D}_b to $z^k \tilde{D}_b$. With the new lift the relation above becomes $\tilde{D}_a \tilde{D}_b \tilde{D}_a = \tilde{D}_b \tilde{D}_a \tilde{D}_b$.

Choose now an arbitrary braid type 1-relation of $\Gamma_{g,r}^s$, say $D_x D_y D_x = D_y D_x D_y$. There exists a 1-holed torus $\Sigma_{1,1} \subset \Sigma_{g,r}^s$ containing x, y , namely a neighborhood of $x \cup y$. Let T be the similar torus containing a, b . Since a, b and x, y are non-separating there exists a homeomorphism $\varphi : \Sigma_{g,r}^s \rightarrow \Sigma_{g,r}^s$ such that $\varphi(a) = x$ and $\varphi(b) = y$. We have then

$$D_x = \varphi D_a \varphi^{-1}, \quad D_y = \varphi D_b \varphi^{-1}.$$

Let us consider now an arbitrary lift $\tilde{\varphi}$ of φ , which is well-defined only up to a central element, and set

$$\tilde{D}_x = \tilde{\varphi} \tilde{D}_a \tilde{\varphi}^{-1}, \quad \tilde{D}_y = \tilde{\varphi} \tilde{D}_b \tilde{\varphi}^{-1}.$$

These lifts are well-defined since they do not depend on the choice of $\tilde{\varphi}$ (the central elements coming from $\tilde{\varphi}$ and $\tilde{\varphi}^{-1}$ mutually cancel). Moreover, we have then

$$\tilde{D}_x \tilde{D}_y \tilde{D}_x = \tilde{D}_y \tilde{D}_x \tilde{D}_y$$

and so the braid type 1-relations (3) are all satisfied. \square

Lemma 2.10. *The choice of lifts of all \tilde{D}_x , with x non-separating, satisfying the requirements of Lemma 2.9 is uniquely defined by fixing the lift \tilde{D}_a of one particular Dehn twist.*

Proof. In fact the choice of \tilde{D}_a fixes the choice of \tilde{D}_b . If x is a non-separating simple closed curve on Σ_g , then there exists another non-separating curve y which intersects it in one point. Thus, by Lemma 2.9, the choice of \tilde{D}_x is unique. \square

Lemma 2.11. *One can choose the lifts of Dehn twists in \widetilde{M}_g so that all braid type relations are satisfied and the lift of the lantern relation is trivial, namely*

$$\widetilde{D}_a \widetilde{D}_b \widetilde{D}_c \widetilde{D}_d = \widetilde{D}_u \widetilde{D}_v \widetilde{D}_w,$$

for the non-separating curves on an embedded $\Sigma_{0,4} \subset \Sigma_g$.

Proof. An arbitrary lift of that lantern relation is of the form $\widetilde{D}_a \widetilde{D}_b \widetilde{D}_c \widetilde{D}_d = z^k \widetilde{D}_u \widetilde{D}_v \widetilde{D}_w$. In this case, we change the lift \widetilde{D}_a into $z^{-k} \widetilde{D}_a$ and adjust the lifts of all other Dehn twists along non-separating curves the way that all braid type 1-relations are satisfied. Then, the required form of the lantern relation is satisfied. \square

We say that the lifts of the Dehn twists are *normalized* if all braid type relations and one lantern relation are lifted in a trivial way.

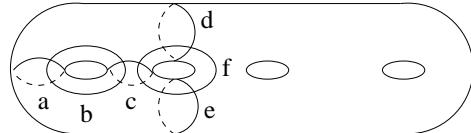
Now the proposition follows from:

Lemma 2.12. *If all lifts of the Dehn twist generators are normalized then $(\widetilde{D}_a \widetilde{D}_b \widetilde{D}_c)^4 = z \widetilde{D}_e \widetilde{D}_d$, where $z \neq 1, z^2 = 1$.*

Proof. We denote by T_γ the action of D_γ in homology. Moreover we denote by R_γ the matrix in $U(\mathbb{C}^{(\mathbb{Z}/k\mathbb{Z})^g})$ corresponding to the prescribed lift $\rho_{g,k}(T_\gamma)$ of the projective representation. The level k is fixed through this section and we drop the subscript k from now on.

Our strategy is as follows. We show that the braid relations are satisfied by the matrices R_γ . It remains to compute the defect of the chain relation in the matrices R_γ .

Consider an embedding of $\Sigma_{1,2} \subset \Sigma_g$ such that all curves from the chain relation are non-separating, and thus like in the figure below:



The subgroup generated by D_a, D_b, D_c, D_d, D_e and D_f act on the homology of the surface Σ_g by preserving the symplectic subspace generated by the homology classes of a, e, b, f and being identity on its orthogonal complement. Now the Weil representation behaves well with respect to the direct sum of symplectic matrices and this enables us to focus our attention on the action of this subgroup on the 4-dimensional symplectic subspace generated by a, e, b, f and to use $\rho_{2,k}$. In this basis the symplectic matrices associated to the above Dehn twists are:

$$T_a = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad T_b = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad T_c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & -1 & 1 & 0 \\ -1 & -1 & 0 & 1 \end{pmatrix},$$

$$T_d = T_e = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}, \quad T_f = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Notice that $T_b = J^{-1} T_a J$, where J is the matrix of the standard symplectic structure.

Set $q = \exp(\frac{\pi i}{k})$, which is a $2k$ -th root of unity. We will change slightly the basis $\{\theta_m, m \in (\mathbb{Z}/k\mathbb{Z})^g\}$ of our representation vector space in order to exchange the two obvious parabolic subgroups of $Sp(2g, \mathbb{Z})$. Specifically we fix the basis given by $-S\theta_m$, with $m \in (\mathbb{Z}/k\mathbb{Z})^g$. We have then:

$$R_a = \text{diag}(q^{\langle L_a x, x \rangle})_{x \in (\mathbb{Z}/k\mathbb{Z})^2}, \text{ where } L_a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$R_c = \text{diag}(q^{\langle L_c x, x \rangle})_{x \in (\mathbb{Z}/k\mathbb{Z})^2}, \text{ where } L_c = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

and

$$R_e = R_d = \text{diag}(q^{\langle L_e x, x \rangle})_{x \in (\mathbb{Z}/k\mathbb{Z})^2}, \text{ where } L_e = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

We set now:

$$R_b = S^3 R_a S \text{ and } R_f = S^3 R_e S,$$

where

Lemma 2.13. *The matrices R_a, R_b, R_c, R_f, R_e are normalized lifts, namely the braid relations are satisfied.*

We postpone the proof of this lemma a few lines. Let us denote by $G(u, v)$ the Gauss sum:

$$G(u, v) = \sum_{x \in \mathbb{Z}/v\mathbb{Z}} \exp\left(\frac{2\pi\sqrt{-1}ux^2}{v}\right).$$

According to [41], p.85-91 the value of the Gauss sum is

$$G(u, v) = dG\left(\frac{u}{d}, \frac{v}{d}\right), \text{ if g.c.d.}(u, v) = d,$$

and for $\text{g.c.d.}(u, v) = 1$ we have:

$$G(u, v) = \begin{cases} \varepsilon(v) \left(\frac{u}{v}\right) \sqrt{v}, & \text{for odd } v, \\ 0, & \text{for } v = 2(\text{mod } 4), \\ \overline{\varepsilon(u)} \left(\frac{v}{u}\right) \left(\frac{1+\sqrt{-1}}{\sqrt{2}}\right) \sqrt{2v}, & \text{for } v = 0(\text{mod } 4). \end{cases}$$

Here $\left(\frac{u}{v}\right)$ is the Jacobi symbol and

$$\varepsilon(a) = \begin{cases} 1, & \text{if } a = 1(\text{mod } 4), \\ \sqrt{-1}, & \text{if } a = 3(\text{mod } 4). \end{cases}$$

Remember that the Jacobi (or the quadratic) symbol $\left(\frac{P}{Q}\right)$ is defined only for odd Q by the recurrent formula:

$$\left(\frac{P}{Q}\right) = \prod_{i=1}^s \left(\frac{P}{q_i}\right),$$

where $Q = q_1 q_2 \dots q_s$ is the prime decomposition of Q , and for prime p the quadratic symbol (also called the Legendre symbol in this setting) is given by:

$$\left(\frac{P}{p}\right) = \begin{cases} 1, & \text{if } P = x^2(\text{mod } p), \\ -1, & \text{otherwise.} \end{cases}$$

The quadratic symbol verifies the following reciprocity law

$$\left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2} \frac{Q-1}{2}},$$

in the case when both P and Q are odd.

Denote by $\omega = \frac{1}{2}G(1, 2k)$. The lift of the chain relation is of the form:

$$(R_a R_b R_c)^4 = \mu R_e R_d,$$

with $\mu \in U(1)$. Our aim now is to compute the value of μ . Set $X = R_a R_b R_c$, $Y = X^2$ and $Z = X^4$. We have then:

$$X_{m,n} = k^{-1} \omega \delta_{n_2, m_2} q^{-(n_1 - m_1)^2 + m_1^2 + (n_1 + n_2)^2}.$$

This implies $Y_{m,n} = 0$ if $\delta_{m_2,n_2} = 0$. If $m_2 = n_2$ then:

$$\begin{aligned} Y_{m,n} &= k^{-2}\omega^2 \sum_{r_1 \in \mathbb{Z}/k\mathbb{Z}} q^{-(m_1-r_1)^2+m_1^2+(r_1+n_2)^2-(n_1-r_1)^2+r_1^2+(n_1+n_2)^2} = \\ &= k^{-2}\omega^2 \sum_{r_1 \in \mathbb{Z}/k\mathbb{Z}} q^{m_2^2+n_2^2+2n_1n_2+2r_1(m_1+m_2+n_1)}. \end{aligned}$$

Therefore $Y_{m,n} = 0$, unless $m_1 + m_2 + n_1 = 0$. Assume that $m_1 + m_2 + n_1 = 0$. Then:

$$Y_{m,n} = k^{-1}\omega^2 q^{m_2^2+n_2^2+2n_1n_2} = k^{-1}\omega^2 q^{-2m_1m_2}.$$

It follows that: $Z_{m,n} = \sum_{r \in (\mathbb{Z}/k\mathbb{Z})^2} Y_{m,r} Y_{r,n}$ vanishes, except when $m_2 = r_2 = n_2$ and $r_1 = -(m_1 + m_2)$, $n_1 = -(r_1 + r_2) = m_1$. Thus Z is a diagonal matrix. If $m = n$ then:

$$Z_{m,n} = k^{-2}\omega^4 Y_{m,r} Y_{r,n} = k^{-2}\omega^4 q^{-2m_1m_2-2r_1r_2} = k^{-2}\omega^4 q^{m_2^2}.$$

We have therefore obtained:

$$(R_a R_b R_c)^4 = k^{-2}\omega^4 T_e^2$$

and thus $\mu = k^{-2}\omega^4 = \left(\frac{G(1,2k)}{2k}\right)^4$. This proves that whenever k is even we have $\mu = -1$. Since this computes the action of the central element z , it follows that $z \neq 1$. \square

Finally we show:

Proof of Lemma 2.13. We know that R_b is $S^3 R_a S$, where S is the S -matrix, up to an eight root of unity. The normalization of this root of unity is given by the braid relation:

$$R_a R_b R_a = R_b R_a R_b$$

We have therefore:

$$(R_b)_{m,n} = k^{-2} \sum_{x \in (\mathbb{Z}/k\mathbb{Z})^2} q^{\langle L_a x, x \rangle + 2\langle n - m, x \rangle}$$

This entry vanishes except when $m_2 = n_2$. Assume that $n_2 = m_2$. Then:

$$(R_b)_{m,n} = k^{-1} \sum_{x_1 \in \mathbb{Z}/k\mathbb{Z}} q^{x_1^2 + 2(n_1 - m_1)x_1} = k^{-1} q^{(n_1 - m_1)^2} \sum_{x_1 \in \mathbb{Z}/k\mathbb{Z}} q^{(x_1 + n_1 - m_1)^2} = k^{-1} q^{(n_1 - m_1)^2} \omega$$

where $\omega = \frac{1}{2} \sum_{x \in \mathbb{Z}/2k\mathbb{Z}} q^{x^2}$ is a Gauss sum. We have first:

$$(R_a R_b R_a)_{m,n} = k^{-1} \omega \delta_{m_2,n_2} q^{-(n_1-m_1)^2+m_1^2+n_1^2} = k^{-1} \omega \delta_{m_2,n_2} q^{2n_1m_1}$$

Further

$$(R_b R_a)_{m,n} = k^{-1} \omega \delta_{m_2,n_2} q^{-(n_1-m_1)^2+n_1^2}$$

so that:

$$\begin{aligned} (R_b R_a R_b)_{m,n} &= k^{-2} \omega^2 \sum_{r \in (\mathbb{Z}/k\mathbb{Z})^2} \delta_{m_2,r_2} \delta_{n_2,r_2} q^{-(n_1-r_1)^2+r_1^2-(r_1-n_1)^2} = \\ &= k^{-1} \omega^2 \delta_{m_2,n_2} q^{2m_1n_1} \sum_{r_1 \in \mathbb{Z}/k\mathbb{Z}} q^{-(r_1-m_1+n_1)^2} = k^{-1} \omega \delta_{m_2,n_2} q^{2n_1m_1} \end{aligned}$$

Similar computations hold for the other pairs of non-commuting matrices in the set R_b, R_c, R_f, R_e . This ends the proof of Lemma 2.13. \square

2.5 Third proof: K -theory computation of $H_2(Sp(2g, \mathbb{Z}/4\mathbb{Z}))$

We give below one more proof using slightly more sophisticated tools which were developed by Barge and Lannes in [2], which allow us to dispose of Deligne's theorem. According to Stein's stability theorem ([65]) it is enough to prove that $H_2(Sp(2g, \mathbb{Z}/4\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z}$, for g large. It is well-known that the second homology of the linear and symplectic groups can be interpreted in terms of the K -theory group K_2 . Denote by $K_1(\mathfrak{A})$, $K_2(\mathfrak{A})$ and $KSp_1(\mathfrak{A})$, $KSp_2(\mathfrak{A})$ the groups of algebraic K -theory of the stable linear groups and symplectic groups over the commutative ring \mathfrak{A} , respectively. See [32] for definitions. Our claim is equivalent to the fact that $KSp_2(\mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$.

Our key ingredient is the exact sequence from ([2], Thm. 5.4.1) which is a generalization of Sharpe's exact sequence (see [32], Thm. 5.6.7) in K -theory:

$$K_2(\mathbb{Z}/4\mathbb{Z}) \rightarrow KSp_2(\mathbb{Z}/4\mathbb{Z}) \rightarrow V(\mathbb{Z}/4\mathbb{Z}) \rightarrow K_1(\mathbb{Z}/4\mathbb{Z}) \rightarrow 1. \quad (13)$$

We first show:

Lemma 2.14. *The homomorphism $K_2(\mathbb{Z}/4\mathbb{Z}) \rightarrow KSp_2(\mathbb{Z}/4\mathbb{Z})$ is trivial.*

Proof of Lemma 2.14. Recall from [2] that this homomorphism is induced by the hyperbolization inclusion $GL(g, \mathbb{Z}/4\mathbb{Z}) \rightarrow Sp(2g, \mathbb{Z}/4\mathbb{Z})$, which sends the matrix A to $A \oplus (A^{-1})^\top$. Therefore it would suffice to show that the pull-back of the universal central extension over $Sp(2g, \mathbb{Z}/4\mathbb{Z})$ by the hyperbolization morphism $SL(g, \mathbb{Z}/4\mathbb{Z}) \rightarrow Sp(2g, \mathbb{Z}/4\mathbb{Z})$ is trivial.

Suppose that we have a central extension by $\mathbb{Z}/2\mathbb{Z}$ over $Sp(2g, \mathbb{Z}/4\mathbb{Z})$. It defines therefore a class in $H^2(Sp(2g, \mathbb{Z}/4\mathbb{Z}); \mathbb{Z}/2\mathbb{Z})$. We want to show that the image of the hyperbolization homomorphism

$$h : H^2(Sp(2g, \mathbb{Z}/4\mathbb{Z}); \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(SL(g, \mathbb{Z}/4\mathbb{Z}); \mathbb{Z}/2\mathbb{Z})$$

is trivial, when $g \geq 3$.

Since these groups are perfect we have the following isomorphisms coming from the universal coefficient theorem:

$$\begin{aligned} H^2(Sp(2g, \mathbb{Z}/4\mathbb{Z}); \mathbb{Z}/2\mathbb{Z}) &\cong \text{Hom}(H_2(Sp(2g, \mathbb{Z}/4\mathbb{Z})), \mathbb{Z}/2\mathbb{Z}), \\ H^2(SL(g, \mathbb{Z}/4\mathbb{Z}); \mathbb{Z}/2\mathbb{Z}) &\cong \text{Hom}(H_2(SL(g, \mathbb{Z}/4\mathbb{Z})), \mathbb{Z}/2\mathbb{Z}). \end{aligned}$$

We proved in section 3.4.2 above that the obvious homomorphism $H_2(Sp(2g, \mathbb{Z})) \rightarrow H_2(Sp(2g, \mathbb{Z}/4\mathbb{Z}))$ is surjective. This implies that the dual map $H^2(Sp(2g, \mathbb{Z}/4\mathbb{Z}); \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(Sp(2g, \mathbb{Z}); \mathbb{Z}/2\mathbb{Z})$ is injective.

In the case of SL we can use the same arguments to prove surjectivity. Anyway it is known (see [61]) that $H_2(SL(g, \mathbb{Z})) \rightarrow H_2(SL(g, \mathbb{Z}/4\mathbb{Z}))$ is an isomorphism and that both groups are isomorphic to $\mathbb{Z}/2\mathbb{Z}$, when $g \geq 3$. This shows that $H^2(SL(g, \mathbb{Z}/4\mathbb{Z}); \mathbb{Z}/2\mathbb{Z}) \rightarrow H^2(SL(g, \mathbb{Z}); \mathbb{Z}/2\mathbb{Z})$ is injective.

Now, we have a commutative diagram:

$$\begin{array}{ccc} H^2(Sp(2g, \mathbb{Z}/4\mathbb{Z}); \mathbb{Z}/2\mathbb{Z}) & \hookrightarrow & H^2(Sp(2g, \mathbb{Z}); \mathbb{Z}/2\mathbb{Z}) \\ h \downarrow & & \downarrow H \\ H^2(SL(g, \mathbb{Z}/4\mathbb{Z}); \mathbb{Z}/2\mathbb{Z}) & \hookrightarrow & H^2(SL(g, \mathbb{Z}); \mathbb{Z}/2\mathbb{Z}) \end{array} \quad (14)$$

The vertical arrow H on the right side is the hyperbolization homomorphism induced by the hyperbolization inclusion $SL(g, \mathbb{Z}) \rightarrow Sp(2g, \mathbb{Z})$. We know that $H^2(Sp(2g, \mathbb{Z}); \mathbb{Z}/2\mathbb{Z})$ is generated by the mod 2 Maslov class. But the restriction of the Maslov cocycle to the subgroup $SL(g, \mathbb{Z})$ is trivial because $SL(g, \mathbb{Z})$ fixes the standard direct sum decomposition of \mathbb{Z}^{2g} in two Lagrangian subspaces. This proves that H is zero. Since the horizontal arrows are injective it follows that h is the zero homomorphism.

An alternative argument is as follows. The hyperbolization homomorphism $H : K_2(\mathbb{Z}/4\mathbb{Z}) \rightarrow KSp_2(\mathbb{Z}/4\mathbb{Z})$ sends the Dennis-Stein symbol $\{r, s\}$ to the Dennis-Stein symplectic symbol $[r^2, s]$, see e.g. ([68], section 6). According to [65] the group $K_2(\mathbb{Z}/4\mathbb{Z})$ is generated by $\{-1, -1\}$ and thus its image by H is generated by $[1, -1] = 0$. \square

It is known that:

$$K_1(\mathbb{Z}/4\mathbb{Z}) = (\mathbb{Z}/4\mathbb{Z})^* = \mathbb{Z}/2\mathbb{Z}, \quad (15)$$

and the problem is to compute the discriminant map $V(\mathbb{Z}/4\mathbb{Z}) \rightarrow \mathbb{Z}/2\mathbb{Z}$.

For an arbitrary ring R , the group $V(R)$ for a ring R is defined as follows (see [2, Section 4.5.1]). Consider the set of triples $(L; q_0, q_1)$, where L is a free R -module of finite rank and q_0 and q_1 are non-degenerate symmetric bilinear forms. Two such triples $(L; q_0, q_1)$ and $(L'; q'_0, q'_1)$ are equivalent, if there exists an R -linear isomorphism $a : L \rightarrow L'$ such that $a^* \circ q'_0 \circ a = q_0$ and $a^* \circ q'_1 \circ a = q_1$. Under direct sum this triples form a monoid. The group $V(R)$ is by definition the quotient of the associated Grothendieck-Witt group by the subgroup generated by Chasles' relations, that is the subgroup generated by the elements of the form:

$$[L; q_0, q_1] + [L; q_1, q_2] - [L; q_0, q_2].$$

There is a canonical map from $V(R)$ to the Grothendieck-Witt group of symmetric non-degenerate bilinear forms over free modules that sends $[L; q_0, q_1]$ to $q_1 - q_0$. Since $\mathbb{Z}/4$ is a local ring, we know that $SK_1(\mathbb{Z}/4\mathbb{Z}) = 1$ and hence by [2, Corollary 4.5.1.5] we have a pull-back square of abelian groups:

$$\begin{array}{ccc} V(\mathbb{Z}/4\mathbb{Z}) & \longrightarrow & I(\mathbb{Z}/4\mathbb{Z}) \\ \downarrow & & \downarrow \\ (\mathbb{Z}/4\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/4\mathbb{Z})^*/((\mathbb{Z}/4\mathbb{Z})^*)^2, \end{array}$$

where $I(\mathbb{Z})$ is the augmentation ideal of the Grothendieck-Witt ring of $\mathbb{Z}/4\mathbb{Z}$. The structure of the groups of units in $\mathbb{Z}/4\mathbb{Z}$ is well-known, and the bottom arrow in the square is then an isomorphism $\mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$, so $V(\mathbb{Z}/4\mathbb{Z}) \simeq I(\mathbb{Z}/4\mathbb{Z})$ and the kernel of $V(\mathbb{Z}/4\mathbb{Z}) \rightarrow (\mathbb{Z}/4\mathbb{Z})^* \simeq K_1(\mathbb{Z}/4\mathbb{Z})$ is the kernel of the discriminant homomorphism $I(\mathbb{Z}/4\mathbb{Z}) \rightarrow (\mathbb{Z}/4\mathbb{Z})^*/((\mathbb{Z}/4\mathbb{Z})^*)^2$. To compute $V(\mathbb{Z}/4\mathbb{Z})$ is therefore enough to compute the Witt ring $W(\mathbb{Z}/4\mathbb{Z})$. Recall that this is the quotient of the monoid of symmetric non-degenerate bilinear forms over finitely generated projective modules modulo the sub-monoid of *split* forms. A bilinear form is split if the underlying free module contains a direct summand N such that $N = N^\perp$. Since, by a classical result of Kaplansky, finitely generated projective modules over $\mathbb{Z}/4\mathbb{Z}$ are free by [53, Lemma 6.3] any split form can be written in matrix form as:

$$\begin{pmatrix} 0 & I \\ I & A \end{pmatrix},$$

for some symmetric matrix A . Isotropic submodules form an inductive system, and therefore any isotropic submodule is contained in a maximal one and these have all the same rank, in case of a split form this rank is necessarily half of the rank of the underlying free module, which is therefore even. The main difficulty in the following computation is due to the fact that as 2 is not a unit in $\mathbb{Z}/4\mathbb{Z}$, so that the classical Witt cancellation lemma is not true. As usual, for any invertible element u of $\mathbb{Z}/4\mathbb{Z}$ we denote by $\langle u \rangle$ the non-degenerate symmetric bilinear form on $\mathbb{Z}/4\mathbb{Z}$ of determinant u .

Proposition 2.7. *The Witt ring $W(\mathbb{Z}/4\mathbb{Z})$ is isomorphic to $\mathbb{Z}/8\mathbb{Z}$, and it is generated by the class of $\langle -1 \rangle$.*

The computation of $W(\mathbb{Z}/4\mathbb{Z})$ was obtained independently by Gurevich and Hadani in [26].

The discriminant of $\omega = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ is 1 and in the proof of Proposition 2.7 below we show that its class

is non-trivial in $W(\mathbb{Z}/4\mathbb{Z})$ and hence it represents a non-trivial element in the kernel of the discriminant map $I(\mathbb{Z}/4\mathbb{Z}) \rightarrow (\mathbb{Z}/4\mathbb{Z})^*/(\mathbb{Z}/4\mathbb{Z})^{*2}$. From the Cartesian diagram above we get that it also represents a non-trivial element in the kernel of leftmost vertical homomorphism $V(\mathbb{Z}/4\mathbb{Z}) \rightarrow K_1(\mathbb{Z}/4\mathbb{Z})$. In particular $KSp_2(\mathbb{Z}/4\mathbb{Z})$ is $\mathbb{Z}/2\mathbb{Z}$.

Proof of Proposition 2.7. Thus given a free $\mathbb{Z}/4\mathbb{Z}$ -module L , any non-degenerate symmetric bilinear form on L is an orthogonal sum of copies of $\langle 1 \rangle$, of $\langle -1 \rangle$ and of a bilinear form β on a free summand N such that for all $x \in N$ we have $\beta(x, x) \in \{0, 2\}$. Fix a basis e_1, \dots, e_n of N . Let B denote the matrix of β in this basis. Expanding the determinant of β along the first column we see that there must be an index $i \geq 2$ such that $\beta(e_1, e_i) = \pm 1$, for otherwise the determinant would not be invertible. Without loss of generality we may assume that $i = 2$ and that $\beta(e_1, e_2) = 1$. Replacing if necessary e_j for $j \geq 3$ by $e_j - \frac{\beta(e_1, e_j)}{\beta(e_1, e_2)}e_2$, we may assume that B is of the form:

$$\begin{pmatrix} 2 & 1 & 0 \\ 1 & a & c \\ 0 & t_c & A \end{pmatrix}$$

where A and c are a square matrix and a row matrix respectively, of the appropriate sizes, and $a \in \{0, 2\}$. But then β restricted to the submodule generated by e_1, e_2 defines a non-singular symmetric bilinear form and therefore $N = \langle e_1, e_2 \rangle \oplus \langle e_1, e_2 \rangle^\perp$, where on the first summand the bilinear form is either split or ω . By induction we have that any symmetric bilinear form is an orthogonal sum of copies of $\langle 1 \rangle, \langle -1 \rangle$, of

$$\omega = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

and split spaces.

It's a classical fact (see [53, Chapter I]) that in $W(\mathbb{Z}/4\mathbb{Z})$ one has $\langle 1 \rangle = -\langle -1 \rangle$. Also $\langle -1 \rangle \oplus \langle -1 \rangle \oplus \langle -1 \rangle \oplus \langle -1 \rangle$ is isometric to $\omega \oplus \langle -1 \rangle \oplus \langle 1 \rangle$. To see this notice that, if e_1, \dots, e_4 denotes the preferred basis for the former bilinear form, then the matrix in the basis $e_1 + e_2, e_1 + e_3, e_1 - e_2 - e_3, e_4$ is precisely $\omega \oplus \langle -1 \rangle \oplus \langle 1 \rangle$. Also, in the Witt ring $\langle 1 \rangle \oplus \langle -1 \rangle = 0$, so $4\langle -1 \rangle = \omega$, and a direct computation shows that $\omega = -\omega$, in particular ω has order at most 2. All these show that $W(\mathbb{Z}/4\mathbb{Z})$ is generated by $\langle -1 \rangle$ and that this form is of order at most 8. It remains to show that ω is a non-trivial element to finish the proof.

Assume the contrary, namely that there is a split form σ such that $\omega \oplus \sigma$ is split. We denote by A the underlying module of ω and by $\{a, b\}$ its preferred basis. Similarly, we denote by S the underlying space of σ of dimension $2n$ and by $\{e_1, \dots, e_n, f_1, \dots, f_n\}$ a basis that exhibits it as a split form. By construction e_1, \dots, e_n generate a totally isotropic submodule E of rank n in $A \oplus S$, and since it is included into a maximal isotropic submodule, we can adjoin to it a new element v such that v, e_1, \dots, e_n is a totally isotropic submodule of $A \oplus S$, and hence has rank $n+1$. By definition there are unique elements $x, y \in \mathbb{Z}/4\mathbb{Z}$ and elements $\varepsilon \in E$ and $\phi \in F$ such that $v = xa + yb + \varepsilon + \phi$. Since v is isotropic we have:

$$2x^2 + 2xy + 2y^2 + \sigma(\varepsilon, \phi) + \sigma(\phi, \phi) \equiv 0 \pmod{4}.$$

Since $E \oplus \mathbb{Z}/4\mathbb{Z}v$ is totally isotropic, then $\sigma(e_i, v) = \sigma(e_i, \phi) = 0$, for every $1 \leq i \leq n$. In particular, since ϕ belongs to the dual module to E with respect to σ , $\phi = 0$, so the above equation implies:

$$2x^2 + 2xy + 2y^2 \equiv 0 \pmod{4}.$$

But now this can only happen when x and y are multiples of 2 in $\mathbb{Z}/4\mathbb{Z}$. Therefore reducing mod 2, we find that $v \pmod{2}$ belongs to the $\mathbb{Z}/2\mathbb{Z}$ -vector space generated by the mod 2 reduction of the elements e_1, \dots, e_n , and by Nakayama's lemma this contradicts the fact that the $\mathbb{Z}/4\mathbb{Z}$ -module generated by v, e_1, \dots, e_n has rank $n+1$. \square

Remark 2.2. Dennis and Stein proved in [14] that $K_2(\mathbb{Z}/2^k\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ for any $k \geq 2$. If we had proved directly that the class of the symmetric bilinear form $\begin{pmatrix} 2^{k-1} & 1 \\ 1 & 2^{k-1} \end{pmatrix}$ generates the kernel of the homomorphism $I(\mathbb{Z}/2^k\mathbb{Z}) \rightarrow (\mathbb{Z}/2^k\mathbb{Z})^*/(\mathbb{Z}/2^k\mathbb{Z})^{*2}$, which is of order two for all $k \geq 2$, then the Sharpe-type exact sequence of Barge and Lannes would yield $KSp_2(\mathbb{Z}/2^k\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$, for any $k \geq 2$. This would permit us to dispose of Stein's stability results. However the description of the Witt group $W^f(\mathbb{Z}/2^k\mathbb{Z})$ seems more involved for $k \geq 3$ and it seems more cumbersome than worthy to fill in all the details.

3 Residual finiteness, finite quotients and their second homology

3.1 Residual finiteness for perfect groups

Perfect groups have a universal central extension with kernel canonically isomorphic to their second integral homology group. In this section we show how to translate the residual finiteness problem for the universal central extension for a perfect group Γ into an homological problem about $H_2(\Gamma)$.

Proposition 3.1. *Let Γ be a finitely generated perfect group and $\tilde{\Gamma}$ be its universal central extension. We denote by C the center $\ker(\tilde{\Gamma} \rightarrow \Gamma)$ of $\tilde{\Gamma}$.*

1. *Suppose that the finite index (normal) subgroup $H \subset \Gamma$ has the property that the image of $H_2(H)$ into $H_2(\Gamma)$ contains dC , for some $d \in \mathbb{Z}$. Let $F = \Gamma/H$ be the corresponding finite quotient of Γ and $p : \Gamma \rightarrow F$ the quotient map. Then $d \cdot p_*(H_2(\Gamma)) = 0$, where $p_* : H_2(\Gamma) \rightarrow H_2(F)$ is the homomorphism induced by p . In particular, if $p_* : H_2(\Gamma) \rightarrow H_2(F)$ is surjective, then $d \cdot H_2(F) = 0$.*

2. Assume that F is a finite quotient of Γ satisfying $d \cdot p_*(H_2(\Gamma)) = 0$. For instance, this is satisfied when $d \cdot H_2(F) = 0$. Let \tilde{F} denote the universal central extension of F . Then the homomorphism $p : \Gamma \rightarrow F$ has a unique lift $\tilde{p} : \tilde{\Gamma} \rightarrow \tilde{F}$ and the kernel of \tilde{p} contains $d \cdot C$. Observe that since F is finite, $H_2(F)$ is also finite, hence in the second item of this proposition we can take $d = |H_2(F)|$.

Proof. The image of H into F is trivial and thus the image of $H_2(H)$ into $H_2(F)$ is trivial. This implies that $p_*(d \cdot H_2(\Gamma)) = 0$, which proves the first part of Proposition 3.1.

By Lemma 2.2 there exists an unique lift $\tilde{p} : \tilde{\Gamma} \rightarrow \tilde{F}$. If $d \cdot p_*(H_2(\Gamma)) = 0$ then Lemma 2.2 yields $d \cdot \tilde{p}(c) = d \cdot p_*(c) = 0$, for any $c \in C$. This settles the second part of Proposition 3.1. \square

Remark 3.1. It might be possible that the $d' \cdot p_*(H_2(\Gamma)) = 0$, for some proper divisor d' of d , so the first part of the proposition 3.1 can only give an upper bound of the orders of the image of the second cohomology, as in proposition 1.3. In order to find lower bounds we need additional information concerning the finite quotients F .

3.2 Proof of Theorem 1.3

Let \mathbb{K} be a *number field*, \mathcal{R} be the set of inequivalent valuations of \mathbb{K} and $S \subset \mathcal{R}$ be a finite set of valuations of \mathbb{K} including all the Archimedean (infinite) ones. Let

$$O(S) = \{x \in \mathbb{K} : v(x) \leq 1, \text{ for all } v \in \mathcal{R} \setminus S\}$$

be the ring of S -integers in \mathbb{K} and $\mathfrak{q} \subset O(S)$ be a nonzero ideal. By \mathbb{K}_v we denote the completion of \mathbb{K} with respect to $v \in \mathcal{R}$. Following [3], we call a domain \mathfrak{A} which arises as $O(S)$ above will be called a *Dedekind domain of arithmetic type*.

Let $\mathfrak{A} = O_S$ be a Dedekind domain of arithmetic type and \mathfrak{q} be an ideal of \mathfrak{A} . Denote by $Sp(2g, \mathfrak{A}, \mathfrak{q})$ the kernel of the surjective homomorphism $p : Sp(2g, \mathfrak{A}) \rightarrow Sp(2g, \mathfrak{A}/\mathfrak{q})$. The surjectivity is not a purely formal fact and follows from the fact that in these cases the symplectic group coincides with the so-called "elementary symplectic group", and that it is trivial to lift elementary generators of $Sp(2g, \mathfrak{A}/\mathfrak{q})$ to $Sp(2g, \mathfrak{A})$, for a proof of this fact when $\mathfrak{A} = \mathbb{Z}$ see ([32], Thm. 9.2.5).

Consider the central extension of $Sp(2g, \mathfrak{A})$ constructed by Deligne in [12], as follows. Let μ (respectively μ_v for a non-complex place v) be the group of roots of unity in \mathbb{K} (and respectively \mathbb{K}_v). By convention one sets $\mu_v = 1$ for a complex place v . Set also $\widetilde{Sp(2g)_S} = \prod_{v \in S} Sp(2g, \mathbb{K}_v)$ and recall that $Sp(2g, \mathfrak{A})$ is an open subgroup of $\widetilde{Sp(2g)_S}$. Denote then by $\widetilde{Sp(2g, \mathfrak{A})}$ the inverse image of $Sp(2g, \mathfrak{A})$ in the universal covering $\widetilde{Sp(2g)_S}$ of $Sp(2g)_S$. Then $\widetilde{Sp(2g, \mathfrak{A})}$ is a central extension of $Sp(2g, \mathfrak{A})$ which fits in an exact sequence:

$$1 \rightarrow \prod_{v \in S} \pi_1(Sp(2g, \mathbb{K}_v)) \rightarrow \widetilde{Sp(2g, \mathfrak{A})} \rightarrow Sp(2g, \mathfrak{A}) \rightarrow 1. \quad (16)$$

There is a natural surjective homomorphism $\pi_1(Sp(2g, \mathbb{K}_v)) \rightarrow \mu_v$. When composed with the map $\mu_v \rightarrow \mu$ sending x to $x^{[\mu_v : \mu]}$ we obtain a homomorphism:

$$R_S : \prod_{v \in S} \pi_1(Sp(2g, \mathbb{K}_v)) \rightarrow \mu. \quad (17)$$

Then Proposition 3.4 below in the case $\mathfrak{A} = \mathbb{Z}$ has the following (less precise) extension for arbitrary \mathfrak{A} :

Proposition 3.2. *The following statements are equivalent:*

1. Any finite index subgroup of the Deligne central extension $\widetilde{Sp(2g, \mathfrak{A})}$, for $g \geq 3$, contains $\ker R$ for some homomorphism $R : \prod_{v \in S} \pi_1(Sp(2g, \mathbb{K}_v)) \rightarrow \nu$, where ν is a finite group.
2. For fixed \mathfrak{A} and $g \geq 3$ there exists some uniform bound for the size of the finite torsion groups $H_2(Sp(2g, \mathfrak{A}/\mathfrak{q}))$, for any nontrivial ideal \mathfrak{q} of \mathfrak{A} .

Proof. Although the Deligne central extension is not in general the universal central extension, it is not far from it. We have indeed the following result:

Lemma 3.1. *We have:*

$$H_2(Sp(2g, \mathfrak{A}); \mathbb{R}) = \mathbb{R} \otimes_{\mathbb{Z}} \prod_{v \in S \cap \mathbb{R}(S)} \pi_1(Sp(2g, \mathbb{K}_v)),$$

where $\mathbb{R}(S)$ denotes the real Archimedean places in S .

Proof. In the case where \mathfrak{A} is the ring of integers of a number field this is basically the result of Borel computing the stable cohomology of arithmetic groups (see [5], p.276). For the general case see [6, 7]. \square

The second step is the following general statement:

Lemma 3.2. *The group $H_2(Sp(2g, \mathfrak{A}))$ is finitely generated.*

Proof. This also follows from the existence of the Borel-Serre compactification ([6]) associated to an arithmetic group. \square

Consequently the free part of $H_2(Sp(2g, \mathfrak{A}))$ is the abelian group $\prod_{v \in S \cap \mathbb{R}(S)} \pi_1(Sp(2g, \mathbb{K}_v))$ and the torsion part $\text{Tors}(H_2(Sp(2g, \mathfrak{A})))$ is a finite group. Moreover, the Deligne central extension $\widetilde{Sp(2g, \mathfrak{A})}$ is a subgroup of the universal central extension of $Sp(2g, \mathfrak{A})$ whose kernel is the free part of $H_2(Sp(2g, \mathfrak{A}))$.

Assume now that the Deligne central extension has the property from the first statement. Thus there exists $k(\mathfrak{A}) \in \mathbb{Z} \setminus \{0\}$ such that $f(k(\mathfrak{A}) \cdot c) = 1$, for any $c \in \prod_{v \in S} \pi_1(Sp(2g, \mathbb{K}_v))$ and any homomorphism $f : \widetilde{Sp(2g, \mathfrak{A})} \rightarrow F$ to a finite group F . Since $\text{Tors}(H_2(Sp(2g, \mathfrak{A})))$ is finite we can choose $k(\mathfrak{A})$ such that, additionally, we have $k(\mathfrak{A}) \cdot c = 0$, for any $c \in \text{Tors}(H_2(Sp(2g, \mathfrak{A})))$.

We need now the following technical result:

Proposition 3.3. *Given an ideal $\mathfrak{q} \in \mathfrak{A}$, for any $g \geq 3$, the homomorphism $p_* : H_2(Sp(2g, \mathfrak{A})) \rightarrow H_2(Sp(2g, \mathfrak{A}/\mathfrak{q}))$ is surjective.*

The proof will be postponed until section 3.4.

From above we have $p_*(k(\mathfrak{A}) \cdot c) = 0$, for every $c \in H_2(Sp(2g, \mathfrak{A}))$. Assuming the surjectivity of p_* we obtain that $k(\mathfrak{A}) \cdot H_2(Sp(2g, \mathfrak{A}/\mathfrak{q})) = 0$, for every ideal \mathfrak{q} . Since all groups $H_2(Sp(2g, \mathfrak{A}/\mathfrak{q}))$ are covered by the finitely generated abelian group $H_2(Sp(2g, \mathfrak{A}))$ we derive that they are torsion groups of uniformly bounded size.

Conversely, assume that there exists some $k(\mathfrak{A}) \in \mathbb{Z} \setminus \{0\}$ such that $k(\mathfrak{A}) \cdot H_2(Sp(2g, \mathfrak{A}/\mathfrak{q})) = 0$, for every ideal $\mathfrak{q} \subset \mathfrak{A}$. Then the surjectivity of p_* implies that $p_*(k(\mathfrak{A}) \cdot c) = 0$, for every ideal \mathfrak{q} .

This implies that $f_*(|\mu| \cdot k(\mathfrak{A}) \cdot c) = 0$, for every morphism $f : Sp(2g, \mathfrak{A}) \rightarrow F$ to a finite group, where $|\mu|$ is the cardinal of the finite group μ . In fact by results of [3] the congruence subgroup kernel is the finite cyclic group μ when \mathbb{K} is totally imaginary (i.e. it has no non-complex places) and is trivial if \mathbb{K} has at least one non-complex place. This means that for any finite index normal subgroup H (e.g. $\ker f$) there exists an elementary subgroup $ESp(2g, \mathfrak{A}, \mathfrak{q})$ contained in H , where $ESp(2g, \mathfrak{A}, \mathfrak{q}) \subset Sp(2g, \mathfrak{A}, \mathfrak{q})$ is a normal subgroup of finite index dividing $|\mu|$. Therefore $f(x)$ factors through the quotient $Sp(2g, \mathfrak{A})/ESp(2g, \mathfrak{A}, \mathfrak{q})$ and the composition $f(|\mu| \cdot x)$ factors through $Sp(2g, \mathfrak{A}/\mathfrak{q})$. Since $H_2(Sp(2g, \mathfrak{A}/\mathfrak{q}))$ is $k(\mathfrak{A})$ -torsion we obtain $f_*(|\mu| \cdot k(\mathfrak{A}) \cdot c) = 0$, as claimed.

In particular we can apply this equality to the morphism f between the universal central extensions of $Sp(2g, \mathfrak{A})$ and F . Then the restriction of f_* to the free part of $H_2(Sp(2g, \mathfrak{A}))$ is then trivial on multiples of $|\mu| \cdot k(\mathfrak{A})$. Thus these multiple elements lie in the kernel of any homomorphism of $\widetilde{Sp(2g, \mathfrak{A})}$ into a finite group. This proves Proposition 3.2. \square

End of proof of Theorem 1.3. Deligne's result from [12] yields an effective uniform bound for the size of the torsion group of $H_2(Sp(2g, \mathfrak{A}/\mathfrak{q}))$, since the first statement of Proposition 3.2 holds for $R = R_S$. \square

3.3 Proof of Theorem 1.2

We now specialize to the case $\mathfrak{A} = \mathbb{Z}$. The proof of Proposition 2.1 used Deligne's theorem. Conversely we have:

Proposition 3.4. *Assume that for any $D \geq 2$, $g \geq 4$ we have $\widetilde{H}_2(Sp(2g, \mathbb{Z}/D\mathbb{Z})) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$. Then any finite index subgroup of the universal central extension $\widetilde{Sp}(2g, \mathbb{Z})$, for $g \geq 4$, contains $2\mathbb{Z}$, where \mathbb{Z} is the central kernel $\ker(\widetilde{Sp}(2g, \mathbb{Z}) \rightarrow Sp(2g, \mathbb{Z}))$.*

Proof. Consider an arbitrary surjective homomorphism $\widehat{q} : \widetilde{Sp}(2g, \mathbb{Z}) \rightarrow \widehat{F}$ onto some finite group \widehat{F} . We set $F = \widehat{F}/q(C)$. Then there is an induced homomorphism $q : \widetilde{Sp}(2g, \mathbb{Z}) \rightarrow F$. Since F is finite the congruence subgroup property for the symplectic groups (see [3, 49, 50]) implies that there is some D such that q factors as $s \circ p$, where $p : \widetilde{Sp}(2g, \mathbb{Z}) \rightarrow Sp(2g, \mathbb{Z}/D\mathbb{Z})$ is the reduction mod D and $s : Sp(2g, \mathbb{Z}/D\mathbb{Z}) \rightarrow F$ is a surjective homomorphism.

Since F is perfect it has an universal central extension \widetilde{F} . There exists then an unique lift $\widetilde{s} : \widetilde{Sp}(2g, \mathbb{Z}/D\mathbb{Z}) \rightarrow \widetilde{F}$ of the homomorphism s , such that $\widetilde{q} = \widetilde{s} \circ \widetilde{p}$. Since \widetilde{F} is universal there is a unique homomorphism $\theta : \widetilde{F} \rightarrow \widehat{F}$ which lifts the identity of F . We claim that $\theta \circ \widetilde{q} = \widehat{q}$. Both homomorphisms are lifts of q and $\widetilde{q} = \widetilde{s} \circ \widetilde{p}$, by the uniqueness claim of Lemma 2.2. Thus $\theta \circ \widetilde{q} = \alpha \circ \widehat{q}$, where α is a homomorphism on $\widetilde{Sp}(2g, \mathbb{Z})$ with target $\ker(\widehat{F} \rightarrow F)$, which is central in \widehat{F} . Since $\widetilde{Sp}(2g, \mathbb{Z})$ is universal we have $H_1(\widetilde{Sp}(2g, \mathbb{Z})) = 0$ and thus α is trivial, as claimed. Eventually, we have $\widehat{q} = \theta \circ \widetilde{q} = \theta \circ \widetilde{s} \circ \widetilde{p}$.

Furthermore, using $H_2(Sp(2g, \mathbb{Z}/D\mathbb{Z})) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$ and Lemma 2.2 we obtain $\widetilde{p}(2c) = 2 \cdot p_*(c) = 0$, where c is the generator of $H_2(Sp(2g, \mathbb{Z}))$. In particular, $2 \cdot \widehat{q}(c) = 0 \in \widehat{F}$, as claimed. \square

Remark 3.2. Using the results in [9, 10] we can obtain that $H_2(Sp(4, \mathbb{Z}/D\mathbb{Z})) = 0$, if $D \neq 2$ is prime and $H_2(Sp(4, \mathbb{Z}/2\mathbb{Z})) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Notice that $Sp(4, \mathbb{Z}/2\mathbb{Z})$ is not perfect, but the extension $\widetilde{Sp}(4, \mathbb{Z})$ still makes sense.

End of proof of Theorem 1.2. Theorem 1.1 and the second part of Proposition 3.4 imply Deligne's theorem, namely the first part of Proposition 3.4. Notice that the third proof of Theorem 1.1 did not use Deligne's theorem and one can extract an independent proof also from the first two. Further the first proof of Theorem 1.1 precisely provides a surjective homomorphism of the universal central extension $\widetilde{Sp}(2g, \mathbb{Z})$ onto a non-trivial central extension of $Sp(2g, 8\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$. Alternatively, Proposition 3.3 and Lemma 2.2 provide such a surjective homomorphism onto the universal central extension of $Sp(2g, D\mathbb{Z})$, when $D \equiv 0 \pmod{4}$. Thus, by Theorem 1.1 the image of the center of $\widetilde{Sp}(2g, \mathbb{Z})$ has order two, as claimed. \square

An immediate corollary is the following K-theory result:

Corollary 3.1. *For $g \geq 3$ we have*

$$KSp_{2,2g}(\mathbb{Z}/D\mathbb{Z}) = \begin{cases} \mathbb{Z}/2\mathbb{Z}, & \text{if } D \equiv 0 \pmod{4}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. According to Stein's stability results ([65], Thm 2.13, and [67]) we have

$$KSp_{2,2g}(\mathbb{Z}/D\mathbb{Z}) \cong KSp_2(\mathbb{Z}/D\mathbb{Z}), \text{ for } g \geq 3, \quad (18)$$

and

$$KSp_{2,2g}(\mathbb{Z}/D\mathbb{Z}) \cong H_2(Sp(2g, \mathbb{Z}/D\mathbb{Z})), \text{ for } g \geq 3. \quad (19)$$

\square

Remark 3.3. The analogous result that $K_{2,n}(\mathbb{Z}/D\mathbb{Z}) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$, if $n \geq 3$ was proved a long time ago (see [14]).

3.4 Proof of Proposition 3.3

In this section we present the homological computations that lead to the proof of Propositions 1.3 and 3.4. Our results hang on the analysis of the extension of groups:

$$1 \rightarrow Sp(2g, \mathfrak{A}, \mathfrak{q}) \rightarrow Sp(2g, \mathfrak{A}) \rightarrow Sp(2g, \mathfrak{A}/\mathfrak{q}) \rightarrow 1,$$

for general Dedekind domains \mathfrak{A} , together with the central extension:

$$1 \rightarrow \mathfrak{sp}_{2g}(q) \rightarrow Sp(2g, \mathbb{Z}/q^{k+1}\mathbb{Z}) \rightarrow Sp(2g, \mathbb{Z}/q^k\mathbb{Z}) \rightarrow 1,$$

for the ring \mathbb{Z} . Recall that, given an ideal $\mathfrak{q} \in \mathfrak{A}$, the group $Sp(2g, \mathfrak{A}, \mathfrak{q})$ is the subgroup of symplectic matrices that are congruent to the identity modulo \mathfrak{q} . This is by definition a *principal congruence subgroup*.

3.4.1 Generators for congruence subgroups

Normal generators of the group $Sp(2g, \mathfrak{A}, \mathfrak{q})$ can be found in ([3], III.12), as follows. Fix a symplectic basis $\{a_i, b_i\}_{1 \leq i \leq g}$ and write the matrix by blocks according to the associated decomposition of \mathfrak{A}^{2g} into maximal isotropic subspaces.

For each pair of distinct integers $i, j \in \{1, \dots, g\}$ denote by $e_{ij} \in \mathfrak{M}_g(\mathbb{Z})$ the matrix whose only non-zero entry is a 1 at the place ij . Set also $\mathbf{1}_k$ for the k -by- k identity matrix.

Then following ([3], Lemma 13.1) $Sp(2g, \mathfrak{A}, \mathfrak{q})$ is the *normal subgroup* of $Sp(2g, \mathfrak{A})$ generated by the matrices:

$$U_{ij}(q) = \begin{pmatrix} \mathbf{1}_g & qe_{ij} + qe_{ji} \\ 0 & \mathbf{1}_g \end{pmatrix}, \quad U_{ii}(q) = \begin{pmatrix} \mathbf{1}_g & qe_{ii} \\ 0 & \mathbf{1}_g \end{pmatrix}, \quad (20)$$

and

$$L_{ij}(q) = \begin{pmatrix} \mathbf{1}_g & 0 \\ qe_{ij} + qe_{ji} & \mathbf{1}_g \end{pmatrix}, \quad L_{ii}(q) = \begin{pmatrix} \mathbf{1}_g & 0 \\ qe_{ii} & \mathbf{1}_g \end{pmatrix}, \quad (21)$$

where $q \in \mathfrak{q}$.

Denote by $E(2g, \mathfrak{A}, \mathfrak{q})$ the subgroup of $Sp(2g, \mathfrak{A}, \mathfrak{q})$ generated by the matrices $U_{ij}(q)$ and $L_{ij}(q)$.

Lemma 3.3. *The group $E(2g, \mathfrak{A}, \mathfrak{q})$ is the subgroup $Sp(2g, \mathfrak{A}, \mathfrak{q}|q^2)$ of $Sp(2g, \mathfrak{A})$ of those symplectic matrices $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ whose entries satisfy the conditions:*

$$B \equiv C \equiv 0 \pmod{\mathfrak{q}}, \text{ and } A \equiv D \equiv \mathbf{1}_g \pmod{\mathfrak{q}^2}. \quad (22)$$

Proof. We follow closely the proof of Lemma 13.1 from [3]. One verifies easily that $Sp(2g, \mathfrak{A}, \mathfrak{q}|q^2)$ is indeed a subgroup of $Sp(2g, \mathfrak{A})$. It then suffices to show that all elements of the form $\begin{pmatrix} A & 0 \\ 0 & (A^{-1})^\top \end{pmatrix}$, with $A \in GL(g, \mathfrak{A})$ satisfying $A \equiv \mathbf{1}_g \pmod{\mathfrak{q}^2}$ belong to $E(2g, \mathfrak{A}, \mathfrak{q})$. Here the notation A^\top stands for the transpose of the matrix A . Next, it suffices to verify this claim when A is an elementary matrix, and hence when A is in $GL(2, \mathfrak{A})$ and $g = 2$. Taking therefore $A = \begin{pmatrix} 1 & 0 \\ q_1 q_2 & 1 \end{pmatrix}$, where $q_1, q_2 \in \mathfrak{q}$, we can write:

$$\begin{pmatrix} A & 0 \\ 0 & (A^{-1})^\top \end{pmatrix} = \begin{pmatrix} 1_2 & \sigma A^\top \\ 0 & 1_2 \end{pmatrix} \begin{pmatrix} 1_2 & 0 \\ -\tau & 1_2 \end{pmatrix} \begin{pmatrix} 1_2 & \sigma \\ 0 & 1_2 \end{pmatrix} \begin{pmatrix} 1_2 & 0 \\ \tau & 1_2 \end{pmatrix}, \quad (23)$$

where $\sigma = \begin{pmatrix} 0 & q_1 \\ q_1 & 0 \end{pmatrix}$ and $\tau = \begin{pmatrix} q_2 & 0 \\ 0 & 0 \end{pmatrix}$. \square

Define now

$$R_{ij}(q) = \begin{pmatrix} \mathbf{1}_g + qe_{ij} & 0 \\ 0 & \mathbf{1}_g - qe_{ji} \end{pmatrix}, \text{ for } i \neq j, \quad (24)$$

and

$$N_{ii}(q) = \begin{pmatrix} \mathbf{1}_g + (q + q^2 + q^3)e_{ii} & -q^2 e_{ii} \\ q^2 e_{ii} & \mathbf{1}_g - qe_{ii} \end{pmatrix}. \quad (25)$$

Proposition 3.5. *The group $Sp(2g, \mathfrak{A}, \mathfrak{q})$ is generated by the matrices $U_{ij}(q)$, $U_{ii}(q)$, $L_{ij}(q)$, $L_{ii}(q)$, $R_{ij}(q)$ and $N_{ii}(q)$, with $q \in B(\mathfrak{q})$, where $B(\mathfrak{q})$ denotes a basis of \mathfrak{q} as a \mathbb{Z} -module. Here i, j are distinct and take values in $\{1, 2, \dots, g\}$.*

Proof. Let G be the group with the generators from the statement, which is obviously contained into $Sp(2g, \mathfrak{A}, \mathfrak{q})$. First, Lemma 3.3 yields the inclusions:

$$G \supset E(2g, \mathfrak{A}, \mathfrak{q}) = Sp(2g, \mathfrak{A}, \mathfrak{q}|\mathfrak{q}^2) \supset Sp(2g, \mathfrak{q}^2). \quad (26)$$

Furthermore, we also have the opposite inclusion:

Lemma 3.4. *We have $Sp(2g, \mathfrak{q}) \subset G \cdot Sp(2g, \mathfrak{q}^2)$.*

These two inclusions imply that:

$$Sp(2g, \mathfrak{A}, \mathfrak{q}) \subset G \cdot Sp(2g, \mathfrak{q}^2) \subset G \quad (27)$$

and hence $G = Sp(2g, \mathfrak{A}, \mathfrak{q})$, finishing the proof of Proposition 3.5. \square

Proof of Lemma 3.4. First $Sp(2g, \mathfrak{A}, \mathfrak{q}^2)$ is a normal subgroup of $Sp(2g, \mathfrak{A}, \mathfrak{q})$ and $Sp(2g, \mathfrak{A}, \mathfrak{q})/Sp(2g, \mathfrak{A}, \mathfrak{q}^2)$ is an abelian group which was described by Newman and Smart in [56], when $\mathfrak{A} = \mathbb{Z}$. Let $\pi : Sp(2g, \mathfrak{A}, \mathfrak{q}) \rightarrow Sp(2g, \mathfrak{A}, \mathfrak{q})/Sp(2g, \mathfrak{A}, \mathfrak{q}^2)$ be the quotient map. The claim of Lemma 3.4 is equivalent to the fact that:

$$\pi(Sp(2g, \mathfrak{A}, \mathfrak{q})) = \pi(G). \quad (28)$$

Notice that although the matrices $\begin{pmatrix} \mathbf{1}_g + qe_{ii} & 0 \\ 0 & \mathbf{1}_g - qe_{ii} \end{pmatrix}$, which would correspond to $R_{ij}(q)$ for $i = j$, are *not symplectic*, they are congruent mod \mathfrak{q}^2 to the symplectic matrices $N_{ii}(q)$.

The proof of the equality above follows as in ([56], Thm.6). For the sake of completeness here is a sketch. Any element of $Sp(2g, \mathfrak{A}, \mathfrak{q})$ has the form $\begin{pmatrix} \mathbf{1}_g + qA & qB \\ qC & \mathbf{1}_g + qD \end{pmatrix}$, where $D \equiv A^\top \pmod{\mathfrak{q}}$, $B \equiv B^\top \pmod{\mathfrak{q}}$ and $C \equiv C^\top \pmod{\mathfrak{q}}$. Then there exist symmetric matrices X, Y such that $X \equiv B \pmod{\mathfrak{q}}$ and $Y \equiv C \pmod{\mathfrak{q}}$. Therefore we can write:

$$\begin{pmatrix} \mathbf{1}_g + qA & qB \\ qC & \mathbf{1}_g + qD \end{pmatrix} \equiv \begin{pmatrix} \mathbf{1}_g & qX \\ 0 & \mathbf{1}_g \end{pmatrix} \begin{pmatrix} \mathbf{1}_g & 0 \\ qY & \mathbf{1}_g \end{pmatrix} \begin{pmatrix} \mathbf{1}_g + qA & 0 \\ qY & \mathbf{1}_g - qA^\top \end{pmatrix} \pmod{\mathfrak{q}^2}. \quad (29)$$

Since the matrices on the right hand side can be expressed mod \mathfrak{q}^2 as products of the matrices $U_{ij}(q)$, $U_{ii}(q)$, $L_{ij}(q)$, $L_{ii}(q)$, $R_{ij}(q)$, $N_{ii}(q)$ it follows that $\pi(G)$ contains $\pi(Sp(2g, \mathfrak{A}, \mathfrak{q}))$. \square

3.4.2 End of the proof of proposition 3.3

If M is endowed with a structure of G -module we denote by M_G the ring of co-invariants, namely the quotient of M by the submodule generated by $\langle g \cdot x - x, g \in G, x \in M \rangle$.

It is known (see [8], VII.6.4) that an exact sequence of groups

$$1 \rightarrow K \rightarrow G \rightarrow Q \rightarrow 1$$

induces the following 5-term exact sequence in homology (with coefficients in an arbitrary G -module M):

$$H_2(G; M) \rightarrow H_2(Q; M_H) \rightarrow H_1(K)_Q \rightarrow H_1(G, M) \rightarrow H_1(Q, M_H) \rightarrow 0. \quad (30)$$

From the 5-term exact sequence associated to the short exact sequence:

$$1 \rightarrow Sp(2g, \mathfrak{A}, \mathfrak{q}) \rightarrow Sp(2g, \mathfrak{A}) \rightarrow Sp(2g, \mathfrak{A}/\mathfrak{q}) \rightarrow 1$$

we deduce that the surjectivity of p_* is equivalent to the result of the following Lemma 3.5 hereafter.

Lemma 3.5. *For any ideal \mathfrak{q} , if $g \geq 3$ we have:*

$$H_1(Sp(2g, \mathfrak{A}, \mathfrak{q}))_{Sp(2g, \mathfrak{A}/\mathfrak{q})} = 0. \quad (31)$$

Proof of Lemma 3.5. For each pair of distinct integers $i, j \in \{1, \dots, g\}$ denote by A_{ij} the symplectic matrix:

$$A_{ij} = \begin{pmatrix} \mathbf{1}_g - e_{ij} & 0 \\ 0 & \mathbf{1}_g + e_{ji} \end{pmatrix}. \quad (32)$$

Then for each triple of distinct integers (i, j, k) and $q \in \mathfrak{q}$ the action of A_{ij} by conjugacy on the generating matrices of $Sp(2g, \mathfrak{A}, \mathfrak{q})$ is given by:

$$A_{ij} \cdot U_{jj}(q) = U_{ii}(q)U_{jj}(q)U_{ij}(q)^{-1}, \quad A_{ki} \cdot U_{ij}(q) = U_{ij}(q)U_{jk}(q)^{-1}, \quad A_{ji} \cdot U_{ij}(q) = U_{ij}(q)U_{jj}(q)^{-2}, \quad (33)$$

$$A_{ij} \cdot L_{jj}(q) = L_{ii}(q)L_{jj}(q)L_{ij}(q), \quad A_{ik} \cdot L_{ij}(q) = L_{ij}(q), \quad A_{ij} \cdot L_{ij}(q) = L_{ij}(q)L_{ii}(q)^2, \quad (34)$$

where $A \cdot U = AUA^{-1}$. We also have:

$$A_{ij} \cdot R_{jk}(q) = R_{jk}(q)R_{ik}(q). \quad (35)$$

Further the symplectic map $J = \begin{pmatrix} 0 & -\mathbf{1}_g \\ \mathbf{1}_g & 0 \end{pmatrix}$ acts as follows:

$$J \cdot U_{ij}(q) = -L_{ij}(q), \quad J \cdot U_{ii}(q) = -L_{ii}(q). \quad (36)$$

Denote by lower cases the classes of the maps $U_{ij}(q)$, $U_{ii}(q)$, $L_{ij}(q)$, $L_{ii}(q)$, $R_{ij}(q)$ and $N_{ii}(q)$ in the quotient $H_1(Sp(2g, \mathfrak{A}, \mathfrak{q}))_{Sp(2g, \mathfrak{A}/\mathfrak{q})}$ of the abelianization $H_1(Sp(2g, \mathfrak{A}, \mathfrak{q}))$. By definition, the action of $Sp(2g, \mathfrak{A}/\mathfrak{q})$ on $H_1(Sp(2g, \mathfrak{A}, \mathfrak{q}))_{Sp(2g, \mathfrak{A}/\mathfrak{q})}$ is trivial.

Using the action of J we obtain that $u_{ij}(q) + l_{ij}(q) = 0$ in $H_1(Sp(2g, \mathfrak{A}, \mathfrak{q}))_{Sp(2g, \mathfrak{A}/\mathfrak{q})}$, and hence we can discard the generators $l_{ij}(q)$. As $g \geq 3$, from the action of A_{ki} on $u_{ij}(q)$ we derive that $u_{jk}(q) = 0$, for every $j \neq k$. Using the action of A_{ij} on $u_{jj}(q)$ we obtain that $u_{jj}(q) = 0$ for every j . Further the action of A_{ij} on $r_{jk}(q)$ yields $r_{ik}(q) = 0$, for all $i \neq k$.

Consider now the symplectic matrix $B_{ii} = \begin{pmatrix} \mathbf{1}_g & 0 \\ e_{ii} & \mathbf{1}_g \end{pmatrix}$. Then

$$B_{ii} \cdot U_{ii}(q) = \begin{pmatrix} \mathbf{1}_g - qe_{ii} & qe_{ii} \\ -qe_{ii} & \mathbf{1}_g + qe_{ii} \end{pmatrix} \quad (37)$$

and hence

$$B_{ii} \cdot U_{ii}(q) \equiv U_{ii}(q)L_{ii}(q)^{-1}N_{ii}(q)^{-1} \pmod{\mathfrak{q}^2}. \quad (38)$$

Recall that the elements of $Sp(2g, \mathfrak{A}, \mathfrak{q}^2) \subset Sp(2g, \mathfrak{A}, \mathfrak{q}|\mathfrak{q}^2)$ can be written as products of the generators $U_{ij}(q)$ and $L_{ij}(q)$ according to Lemma 3.3, whose images in the quotient $H_1(Sp(2g, \mathfrak{A}, \mathfrak{q}))_{Sp(2g, \mathfrak{A}/\mathfrak{q})}$ vanish. Therefore $B_{ii} \cdot u_{ii}(q) = u_{ii}(q) + l_{ii}(q) - n_{ii}(q)$. This proves that $n_{ii}(q) = 0$ in $H_1(Sp(2g, \mathfrak{A}, \mathfrak{q}))_{Sp(2g, \mathfrak{A}/\mathfrak{q})}$. Consequently $H_1(Sp(2g, \mathfrak{A}, \mathfrak{q}))_{Sp(2g, \mathfrak{A}/\mathfrak{q})} = 0$, as claimed. \square

4 Mapping class group quotients

4.1 Preliminaries on quantum representations

The results of this section are the counterpart of those obtained in section 2.4, by considering $SU(2)$ instead of abelian quantum representations. The first author proved in [18] that central extensions of the mapping class group M_g by \mathbb{Z} are residually finite. The same method actually can be used to show the abundance of finite quotients with large torsion in their essential second homology and to prove that the mapping class group has property A_2 for the trivial modules.

A quantum representation is a projective representation, depending on an integer k , which lifts to a linear representation $\tilde{\rho}_k : M_g(12) \rightarrow U(N(k, g))$ of the central extension $M_g(12)$ of the mapping class group M_g by \mathbb{Z} . The later representation corresponds to invariants of 3-manifolds with a p_1 -structure. Masbaum, Roberts ([45]) and Gervais ([21]) gave a precise description of this extension. Namely, the cohomology class $c_{M_g(12)} \in H^2(M_g, \mathbb{Z})$ associated to this extension equals 12 times the signature class χ . It is known (see [40]) that the group $H^2(M_g)$ is generated by χ , when $g \geq 2$. Recall that χ is the class of one fourth the

Meyer signature cocycle. We denote more generally by $M_g(n)$ the central extension by \mathbb{Z} whose class is $c_{M_g(n)} = n\chi$.

It is known that M_g is perfect and $H_2(M_g) = \mathbb{Z}$, when $g \geq 4$ (see [57], for instance). Thus, for $g \geq 4$, M_g has an universal central extension by \mathbb{Z} , which can be identified with the central extension $M_g(1)$. This central extension makes sense for M_3 , as well, although one only knows that $H_2(M_3) = \mathbb{Z} \oplus A$, with $A \in \{0, \mathbb{Z}/2\mathbb{Z}\}$. However, using its explicit presentation for $g = 3$ we derive that $M_g(1)$ is perfect for $g \geq 3$.

Let c be the generator of the center of $M_g(1)$, which is 12 times the generator of the center of $M_g(12)$. Denote by $M_g(1)_n$ the quotient of $M_g(1)$ obtained by imposing $c^n = 1$, this is a non-trivial central extension of the mapping class group by $\mathbb{Z}/n\mathbb{Z}$. We will say that a quantum representation $\tilde{\rho}_p$ *detects* the center of $M_g(1)_n$ if it factors through $M_g(1)_n$ and is injective on its center.

If we choose the $\text{SO}(3)$ -TQFT with parameter $A = -\zeta_p^{(p+1)/2}$, where ζ_p is a primitive p -th root of unity, so that A is a primitive $2p$ root of unity with $A^2 = \zeta_p$. This data leads to a quantum representation $\tilde{\rho}_p$ for which Masbaum and Roberts computed in [45] that $\tilde{\rho}_p(c) = A^{-12-p(p+1)}$.

Lemma 4.1. *For each prime power q^s there exists some quantum representations $\tilde{\rho}_p$ which detects the center of $M_g(1)_{q^s}$.*

Proof. We noted that $\tilde{\rho}_p = \zeta_{2p}^{-12-p(p+1)}$, where ζ_{2p} is a $2p$ -root of unity.

1. If q is a prime number $q \geq 5$ we let $p = q^s$. Then $2p$ divides $p(p+1)$ and $\tilde{\rho}_p(c) = \zeta_{2p}^{-12} = \zeta_p^{-6}$ is of order $p = q^s$. Thus the representation $\tilde{\rho}_p$ detects the center of $M_g(1)_{q^s}$.
2. If $q = 2$, we set $p = 2$. Then $\tilde{\rho}_2(c) = \zeta_2$, and $\tilde{\rho}_2$ detects the center of $M_g(1)_2$.
3. Set now $p = 12r$ for some integer $r > 1$ to be fixed later. Then $\tilde{\rho}_p(c) = \zeta_{24r}^{-12-12r(12r+1)} = \zeta_{2r}^{-1-r(12r+1)} = \zeta_{2r}^{-1-r}$. This $2r$ -th root of the unit has order $\text{l.c.m.}(1+r, 2r)/(1+r) = 2r/\text{g.c.d.}(1+r, 2r)$. An elementary computation shows that $\text{g.c.d.}(1+r, 2r) = 1$ or 2 depending on whether r is even or odd.
 - If $r = 2^s$, then $\zeta_{2 \cdot 2^s}^{-1-2^s}$ is of order 2^{s+1} , the representation $\tilde{\rho}_p$ detects the center of through $M_g(1)_{2^{s+1}}$.
 - If $r = 3^s$, then $\zeta_{2 \cdot 3^s}^{-1-3^s}$ is of order 3^s , the representation $\tilde{\rho}_p$ detects the center of $M_g(1)_{3^s}$.

□

4.2 Proof of Theorem 1.4

We have first the following lemma:

Lemma 4.2. *Let G be a perfect finitely presented group, \tilde{G} denote its universal central extension, $p : G \rightarrow F$ be a surjective homomorphism onto a finite group F and $\hat{p} : \tilde{G} \rightarrow \Gamma$ be some lift of p to a finite central extension Γ of F . Assume that the image $C = \hat{p}(Z(\tilde{G}))$ of the center $Z(\tilde{G})$ of \tilde{G} contains an element of order q . Then there exists an element of $p_*(H_2(G)) \subset H_2(F)$ of order q .*

Proof. Observe that $Z(\tilde{G})$ coincide with the subgroup $H_2(G)$ of \tilde{G} . Further Γ is a central extension of F by $C = \ker(\Gamma \rightarrow F)$. According to lemma 2.2 there exists a lift $\tilde{p} : \tilde{G} \rightarrow \tilde{F}$ of p , to the universal central extension \tilde{F} of F . There exists a unique homomorphism $s : \tilde{F} \rightarrow \Gamma$ of central extensions of F i.e. lifting the identity map of F . The homomorphisms \hat{p} and $s \circ \tilde{p} : \tilde{G} \rightarrow \Gamma$ are both lifts of p . Therefore there exists a map $a : \tilde{G} \rightarrow C$ such that $\hat{p}(x) = a(x)s \circ \tilde{p}(x)$, for every $x \in \tilde{G}$. Since C is central we derive that $a : \tilde{G} \rightarrow C$ is a homomorphism. Since a universal central extension as \tilde{G} must be perfect, it follows that a is trivial and hence $\hat{p} = s \circ \tilde{p}$.

In particular, this holds when restricting to $Z(\tilde{G}) = H_2(G)$. But the restriction of \tilde{p} to $H_2(G)$ coincides with the homomorphism $p_* : H_2(G) \rightarrow H_2(F)$, by lemma 2.2.

If $z \in H_2(G)$ is such that $\hat{p}(z)$ has order q in C then $p_*(z) \in p_*(H_2(F)) \subset \tilde{F}$ is sent by s into some element of order q . Therefore $p_*(z)$ has order a multiple of q . A suitable power of it has then the required order. □

Remark 4.1. A cautionary remark is in order. Assume that $H_2(G) = \mathbb{Z}$ in the key lemma above and $H \subset K$ is the kernel of p . If the image of $H_2(H)$ in $H_2(G)$ is $d\mathbb{Z}$ then we can only assert that the image $p_*(H_2(G))$ in $H_2(F)$ is of the form $\mathbb{Z}/d'\mathbb{Z}$, for some divisor d' of d , which might be proper divisor. For instance taking $G = Sp(2g, \mathbb{Z})$ and $F = Sp(2g, \mathbb{Z}/D\mathbb{Z})$, where D is even and not multiple of 4, then $d = 2$ by ([58], Thm. F), while $d' = 1$ as $H_2(Sp(2g, \mathbb{Z}/D\mathbb{Z})) = 0$. The apparent contradiction with lemma 4.2 comes from the fact that we considered a lift $\hat{p} : \tilde{G} \rightarrow \Gamma$, which a rather strong assumption. If H were perfect, as it is the case when $F = Sp(2g, \mathbb{Z}/2\mathbb{Z})$ then the universal central extension \tilde{H} would come with a homomorphism $\tilde{H} \rightarrow \tilde{G}$. Although the image of \tilde{H} is a finite index subgroup, it is not, in general, a normal subgroup of \tilde{G} . Passing to a finite index normal subgroup of \tilde{H} would amount to change H into a smaller subgroup H' and hence F is replaced by a larger quotient F' . This was precisely the reasoning in section 2.3, where we started with $F = Sp(2g, \mathbb{Z}/2\mathbb{Z})$ and arrived to $F' = Sp(2g, \mathbb{Z}/8\mathbb{Z})$.

End of proof of Theorem 1.4. By a classical result of Malcev [44], finitely generated subgroups of linear groups over a commutative unital ring are residually finite. This applies to the images of quantum representations. Hence there are finite quotients \tilde{F} of these for which the image of the generator of the center is not trivial. By Lemma 4.1 we may find quantum representations for which the order of the image of the center can have arbitrary prime power order p . Hence, for any prime p there are finite quotients \tilde{F} of $M_g(1)$ in which the image of the center has an element of order p . We apply Lemma 4.2 to the quotient F of \tilde{F} by the image of the center to get finite quotients of the mapping class group with arbitrary primes in the essential homology $EH_2(F, M_g)$. \square

Concrete finite quotients with arbitrary torsion in their essential homology from mapping class groups can be constructed as follows. Let p be a prime different from 2 and 3. According to Gilmer and Masbaum ([22]) we have that $\tilde{\rho}_p(\tilde{M}_g(1)) \subset U(N(p, g)) \cap GL(\mathcal{O}_p)$ for prime p , where \mathcal{O}_p is the following ring of cyclotomic integers $\mathcal{O}_p = \begin{cases} \mathbb{Z}[\zeta_p], & \text{if } p \equiv -1 \pmod{4} \\ \mathbb{Z}[\zeta_{4p}], & \text{if } p \equiv 1 \pmod{4}. \end{cases}$

Let then consider the principal ideal $\mathfrak{m} = (1 - \zeta_p)$ which is a prime ideal of \mathcal{O}_p . It is known that prime ideals of \mathcal{O}_p are maximal and then $\mathcal{O}_p/\mathfrak{m}^n$ is a finite ring for every n . Let then $\Gamma_{p,\mathfrak{m},n}$ be the image of $\tilde{\rho}_p(M_g(1))$ into the finite group $GL(N(p, g), \mathcal{O}_p/\mathfrak{m}^n)$ and $F_{p,\mathfrak{m},n}$ be the quotient $\Gamma_{p,\mathfrak{m},n}/(\tilde{\rho}_p(c))$ by the image of the center of $M_g(1)$.

The image $\tilde{\rho}_p(c)$ of the generator c into $\Gamma_{p,\mathfrak{m},n}$ is the scalar root of unity ζ_p^{-6} , which is a non-trivial element of order p in the ring $\mathcal{O}_p/\mathfrak{m}^n$ and hence an element of order p into $GL(N(p, g), \mathcal{O}_p/\mathfrak{m}^n)$. Notice that this is a rather exceptional situation, which does not occur for other prime ideals in unequal characteristic (see Proposition 4.1).

Lemma 4.2 implies then that the image $p_*(H_2(M_g))$ within $H_2(F_{p,\mathfrak{m},n})$ contains an element of order p . This result also shows the contrast between the mapping class group representations and the Weil representations:

Corollary 4.1. *If $g \geq 3$, p is prime and $p \notin \{2, 3\}$ (or more generally, p does not divide 12 and not necessarily prime), then $\tilde{\rho}_p(\tilde{M}_g)$ is a non-trivial central extension of $\rho_p(M_g)$. Furthermore, under the same hypotheses on g and p , if $\mathfrak{m} = (1 - \zeta_p)$, then the extension $\Gamma_{p,\mathfrak{m},n}$ of the finite quotient $F_{p,\mathfrak{m},n}$ is non-trivial.*

Proof. If the extension were trivial then by universality $\tilde{\rho}_p$ would kill the center of $M_g(1)$, and this is not the case. The same argument yields the second claim. \square

Remark 4.2. Although the group M_2 is not perfect, because $H_1(M_2) = \mathbb{Z}/10\mathbb{Z}$, it still makes sense to consider the central extension \tilde{M}_2 arising from the TQFT. Then the computations above show that the results of Theorem 1.4 and Corollary 4.1 hold for $g = 2$ if p is a prime and $p \notin \{2, 3, 5\}$.

Remark 4.3. The finite quotients $F_{p,\mathfrak{m},n}$ associated to the ramified principal ideal $\mathfrak{m} = (1 - \zeta_p)$ were previously considered by Masbaum in [46].

When $p \equiv -1 \pmod{4}$ the authors of [19, 47] found many finite quotients of M_g by using more sophisticated means. However, the results of [19, 47] and the present ones are of a rather different nature. Assume that \mathfrak{n} is a prime ideal of \mathcal{O}_p such that $\mathcal{O}_p/\mathfrak{n}$ is the finite field \mathbb{F}_q with q elements. In fact the case of equal characteristics $\mathfrak{n} = \mathfrak{m} = (1 - \zeta_p)$ is the only case where non-trivial torsion can arise, according to:

Proposition 4.1. *If \mathfrak{n} is a prime ideal of unequal characteristic (i.e. such that $\text{g.c.d.}(p, q) = 1$) and $p, q \geq 5$ then $EH_2(F_{p,\mathfrak{n},n}, M_g) = 0$. Moreover, for all but finitely many prime ideal \mathfrak{n} of unequal characteristic both groups $\Gamma_{p,\mathfrak{n},1}$ and $F_{p,\mathfrak{n},1}$ coincide with $SL(N(p, g), \mathbb{F}_q)$ and hence $H_2(F_{p,\mathfrak{n},1}) = 0$.*

Proof. The image of a p -th root of unity scalar in $SL(N(p, g), \mathbb{F}_q)$ is trivial, as soon as $\text{g.c.d.}(p, q) = 1$. Thus $\Gamma_{p,\mathfrak{n},n} \rightarrow F_{p,\mathfrak{n},n}$ is an isomorphism and hence the image of $H_2(M_g)$ into $H_2(F_{p,\mathfrak{n},n})$ must be trivial. A priori this does not mean that $H_2(F_{p,\mathfrak{n},n}) = 0$. However, Masbaum and Reid proved in [47] that for all but finitely many prime ideals \mathfrak{n} in \mathcal{O}_p the image $\Gamma_{p,\mathfrak{n},1} \subset GL(N(p, g), \mathbb{F}_q)$ is the whole group $SL(N(p, g), \mathbb{F}_q)$. It follows that the projection homomorphism $\widetilde{M}_g(1) \rightarrow SL(N(p, g), \mathbb{F}_q)$ factors through $M_g \rightarrow SL(N(p, g), \mathbb{F}_q)$. But $H_2(SL(N, \mathbb{F}_q)) = 0$, for $N \geq 4, q \geq 5$, as $SL(N, \mathbb{F}_q)$ itself is the universal central extension of $PSL(N, \mathbb{F}_q)$. \square

4.3 Property A_2 and the proof of Theorem 1.5

Recall that an equivalent formulation of Serre's' property A_2 is

Definition 4.1. *Let G be a discrete group and \widehat{G} its profinite completion. Then G has property A_2 for the finite \widehat{G} -module M if the homomorphism $H^k(\widehat{G}, M) \rightarrow H^k(G, M)$ is an isomorphism for $k \leq 2$ and injective for $k = 3$.*

Proposition 4.2. *Let $g \geq 4$ be an integer. For any finitely generated abelian group A and any central extension*

$$1 \rightarrow A \rightarrow E \rightarrow M_g \rightarrow 1$$

the group E is residually finite.

The key result that interlocks between Proposition 4.2 and property A_2 is:

Proposition 4.3. *1. A residually finite group G has property A_2 for all finite G -modules M if and only if any extension by a finite abelian group is residually finite.*

2. Moreover for trivial G -modules it is enough to consider central extensions of G .

Then Theorem 1.5 is a consequence of the two Propositions above.

4.3.1 Proof of Proposition 4.2

First we treat the following special case:

Proposition 4.4. *For any integer $n \geq 2$, the group $M_g(1)_n$ obtained by reducing mod n a generator of the center of $M_g(1)$ is residually finite.*

Proof. Write $\mathbb{Z}/n\mathbb{Z}$ as a finite product of cyclic groups of prime power order $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z}$. Then this isomorphism induces an embedding $M_g(1)_k \hookrightarrow M_g(1)_{p_1^{r_1}} \times \cdots \times M_g(1)_{p_s^{r_s}}$, and it suffices to prove Proposition 4.4 when n is a prime power. Since M_g is known to be residually finite [24], by Malcev's result on the residual finiteness of finitely generated linear groups, it is enough to find for each prime power q^s a linear representation of the universal central extension $M_g(1)$ that factors through $M_g(1)_{q^s}$ and detects its center, and this is what Lemma 4.2 provides. \square

End of proof of Proposition 4.2. We will use below that a group is residually finite if and only if finite index subgroups are residually finite. Given our central extension

$$1 \rightarrow A \rightarrow E \rightarrow M_g \rightarrow 1$$

the five term exact sequence in homology reduces to:

$$H_2(M_g; \mathbb{Z}) \rightarrow A \rightarrow H_1(E; \mathbb{Z}) \rightarrow 0$$

because the mapping class group is perfect. Therefore, any element $f \in E$ that is not in A , projects non-trivially in the mapping class group and is therefore detected by a finite quotient of this group. If $f \in A$ but is not in the image of $H_2(M_g; \mathbb{Z})$, then it projects non-trivially into the finitely generated abelian group $H_1(E; \mathbb{Z})$, and is therefore detected by a finite abelian quotient of E . It remains to detect the elements in the image of $H_2(M_g; \mathbb{Z})$. Recall the following result:

Lemma 4.3. Let A be a finitely generated abelian group, B a subgroup of A . Then there exists a direct factor C of A that contains B as a subgroup of finite index.

Apply this lemma to the image B of $H_2(M_g; \mathbb{Z})$ into A , let p_C be the projection onto the subgroup C and consider the push-out diagram:

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & M_g & \longrightarrow 1 \\ & & \downarrow p_C & & \downarrow & & \parallel & \\ 1 & \longrightarrow & C & \longrightarrow & E_C & \longrightarrow & M_g & \longrightarrow 1 \end{array}$$

Then it is sufficient to prove that E_C is residually finite in order to show that E is residually finite.

Now, the mapping class group M_g is perfect, and therefore we have a push-out diagram:

$$\begin{array}{ccccccc} 1 & \longrightarrow & H_2(M_g; \mathbb{Z}) & \longrightarrow & M_g(1) & \longrightarrow & M_g & \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \parallel & \\ 1 & \longrightarrow & C & \longrightarrow & E_C & \longrightarrow & M_g & \longrightarrow 1, \end{array}$$

where the first row is the universal central extension, and the arrow $H_2(M_g; \mathbb{Z}) \rightarrow C$ is the one appearing in the five term exact sequence of the bottom extension. Recall that for $g \geq 4$, $H_2(M_g; \mathbb{Z}) = \mathbb{Z}$. Two cases could occur:

1. Either $H_2(M_g; \mathbb{Z}) \rightarrow C$ is injective and in this case E_C contains the residually finite group $M_g(1)$ as a subgroup of finite index, and this is known to be residually finite (see [18]).
2. Or the image of $H_2(M_g; \mathbb{Z}) \rightarrow C$ is a cyclic group $\mathbb{Z}/k\mathbb{Z}$ and E_C contains as a finite index subgroup the reduction mod k of the universal central extension, and we conclude applying Proposition 4.4.

□

4.3.2 Proof of proposition 4.3 (1)

Assume that every extension of G by a finite abelian group is residually finite. Let $x \in H^2(G; A)$ be represented by the extension:

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1.$$

By the equivalent property D_2 (see the next subsection), it is enough to find a finite index subgroup $H \subset G$ such that x is zero in $H^2(H; A)$. Since E is residually finite, for each non-trivial element $a \in A$ choose a finite quotient F_a of E in which the image of a is not identity. Let B_a be the image of A in F_a , and $Q_a = E_a / B_a$. Denote by F_A , B_A and Q_A the products of these finitely many groups over the non-trivial elements in A . Then the diagonal map $E \rightarrow F_A$ fits into a commutative diagram:

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow & \\ 1 & \longrightarrow & E_A & \longrightarrow & F_A & \longrightarrow & Q_A & \longrightarrow 1 \end{array}$$

Let K be the kernel $\ker(G \rightarrow Q_A)$. Then K is a finite index normal subgroup and the pull back of x to $H^2(K; A)$ is trivial.

Conversely, assume that extension G has property A_2 and let

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1$$

be an extension of G by the finite abelian group A . Then, by [63, Ex. 2 Ch. I.2.6], we have a natural short exact sequence of profinite completions:

$$1 \longrightarrow \widehat{A} \longrightarrow \widehat{E} \longrightarrow \widehat{G} \longrightarrow 1$$

that fits into a commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & A & \longrightarrow & E & \longrightarrow & G & \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow & \\ 1 & \longrightarrow & \widehat{A} & \longrightarrow & \widehat{E} & \longrightarrow & \widehat{G} & \longrightarrow 1 \end{array}$$

Since A is finite $A \simeq \widehat{A}$, and since G is residually finite the rightmost downward arrow is an injection. By the five lemma the homomorphism $E \hookrightarrow \widehat{E}$ is also injective, and hence E is residually finite, as a subgroup of a profinite group.

4.3.3 Proof of proposition 4.3 (2) and property E_n

It would be nice, but probably difficult, to understand under which assumptions property A_2 for a residually finite, finitely presented group G and all finite trivial \widehat{G} -modules implies the property A_2 . However, there exists a stronger related condition on groups for which this kind of statement will hold. Serre introduced several equivalent properties in ([63], Ex.1), as follows. One says that a residually finite group G has property:

1. (A_n) if $H^j(\widehat{G}; M) \rightarrow H^j(G, M)$ is bijective for $j \leq n$ and injective for $j = n+1$, for all finite G -modules M .
2. (B_n) if $H^j(\widehat{G}; M) \rightarrow H^j(G, M)$ is surjective for $j \leq n$ and for all finite G -modules M .
3. (C_n) for each $x \in H^j(G, M)$, $1 \leq j \leq n$, there exists a discrete G -module M' containing M such that the image of x in $H^j(G; M') = 0$.
4. (D_n) for each $x \in H^j(G, M)$, $1 \leq j \leq n$, there exists a subgroup $H \subset G$ of finite index in G such that the image of x in $H^j(H, M)$ is zero.

Then Serre stated that properties A_n , B_n , C_n and D_n are equivalent. It is easy to see that these properties are also equivalent when we fix the \widehat{G} -module M , or we let it run over the finite trivial \widehat{G} -modules.

Denote by $\widehat{H}^n(G; M) = \lim_{H \subset_f G} H^j(H, M)$, where the direct limit is taken with respect with the directed set of $H \subset_f G$, meaning that H is a finite index subgroup of G . The directed set of inclusions homomorphisms induce a homomorphism

$$H^n(G; M) \rightarrow \widehat{H}^n(G; M)$$

We can therefore rephrase condition D_n by asking that the homomorphism $H^n(G; M) \rightarrow \widehat{H}^n(G; M)$ have zero image. This is therefore a consequence of the following stronger condition: a group G has property E_n if $\widehat{H}^j(G; M) = 0$, for $1 \leq j \leq n$ and for all finite \widehat{G} -modules M . An interesting fact concerning this condition is the following:

Proposition 4.5. *If a residually finite group G has property E_n for all finite trivial \widehat{G} -modules then it has property E_n .*

Proof. First we can easily step from \mathbb{F}_p coefficients to any trivial G -module.

Lemma 4.4. *Condition (D_n) for G and all trivial \widehat{G} -modules \mathbb{F}_p implies (D_n) for G and all trivial \widehat{G} -modules M .*

The second ingredient allows us to pass from all trivial coefficients to arbitrary coefficients:

Lemma 4.5. *Condition (E_n) for G and all trivial \widehat{G} -modules M implies (E_n) for G and all \widehat{G} -modules M .*

This proves the claim of proposition 4.5. □

In the proof of lemma 4.5 we will make use of the following rather well-known result:

Lemma 4.6. *If $J \subset I$ are two directed sets such that J is cofinal in I then for any direct system of abelian groups (A_i, f_{ij}) indexed by I we have*

$$\lim_{\alpha, \beta \in J} (A_\alpha, f_{\alpha\beta}) = 0, \quad \text{if and only if} \quad \lim_{i, j \in I} (A_i, f_{ij}) = 0.$$

Proof of lemma 4.4. This follows from decomposing the abelian group A in p -primary components and then use induction on the rank of the composition series of A and the 5-lemma. \square

Proof of lemma 4.5. Let now M be an arbitrary finite G -module. Let K_M be the kernel of the G -action on M . We denote by A the trivial G -module which is isomorphic as an abelian group to M . By hypothesis condition (E_n) is satisfied for the group G and the trivial module A , so that $\widehat{H}^j(G, ; A) = 0$, $1 \leq j \leq n$. Since M is finite K_M is of finite index in G . Consider the set $J_M = \{H \subset_f K_M\}$ of finite index subgroups of $K_M \subset G$. This is a subset of the directed set I_G of finite index subgroups of G . Further J_M is cofinal in I_G with respect to the inclusion as any subgroup $H \in I_G$ contains the subgroup $H \cap K_M \subset_f K_M$. According to lemma 4.6 we have then $\lim_{H \subset_f K_M} H^j(H, A) = 0$. Furthermore, for each $H \subset K_M$ the H -modules A and M are isomorphic as both are trivial. Thus there exists a canonical family of isomorphisms $i_H : H^j(H, A) \cong H^j(H, M)$ which is compatible with the direct structures on the cohomology groups indexed by $J_M = \{H \subset_f K_M\}$. We have therefore $\lim_{H \subset_f K_M} H^j(H, M) = 0$. However using again lemma 4.6 for the set J_M and I_G in the reverse direction to obtain $\widehat{H}^j(G, ; M) = 0$, $1 \leq j \leq n$. \square

End of proof of Proposition 4.3 (2). This is an immediate consequence of Lemma 4.4 and the equivalence of conditions D_2 and A_2 . \square

Remark 4.4. The analog of lemma 4.4 holds also property A_n , with the same proof. However, this is not clear for lemma 4.5.

Remark 4.5. The discussion about property E_n clarifies some of the statements in [25]. Specifically, Lemmas 3.1. and 3.2. from [25] concern only property E_n instead of property A_n . Nevertheless, the main result of [25] is valid with the same proof.

5 Towards an inductive proof of Theorem 1.1

5.1 Motivation

For a prime p , an integer $k \geq 1$ we have two fundamental extensions:

$$1 \rightarrow Sp(2g, \mathbb{Z}, p^k) \rightarrow Sp(2g, \mathbb{Z}) \rightarrow Sp(2g, \mathbb{Z}/p^k\mathbb{Z}) \rightarrow 1,$$

and

$$1 \rightarrow \mathfrak{sp}_{2g}(p) \rightarrow Sp(2g, \mathbb{Z}/p^{k+1}\mathbb{Z}) \rightarrow Sp(2g, \mathbb{Z}/p^k\mathbb{Z}) \rightarrow 1. \quad (39)$$

In particular, every element in $Sp(2g, \mathbb{Z}, p^k)$ can be written as $\mathbf{1}_{2g} + p^k A$, for some matrix A with integer entries. If the symplectic form is written as $J_g = \begin{pmatrix} 0 & \mathbf{1}_g \\ -\mathbf{1}_g & 0 \end{pmatrix}$ then the matrix A satisfies the equation $A^\top J_g + J_g A \equiv 0 \pmod{q}$. Then we set $\mathfrak{sp}_{2g}(p)$ for the additive group of those matrices with entries in $\mathbb{Z}/p\mathbb{Z}$ that satisfy the equation ${}^t M J_g + J_g M \equiv 0 \pmod{q}$. In particular this subgroup is independent of the integer k .

The homomorphism $j_q : Sp(2g, \mathbb{Z}, p^k) \rightarrow \mathfrak{sp}_{2g}(p)$ sending $\mathbf{1}_{2g} + p^k A$ onto $A \pmod{p}$ is surjective (see [62]).

The different actions of the symplectic group $Sp(2g, \mathbb{Z})$ that $\mathfrak{sp}_{2g}(p)$ inherits from these descriptions coincide. We will use in this text the action that is induced by the conjugation action on $Sp(2g, \mathbb{Z}, p)$ via the surjective map j_q . Notice that clearly this action factors through $Sp(2g, \mathbb{Z}/p\mathbb{Z})$.

The second page of the Hochschild-Serre spectral sequence associated to the exact sequence (39) in low degrees is as follows:

$H_2(\mathfrak{sp}_{2g}(p))_{Sp(2g, \mathbb{Z}/p^k\mathbb{Z})}$	$H_1(Sp(2g, \mathbb{Z}/p^k\mathbb{Z}); \mathfrak{sp}_{2g}(p))$	$H_2(Sp(2g, \mathbb{Z}/p^k\mathbb{Z}))$
0	0	
\mathbb{Z}		

(40)

In fact from Lemma 3.5 we obtain:

$$H_1(\mathfrak{sp}_{2g}(p))_{Sp(2g, \mathbb{Z}/p^k\mathbb{Z})} = H_1(\mathfrak{sp}_{2g}(p))_{Sp(2g, \mathbb{Z}/p\mathbb{Z})} = 0.$$

as the action of $Sp(2g, \mathbb{Z}/p^k\mathbb{Z})$ on $\mathfrak{sp}_{2g}(p)$ factors through the action of $Sp(2g, \mathbb{Z}/p\mathbb{Z})$.

Thus the calculations needed for an inductive computation of $H_2(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}))$ are then the result in Theorem 1.6 and the following Theorem of Putman (see [58], Thm. G):

Theorem 5.1. *For any odd prime p , any integer $k \geq 1$ and any $g \geq 3$ we have:*

$$H_1(Sp(2g, \mathbb{Z}/p^k\mathbb{Z}), \mathfrak{sp}_{2g}(p)) = 0. \quad (41)$$

Moreover, this holds true also when $p = 2$ and $k = 1$.

Unfortunately we do not know whether $H_1(Sp(2g, \mathbb{Z}/2^k\mathbb{Z}); \mathfrak{sp}_{2g}(2)) = 0$ or not for $k \geq 2$. However this is true when $k = 1$ and we derive:

Corollary 5.2. *Assume Theorem 1.6 holds. Then $H_2(Sp(2g, \mathbb{Z}/4\mathbb{Z})) \in \{0, \mathbb{Z}/2\mathbb{Z}\}$, for all $g \geq 4$.*

Proof. Proposition 3.3 implies that $H_2(Sp(2g, \mathbb{Z}/4\mathbb{Z}))$ is cyclic, for $g \geq 4$. Since $H_2(Sp(2g, \mathbb{Z}/2\mathbb{Z})) = 0$, and $H_1(Sp(2g, \mathbb{Z}/2\mathbb{Z}), \mathfrak{sp}_{2g}(2)) = 0$ from Putman's theorem 5.1, the only non-zero term of the second page of the Hochschild-Serre spectral sequence above computing the cohomology of $Sp(2g, \mathbb{Z}/4\mathbb{Z})$ is $H_2(\mathfrak{sp}_{2g}(2))_{Sp(2g, \mathbb{Z}/2\mathbb{Z})}$. Then, by Theorem 1.6 the rank of $H_2(Sp(2g, \mathbb{Z}/4\mathbb{Z}))$ is at most 1, which proves the claim. \square

5.2 Generators for the module $\mathfrak{sp}_{2g}(p)$

We describe first a small set of generators of $\mathfrak{sp}_{2g}(p)$ as an $Sp(2g, \mathbb{Z})$ -module. Denote by $\mathfrak{M}_g(R)$ the R -module of g -by- g matrices with entries from the ring R . A direct computation shows that a matrix $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathfrak{M}_{2g}(\mathbb{Z}/p\mathbb{Z})$ written by blocks is in $\mathfrak{sp}_{2g}(p)$ if and only if $A + D^\top \equiv 0 \pmod{p}$ and both B and C are symmetric matrices. It will be important for our future computations to keep in mind that the subgroup $GL(g, \mathbb{Z}) \subset Sp(2g, \mathbb{Z})$ preserves this decomposition into blocks. From this description we immediately get a set of generators of $\mathfrak{sp}_{2g}(p)$ as an additive group. Recall that $e_{ij} \in \mathfrak{M}_g(R)$ denotes the elementary matrix whose only non-zero coefficient is 1 at the place ij . Define now the following matrices in $\mathfrak{sp}_{2g}(p)$:

$$u_{ij} = \begin{pmatrix} 0 & e_{ij} + e_{ji} \\ 0 & 0 \end{pmatrix}, \quad u_{ii} = \begin{pmatrix} 0 & e_{ii} \\ 0 & 0 \end{pmatrix}, \quad l_{ij} = \begin{pmatrix} 0 & 0 \\ e_{ij} + e_{ji} & 0 \end{pmatrix}, \quad l_{ii}(q) = \begin{pmatrix} 0 & 0 \\ e_{ii} & 0 \end{pmatrix} \quad (42)$$

$$r_{ij} = \begin{pmatrix} e_{ij} & 0 \\ 0 & -e_{ji} \end{pmatrix}, \quad n_{ii}(q) = \begin{pmatrix} e_{ii} & 0 \\ 0 & -e_{ii} \end{pmatrix} \quad (43)$$

These correspond naturally to the projections of the generators of $Sp(2g, \mathbb{Z}, p)$ described in Proposition 3.3. Therefore we have:

Proposition 5.1. *As an $Sp(2g, \mathbb{Z}/p\mathbb{Z})$ -module, $\mathfrak{sp}_{2g}(p)$ is generated by u_{ij} , u_{ii} , l_{ij} and l_{ii} , where $i, j \in \{1, 2, \dots, g\}$.*

And as $GL_{2g}(\mathbb{Z}/p\mathbb{Z})$ -module we have:

Lemma 5.1. *Let $\text{Sym}_g(\mathbb{Z}/p\mathbb{Z}) \subset \mathfrak{M}_g(\mathbb{Z}/p\mathbb{Z})$ denotes the submodule of symmetric matrices. We have an identification of $GL(g, \mathbb{Z})$ -modules:*

$$\mathfrak{sp}_{2g}(p) = \mathfrak{M}_g(\mathbb{Z}/p\mathbb{Z}) \oplus \text{Sym}_g(\mathbb{Z}/p\mathbb{Z}) \oplus \text{Sym}_g(\mathbb{Z}/p\mathbb{Z})$$

The action of $GL(p, \mathbb{Z})$ on $\mathfrak{M}_g(\mathbb{Z}/p\mathbb{Z})$ is by conjugation, the action on the first copy $\text{Sym}_g(\mathbb{Z}/p\mathbb{Z})$ is given by $x \cdot S = xS^t x$ and on the second copy $\text{Sym}_g(\mathbb{Z}/p\mathbb{Z})$ is given by $x \cdot S = {}^t x^{-1} S x^{-1}$.

A set of generators for $\mathfrak{M}_g(\mathbb{Z}/p\mathbb{Z})$ is given by the set of elements r_{ij} and n_{ii} , $1 \leq i, j \leq g$, $i \neq j$. The two copies of $\text{Sym}_g(\mathbb{Z}/p\mathbb{Z})$ are generated by the matrices l_{ij} and u_{ij} respectively, where $1 \leq i, j \leq g$.

5.3 Proof of Theorem 1.6

Notice first that as the action of $Sp(2g, \mathbb{Z}/p^k\mathbb{Z})$ factors through $Sp(2g, \mathbb{Z}/p\mathbb{Z})$ via the mod p^{k-1} reduction map, for any $k \geq 2$ we have $H_2(\mathfrak{sp}_{2g}(p); \mathbb{Z})_{Sp(2g, \mathbb{Z}/p^k\mathbb{Z})} \simeq H_2(\mathfrak{sp}_{2g}(p))_{Sp(2g, \mathbb{Z}/p\mathbb{Z})}$. Also, as $\mathfrak{sp}_{2g}(p)$ is an abelian group there is a canonical isomorphism:

$$H_2(\mathfrak{sp}_{2g}(p)) = \wedge^2 \mathfrak{sp}_{2g}(p). \quad (44)$$

The group $\wedge^2 \mathfrak{sp}_{2g}(p)$ is generated by the set of exterior powers of pairs of generators given in Proposition 5.1, which we split naturally into three disjoint subsets:

1. The subset $S \wedge S$ of exterior powers $l_{ij} \wedge u_{kl}, l_{ij} \wedge l_{kl}, u_{ij} \wedge u_{kl}$ and
2. the subset $S \wedge M$ of exterior power $l_{ij} \wedge n_{kk}, u_{ij} \wedge n_{kk}, l_{ij} \wedge r_{kl}$,
3. the subset $M \wedge M$ of exterior powers $r_{ij} \wedge r_{kl}, r_{ij} \wedge n_{kk}$,

We will first show that the image of $S \wedge S$ and $S \wedge M$ is 0 in $\wedge^2 \mathfrak{sp}_{2g}(p)$, and in a second time we will show how the $\mathbb{Z}/2\mathbb{Z}$ factor appears in the image of $M \wedge M$. It will also be clear from the proof why there is no such non-trivial element in odd characteristic.

We use constantly the trivial fact that the action of $Sp(2g, \mathbb{Z}/p\mathbb{Z})$ is trivial on the co-invariants module. So to show the nullity of the image of a generator it is enough to show that in each orbit of a generating element of $S \wedge M$ or $S \wedge M$ there is the 0 element. We will in particular heavily use the fact that the symmetric group $\mathfrak{S}_g \subset GL(g, \mathbb{Z}/p\mathbb{Z}) \subset Sp(2g, \mathbb{Z}/p\mathbb{Z})$ acts on the basis elements by permuting the indices. Notice that the symmetric group action respects the above partition into three sets of elements. To emphasize when we use such a permutation to identify two elements in the co-invariant module we will use the notation \doteq instead of $=$.

Nullity of the generators in $S \wedge S$. Picking one representative in each \mathfrak{S}_g -orbit we are left with the following elements. Here “Type” refers to the number of distinct indexes that appear in the wedge, as this is the only thing that really matters. Of course type IV elements appear only for $g \geq 4$.

1. Type I: $u_{11} \wedge l_{11}$.
2. Type II: $u_{11} \wedge u_{22}, l_{11} \wedge l_{22}, u_{11} \wedge l_{22}, u_{11} \wedge u_{12}, l_{11} \wedge l_{12}, u_{12} \wedge l_{12}, u_{12} \wedge l_{22}, u_{11} \wedge l_{12}$.
3. Type III: $u_{11} \wedge u_{23}, l_{11} \wedge l_{23}, u_{12} \wedge u_{23}, l_{12} \wedge l_{23}, u_{11} \wedge l_{23}, l_{11} \wedge u_{23}, u_{12} \wedge l_{23}$.
4. Type IV: $u_{12} \wedge u_{34}, l_{12} \wedge l_{34}, u_{12} \wedge l_{34}$.

Using the fact that $J_g \cdot u_{ij} = -l_{ij}$, one can identify some generators in M , for instance $u_{11} \wedge u_{22} = l_{11} \wedge l_{22}$, and we are left with:

1. Type I: $u_{11} \wedge l_{11}$.
2. Type II: $u_{11} \wedge u_{22}, u_{11} \wedge l_{22}, u_{11} \wedge u_{12}, u_{11} \wedge l_{12}, u_{12} \wedge l_{12}, u_{12} \wedge l_{22}$.
3. Type III: $u_{11} \wedge u_{23}, u_{12} \wedge u_{23}, u_{11} \wedge l_{23}, u_{12} \wedge l_{23}$.
4. Type IV: $u_{12} \wedge u_{34}, u_{12} \wedge l_{34}$.

We consider now two families of elements in the symplectic group:

$$\tau_{ij}^u = \begin{pmatrix} 1_g & e_{ii} + e_{jj} \\ 0 & 1_g \end{pmatrix}, \quad \tau_{ij}^l = \begin{pmatrix} 1_g & 0 \\ e_{ii} + e_{jj} & 1_g \end{pmatrix}$$

A direct computation shows that:

$$\tau_{ij}^u \cdot u_{kl} = u_{kl}, \quad \tau_{ij}^u \cdot r_{ij} = r_{ij} - u_{ij}, \text{ for all } i, j, k, l \quad (45)$$

$$\tau_{ij}^l \cdot l_{kl} = l_{kl}, \quad \tau_{ij}^l \cdot r_{ij} = r_{ij} + l_{ij}, \text{ for all } i, j, k, l \quad (46)$$

In particular, we obtain:

$$\tau_{ij}^u \cdot (u_{kl} \wedge r_{ij}) = u_{kl} \wedge r_{ij} - u_{kl} \wedge u_{ij} \quad (47)$$

and

$$\tau_{ij}^l \cdot (l_{kl} \wedge r_{ij}) = l_{kl} \wedge r_{ij} + l_{kl} \wedge l_{ij} \quad (48)$$

And this shows that all elements of the form $u \wedge u$ or $l \wedge l$ vanish except possibly for $u_{11} \wedge u_{22}$. We are left then with:

1. Type I: $u_{11} \wedge l_{11}$.
2. Type II: $u_{11} \wedge u_{22}$, $u_{11} \wedge l_{22}$, $u_{11} \wedge l_{12}$, $u_{12} \wedge l_{12}$, $u_{12} \wedge l_{22}$.
3. Type III: $u_{11} \wedge l_{23}$, $u_{12} \wedge l_{23}$.
4. Type IV: $u_{12} \wedge l_{34}$.

Consider the exchange map E_{ij} which corresponds at the level of the underlying symplectic basis to a transposition inside two couples of basis elements $a_i \leftrightarrow -b_i$ and $a_j \leftrightarrow -b_j$, leaving the other basis elements untouched. By construction, we have $E_{ij} \cdot u_{ij} = -l_{ij}$, $E_{ij} \cdot u_{ii} = -l_{ii}$, $E_{ij} \cdot u_{jj} = -l_{jj}$ and $E_{ij} \cdot u_{kl} = u_{kl}$ if $\{i, j\} \cap \{k, l\} = \emptyset$. For instance, we have: $E_{23} \cdot (u_{11} \wedge l_{23}) = u_{11} \wedge u_{23} \doteq u_{11} \wedge l_{23}$, $E_{12} \cdot (u_{12} \wedge l_{22}) = -l_{12} \wedge u_{22} \doteq u_{11} \wedge l_{12}$ and $E_{23} \cdot (u_{11} \wedge u_{22}) = -u_{11} \wedge l_{22}$. Thus we are left with:

1. Type I: $u_{11} \wedge l_{11}$.
2. Type II: $u_{11} \wedge l_{22}$, $u_{11} \wedge l_{12}$, $u_{12} \wedge l_{12}$.

We now use the maps A_{ij} defined in the proof of Lemma 3.3. We compute:

1. $A_{12}(u_{11} \wedge l_{22}) = u_{11} \wedge (l_{11} + l_{22} - l_{12})$. So that $u_{11} \wedge l_{11} = u_{11} \wedge l_{12}$.
2. $A_{12}(u_{12} \wedge l_{22}) = u_{12} \wedge (l_{11} + l_{22} + l_{12})$, so that $-u_{12} \wedge l_{12} = u_{12} \wedge l_{11} = E_{12}(u_{12} \wedge l_{11}) = l_{12} \wedge u_{11} = -u_{11} \wedge l_{12}$.
3. $A_{12}(u_{22} \wedge l_{22}) = u_{22} \wedge (l_{11} + l_{22} + l_{12})$. So that $u_{11} \wedge l_{22} \doteq u_{22} \wedge l_{11} = u_{22} \wedge l_{12} \doteq u_{11} \wedge l_{12}$.

Finally,

$$A_{23}(u_{13} \wedge l_{12}) = (u_{13} - u_{12}) \wedge l_{12},$$

and we conclude that $u_{12} \wedge l_{12} = 0$, which eliminates the last four remaining elements.

Nullity of the generators in $S \wedge M$. We will use again the maps τ_{ij}^u and τ_{kl}^l . A direct computation shows that:

$$\tau_{ij}^l \cdot u_{ij} = u_{jj} - l_{jj} - n_{jj}, \text{ for all } i \neq j \quad (49)$$

and

$$\tau_{ij}^u \cdot l_{jk} = r_{jk} + l_{jk}, \text{ for pairwise distinct } i, j, k \quad (50)$$

Applying the first map to the elements of the form $l_{st} \wedge u_{ij}$ we conclude that for all s, t, j we have $l_{st} \wedge n_{jj} = 0$. And applying the second map to the elements of the form $u_{st} \wedge l_{jk}$ we conclude that for all s, t, j, k such that $s \neq t$ and $j \neq k$ we have $u_{st} \wedge r_{jk} = 0$. As a direct computation shows that $J_g n_{ii} = -n_{ii}$ and $J \cdot r_{ij} = -r_{ji}$, applying the map J_g to the above trivial elements we conclude that all elements are trivial in $S \wedge M$.

Image of $M \wedge M$. First we will do a small detour through bilinear forms on matrices. Until the very end we work on an arbitrary field \mathbb{K} . Denote by $\mathbf{1}_n$ the identity matrix. Recall that, if $i \neq j$, then $\mathbf{1}_n + e_{ij}$ has inverse $\mathbf{1}_n - e_{ij}$ and that elementary matrices multiply according to the rule $e_{ij}e_{st} = \delta_{js}e_{it}$. We start by a very classical result:

Lemma 5.2. *Let tr denote the trace map. Then for any field \mathbb{K} and any integer n the homomorphism:*

$$\begin{array}{ccc} M_n(\mathbb{K}) & \rightarrow & \text{Hom}(M_n(\mathbb{K}), \mathbb{K}) \\ A & \mapsto & B \rightsquigarrow \text{tr}(AB) \end{array}$$

is an isomorphism.

A little less classical is:

Theorem 5.3. *The \mathbb{K} -vector space $\text{Hom}_{GL_n(\mathbb{K})}(\mathfrak{M}_n(\mathbb{K}), \mathfrak{M}_n(\mathbb{K}))$ has dimension 2. It is generated by the identity map $Id_{\mathfrak{M}_n(\mathbb{K})}$ and by the map $\Psi(M) = \text{tr}(M)\mathbf{1}_n$.*

Proof. It is easy to check that the two equivariant maps $Id_{\mathfrak{M}_n(\mathbb{K})}$ and Ψ are linearly independent. Indeed, evaluating a linear dependence relation $\alpha Id_{\mathfrak{M}_n(\mathbb{K})} + \beta \Psi = 0$ on e_{12} one gets $\alpha = 0 = \beta$.

Fix an arbitrary $\phi \in \text{Hom}_{GL_n(\mathbb{K})}(\mathfrak{M}_n(\mathbb{K}), \mathfrak{M}_n(\mathbb{K}))$. Denote by $A = (a_{ij})$ the matrix $\phi(e_{11})$. Consider two integers $1 < s, t \leq n$. From the equality $(\mathbf{1}_n + e_{st})e_{11}(\mathbf{1}_n - e_{st}) = e_{11}$ we deduce that:

$$\phi(e_{11}) = (\mathbf{1}_n + e_{st})\phi(e_{11})(\mathbf{1}_n - e_{st}) \quad (51)$$

$$= \phi(e_{11}) + e_{st}\phi(e_{11}) - \phi(e_{11})e_{st} - e_{st}\phi(e_{11})e_{st} \quad (52)$$

$$= \phi(e_{11}) + \sum_{1 \leq j \leq n} a_{tj}e_{sj} - \sum_{1 \leq i \leq n} a_{is}e_{it} - a_{ts}e_{st} \quad (53)$$

Therefore, for $1 < s, t \leq n$ we have:

$$\sum_{1 \leq j \leq n} a_{tj}e_{sj} - \sum_{1 \leq i \leq n} a_{is}e_{it} - a_{ts}e_{st} = 0 \quad (54)$$

The first term in this sum is a matrix with only one non-zero row, the second a matrix with one non-zero column and the third a matrix with a single (possibly) non-zero entry. The only common entry for this three matrices appears for $j = t$ and $i = s$, where we get the equation $a_{tt} - a_{ss} - a_{ts} = 0$. Otherwise, $a_{tj} = 0$, for all $j \neq t$, and $a_{is} = 0$, for all $i \neq s$. Observe that, in particular, $a_{st} = 0$. Summing up, either in the column s or in the row t of the matrix A , the only possible non-zero elements are those that appear in the equation $a_{tt} - a_{ss} - a_{ts} = 0$.

Inverting the roles of s and t one gets that $a_{ts} = 0$, and letting s and t vary one deduces that $A = \phi(e_{ii})$ is of the form $\lambda e_{11} + \mu \sum_{i=2}^n e_{ii}$ for two scalars $\lambda, \mu \in \mathbb{K}$.

Let T_{ij} be the invertible matrix that interchanges the basis vectors i and j . Then $T_{ij}e_{ii}T_{ij} = e_{jj}$, $T_{ij}e_{jj}T_{ij} = e_{ii}$ and $T_{ij}e_{kk}T_{ij} = e_{kk}$ for $k \neq i$ and $k \neq j$. Therefore, $\phi(e_{jj}) = \phi(T_{1j}e_{11}T_{1j}) = T_{1j}\phi(e_{11})T_{1j}$. And from the description of $\phi(e_{ii})$ one gets:

$$\phi(e_{jj}) = \lambda e_{jj} + \sum_{i \neq j} \mu e_{ii}, \text{ for all } 1 \leq j \leq n.$$

From the relation $(\mathbf{1}_n + e_{ij})e_{ii}(\mathbf{1}_n - e_{ij}) = e_{ii} - e_{ij}$ we get:

$$\phi((\mathbf{1}_n + e_{ij})e_{ii}(\mathbf{1}_n - e_{ij})) = \phi(e_{ii}) - \phi(e_{ij}) \quad (55)$$

$$= (\mathbf{1}_n + e_{ij})\phi(e_{ii})(\mathbf{1}_n - e_{ij}) \quad (56)$$

$$= \phi(e_{ii}) + e_{ij}\phi(e_{ii}) - \phi(e_{ii})e_{ij} - e_{ij}\phi(e_{ii})e_{ij}, \quad (57)$$

and in particular:

$$\phi(e_{ij}) = -e_{ij}\phi(e_{ii}) + \phi(e_{ii})e_{ij} + e_{ij}\phi(e_{ii})e_{ij} \quad (58)$$

$$= -\mu e_{ij} + \lambda e_{ij} \quad (59)$$

$$= (\lambda - \mu)e_{ij} \quad (60)$$

This shows that ϕ is completely determined by $\phi(e_{ii})$ and that $\text{Hom}_{GL_n(\mathbb{K})}(\mathfrak{M}_n(\mathbb{K}), \mathfrak{M}_n(\mathbb{K}))$ has dimension at most 2. Observe that the identity map $Id_{\mathfrak{M}_n(\mathbb{K})}$ corresponds to $\lambda = 1, \mu = 0$ and that Ψ corresponds to $\lambda = \mu = 1$. \square

From this two lemmas we deduce the result that will save us from lengthy computations:

Proposition 5.2. *For any field \mathbb{K} the vector space of bilinear forms on $\mathfrak{M}_n(\mathbb{K})$ invariant under conjugation by $GL_n(\mathbb{K})$ has as basis the bilinear maps $(A, B) \mapsto \text{tr}(A)\text{tr}(B)$ and $(A, B) \mapsto \text{tr}(AB)$. If $\text{char}(\mathbb{K}) \neq 2$, the subspace of alternating bilinear forms is trivial. If $\text{char}(\mathbb{K}) = 2$ the space of bilinear alternating forms is generated by the form $(A, B) \mapsto \text{tr}(A)\text{tr}(B) + \text{tr}(AB)$.*

Consider now the canonical map

$$\wedge^2(\mathfrak{M}_g(\mathbb{Z}/p\mathbb{Z})) \rightarrow \wedge^2(\mathfrak{M}_g(\mathbb{Z}/p\mathbb{Z}))_{GL_g(\mathbb{Z}/p\mathbb{Z})} \rightarrow \wedge^2(\mathfrak{sp}_{2g}(p))_{GL_g(\mathbb{Z}/p\mathbb{Z})} \rightarrow \wedge^2(\mathfrak{sp}_{2g}(p))_{Sp(2g, \mathbb{Z}/p\mathbb{Z})}. \quad (61)$$

By construction its image is the image of $M \wedge M$ in $\wedge^2(\mathfrak{sp}_{2g}(p))_{Sp(2g, \mathbb{Z}/2\mathbb{Z})}$. By Proposition 5.2, it is 0 if p is odd and it is at most $\mathbb{Z}/2\mathbb{Z}$ if $p = 2$. To detect this $\mathbb{Z}/2\mathbb{Z}$ factor, first notice that by the above exact sequence it has to be the class of $n_{11} \wedge n_{22}$, for the unique $GL_g(\mathbb{Z})$ -invariant alternating form on $\mathfrak{M}_g(\mathbb{Z}/2\mathbb{Z})$ does not vanish on this element. Now, fix a symplectic basis $\{a_i, b_i\}_{1 \leq i \leq g}$ of \mathbb{Z}^{2g} . Then, the $2g + 1$ transvections along the elements $a_i, b_j - b_{j+1}$ for $1 \leq i \leq g$ and $1 \leq j \leq g - 1$, b_g and b_3 generate $Sp(2g, \mathbb{Z}/2\mathbb{Z})$, for instance because they are the canonical images of the Lickorish Dehn twists generators of the mapping class group. One checks directly, using all elements we know they vanish in $\wedge^2(\mathfrak{sp}_{2g}(2))_{Sp(2g, \mathbb{Z}/2\mathbb{Z})}$, that the action of these generators on $n_{11} \wedge n_{22}$ is trivial. This finishes our proof.

Remark 5.1. It is clear from the proof that the copy $\mathbb{Z}/2\mathbb{Z}$ we have detected is stable, in the sense that the homomorphism $\wedge^2(\mathfrak{sp}_{2g}(2))_{Sp(2g, \mathbb{Z}/2\mathbb{Z})} \rightarrow \wedge^2(\mathfrak{sp}_{2g+2}(2))_{Sp(2g+2, \mathbb{Z}/2\mathbb{Z})}$ is an isomorphism, for all $g \geq 3$, since both are detected by the obvious stable element $n_{11} \wedge n_{22}$.

A Appendix: Weil representations using theta functions

A.1 Weil representations at level k , for even k following [16, 23, 17]

Let \mathcal{S}_g be the Siegel space of $g \times g$ symmetric matrices Ω of complex entries having the imaginary part $\text{Im}\Omega$ positive defined. There is a natural $Sp(2g, \mathbb{Z})$ action on $\mathbf{C}^g \times \mathcal{S}_g$ given by

$$\gamma \cdot (z, \Omega) = (((C\Omega + D)^\top)^{-1})z, (A\Omega + B)(C\Omega + D)^{-1}. \quad (62)$$

The dependence of the classical theta function $\theta(z, \Omega)$ on Ω is expressed by a functional equation which describes its behavior under the action of $Sp(2g, \mathbb{Z})$. Let $\Gamma(1, 2)$ be the so-called theta group consisting of elements $\gamma \in Sp(2g, \mathbb{Z})$ which preserve the quadratic form

$$Q(n_1, n_2, \dots, n_{2g}) = \sum_{i=1}^g n_i n_{i+g} \in \mathbb{Z}/2\mathbb{Z},$$

which means that $Q(\gamma(x)) = Q(x)(\text{mod } 2)$. We represent any element $\gamma \in Sp(2g, \mathbb{Z})$ as $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ where A, B, C, D are $g \times g$ matrices. Then $\Gamma(1, 2)$ may be alternatively described as the set of those elements γ having the property that the diagonals of $A^\top C$ and $B^\top D$ are even. Let \langle , \rangle denote the standard hermitian product on \mathbb{C}^{2g} . The functional equation, as stated in [55] is:

$$\theta((C\Omega + D)^\top z, (A\Omega + B)(C\Omega + D)^{-1}) = \zeta_\gamma \det(C\Omega + D)^{1/2} \exp(\pi\sqrt{-1}\langle z, (C\Omega + D)^{-1}Cz \rangle) \theta(z, \Omega),$$

for $\gamma \in \Gamma(1, 2)$, where ζ_γ is a certain 8th root of unity.

If $g = 1$ we may suppose that $C > 0$ or $C = 0$ and $D > 0$ so the imaginary part $\text{Im}(C\Omega + D) \geq 0$ for Ω in the upper half plane. Then we will choose the square root $(C\Omega + D)^{1/2}$ in the first quadrant. Now we can express the dependence of ζ_γ on γ as follows:

1. for even C and odd D , $\zeta_\gamma = \sqrt{-1}^{(D-1)/2} (\frac{C}{|D|})$,
2. for odd C and even D , $\zeta_\gamma = \exp(-\pi\sqrt{-1}C/4)(\frac{D}{C})$,

where $(\frac{x}{y})$ is the usual Jacobi symbol ([29]).

For $g > 1$ it is less obvious to describe this dependence. We fix first the choice of the square root of $\det(C\Omega + D)$ in the following manner: let $\det^{\frac{1}{2}}\left(\frac{Z}{\sqrt{-1}}\right)$ be the unique holomorphic function on \mathcal{S}_g satisfying

$$\left(\det^{\frac{1}{2}}\left(\frac{Z}{\sqrt{-1}}\right)\right)^2 = \det\left(\frac{Z}{\sqrt{-1}}\right),$$

and taking in $\sqrt{-1}\mathbf{1}_g$ the value 1. Next define

$$\det^{\frac{1}{2}}(C\Omega + D) = \det^{\frac{1}{2}}(D)\det^{\frac{1}{2}}\left(\frac{\Omega}{\sqrt{-1}}\right)\det^{\frac{1}{2}}\left(\frac{-\Omega^{-1} - D^{-1}C}{\sqrt{-1}}\right),$$

where the square root of $\det(D)$ is taken to lie in the first quadrant. Using this convention we may express ζ_γ as a Gauss sum for invertible D (see [15], p.26-27)

$$\zeta_\gamma = \det^{-\frac{1}{2}}(D) \sum_{l \in \mathbb{Z}^g / D\mathbb{Z}^g} \exp(\pi\sqrt{-1}\langle l, BD^{-1}l \rangle), \quad (63)$$

and in particular we recover the formula from above for $g = 1$. On the other hand for $\gamma = \begin{pmatrix} A & 0 \\ 0 & (A^\top)^{-1} \end{pmatrix}$ we have $\zeta_\gamma = (\det A)^{-1/2}$. When $\gamma = \begin{pmatrix} 1_g & B \\ 0 & 1_g \end{pmatrix}$ then the multiplier system is trivial, $\zeta_\gamma = 1$, and eventually for $\gamma = \begin{pmatrix} 0 & -1_g \\ 1_g & 0 \end{pmatrix}$ we have $\zeta_\gamma = \exp(\pi\sqrt{-1}g/4)$. Actually this data determines completely ζ_γ .

Denote $\det^{\frac{1}{2}}(C\Omega + D) = j(\gamma, \Omega)$. Then there exists a map

$$s : \mathrm{Sp}(2g, \mathbb{R}) \times \mathrm{Sp}(2g, \mathbb{R}) \longrightarrow \{-1, 1\}$$

satisfying

$$j(\gamma_1\gamma_2, \Omega) = s(\gamma_1, \gamma_2)j(\gamma_1, \gamma_2\Omega)j(\gamma_2, \Omega).$$

We recall that a multiplier system ([15]) for a subgroup $\Gamma \subset \mathrm{Sp}(2g, \mathbb{R})$ is a map $m : \Gamma \longrightarrow \mathbf{C}^*$ such that

$$m(\gamma_1) = s(\gamma_1, \gamma_2)m(\gamma_1)m(\gamma_2).$$

An easy remark is that, once a multiplier system m is chosen, the product $A(\gamma, \Omega) = m(\gamma)j(\gamma, \Omega)$ verifies the cocycle condition

$$A(\gamma_1\gamma_2, \Omega) = A(\gamma_1, \gamma_2\Omega)A(\gamma_2, \Omega),$$

for $\gamma_i \in \Gamma$. Then another formulation of the dependence of ζ_γ on γ is to say that it is the multiplier system defined on $\Gamma(1, 2)$. Remark that using the congruence subgroups property due to Mennicke ([49, 50]) and Bass, Milnor and Serre ([3]) any two multiplier systems defined on a subgroup of the theta group are identical on some congruence subgroup.

Consider now the level k theta functions. For $m \in (\mathbb{Z}/k\mathbb{Z})^g$ these are defined by

$$\theta_m(z, \Omega) = \sum_{l \in m + k\mathbb{Z}^g} \exp\left(\frac{\pi\sqrt{-1}}{k}(\langle l, \Omega l \rangle + 2\langle l, z \rangle)\right) \quad (64)$$

or, equivalently, by

$$\theta_m(z, \Omega) = \theta(m/k, 0)(kz, k\Omega).$$

where $\theta(*, *)$ are the theta functions with rational characteristics ([55]) given by

$$\theta(a, b)(z, \Omega) = \sum_{l \in \mathbb{Z}^g} \exp\left(\frac{\pi\sqrt{-1}}{k}(\langle l + a, \Omega(l + a) \rangle + 2\langle l + a, z + b \rangle)\right) \quad (65)$$

for $a, b \in \mathbb{Q}^g$. Obviously $\theta(0, 0)$ is the usual theta function.

Let us denote by $R_8 \subset \mathbf{C}$ the group of 8^{th} roots of unity. Then R_8 becomes also a subgroup of the unitary group $U(n)$ acting by scalar multiplication. Consider also the theta vector of level k :

$$\Theta_k(z, \Omega) = (\theta_m(z, \Omega))_{m \in (\mathbb{Z}/k\mathbb{Z})^g}.$$

Proposition A.1 ([16, 23, 17]). *The theta vector satisfies the following functional equation:*

$$\Theta_k(\gamma \cdot (z, \Omega)) = \zeta_\gamma \det(C\Omega + D)^{1/2} \exp(k\pi\sqrt{-1}\langle z, (C\Omega + D)^{-1}Cz \rangle) \rho_g(\gamma)(\Theta_k(z, \Omega)) \quad (66)$$

where

1. γ belongs to the theta group $\Gamma(1, 2)$ if k is odd and to $\mathrm{Sp}(2g, \mathbb{Z})$ elsewhere.
2. $\zeta_\gamma \in R_8$ is the (fixed) multiplier system described above.
3. $\rho_g : \Gamma(1, 2) \longrightarrow U(V_g(k))$ is a group homomorphism. For even k the corresponding map $\rho_g : \mathrm{Sp}(2g, \mathbb{Z}) \longrightarrow U(V_g(k))$ becomes a group homomorphism (denoted also by ρ_g when no confusion arises) when passing to the quotient $U(V_g(k))/R_8$.
4. ρ_g is determined by the formulas (1-3).

Remark A.1. This result is stated also in [36] for some modified theta functions but in less explicit form.

A.2 Linearizability of Weil representations for odd level k

The proof for the linearizability of the Weil representation associated to $\mathbb{Z}/k\mathbb{Z}$ for odd k was first given by A.Andler (see [1], Appendix AIII) and then extended to other local rings in [11]. Let $\eta : \mathrm{Sp}(2g, \mathbb{Z}) \times \mathrm{Sp}(2g, \mathbb{Z}) \rightarrow R_8 \subset U(1)$ be the cocycle determined by the Weil representation associated to $\mathbb{Z}/k\mathbb{Z}$. The image S^2 of $\begin{pmatrix} -1_g & 0 \\ 0 & -1_g \end{pmatrix}$ is the involution

$$S^2\theta_m = \theta_{-m}, \quad m \in (\mathbb{Z}/k\mathbb{Z})^g$$

Thus $S^4 = 1$ and S^2 has eigenvalues $+1$ and -1 . Moreover S^2 is central and hence the Weil representation splits according to the eigenspaces decomposition. Further, the determinant of each factor representation is a homogeneous function whose degree is the respective dimension of the factor. Therefore we could express for each one of the two factors, η to the power the dimension of the respective factor as a determinant cocycle. The difference between the two factors dimensions is the trace of S^2 , namely 1 for odd k and 2^g for even k . This implies that η for odd k and η^{2^g} , for even k is a boundary cocycle. However $\eta^8 = 1$ and hence for even k and $g \geq 3$ this method could not give any non-trivial information about η .

References

- [1] A.Andler and S.Ramanan, Moduli of abelian varieties, Lect. Notes. Math. 1644, 1996.
- [2] J. Barge and J. Lannes, Suites de Sturm, indice de Maslov et périodicité de Bott, [Sturm sequences, Maslov index and Bott periodicity], *Progress in Mathematics*, 267. Birkhäuser Verlag, Basel, 2008. viii+199 pp.
- [3] H. Bass, J. Milnor and J.-P. Serre, *Solution of the congruence subgroup problem for SL_n ($n \geq 3$) and Sp_{2n} ($n \geq 2$)*, Inst. Hautes Études Sci. Publ. Math. No. 33, 1967, 59–137.
- [4] R. Beyl, *The Schur multiplicator of $SL(2, \mathbb{Z}/m\mathbb{Z})$ and the congruence subgroup property*, Math.Z. 91(1986), 23–42.
- [5] A. Borel, *Stable real cohomology of arithmetic groups*, Ann. Sci. École Norm. Sup. (4) 7 (1974), 235–272.
- [6] A. Borel and J.P. Serre, *Cohomologie à supports compacts des immeubles de Bruhat-Tits: applications à la cohomologie des groupes S -arithmétiques*, C.R. Acad. Sci. Paris 272 (1971), 110–113.
- [7] A. Borel, *Cohomologie réelle stable de groupes S -arithmétiques classiques*, C. R. Acad. Sci. Paris Sér. A-B 274 (1972), A1700–A1702.
- [8] K. Brown, Cohomology of groups, Graduate Texts in Math., Springer-Verlag, 1994.
- [9] A. Brownstein and R. Lee, *Cohomology of the symplectic group $\mathrm{Sp}_4(\mathbb{Z})$. I. The odd torsion case*, Trans. Amer. Math. Soc. 334 (1992), 575–596.
- [10] A. Brownstein and R. Lee, *Cohomology of the symplectic group $\mathrm{Sp}(4, \mathbb{Z})$. II. Computations at the prime 2*, Michigan Math. J. 41 (1994), 181–208.
- [11] G. Cliff, D. McNeilly and F. Szechtman, *Weil representations of symplectic groups over rings*, J. London Math. Soc. (2) 62 (2000), 423–436.
- [12] P. Deligne, *Extensions centrales non résiduellement finies de groupes arithmétiques*, C. R. Acad. Sci. Paris Sér. A-B 287 (1978), no. 4, A203–A208.
- [13] R. K. Dennis and M. R. Stein, *The functor K : a survey of computations and problems*, Algebraic K-Theory II, Lecture Notes in Math., vol. 342, Springer-Verlag, Berlin and New York, 1973, pp. 243–280.
- [14] R. K. Dennis and M. R. Stein, *K_2 of discrete valuation rings*, Adv. in Math. 18 (1975), 182–238.

- [15] J. Freitag, Theta functions. Lect. Notes in Math. 1487, Springer Verlag, 1987.
- [16] L. Funar, *Représentations du groupe symplectique et variétés de dimension 3*, C. R. Acad. Sci. Paris Sér. I Math. 316 (1993), 1067–1072.
- [17] L. Funar, *Some abelian invariants of 3-manifolds*, Rev. Roumaine Math. Pures Appl. 45 (2000), 825–861.
- [18] L. Funar, *Two questions on mapping class groups*, Proc. Amer. Math. Soc. 139 (2011), 375–382.
- [19] L. Funar, *Zariski density and finite quotients of mapping class groups*, Int. Math. Res. Not. 2012, doi:10.1093/imrn/rns097.
- [20] L. Funar and R. Kashaev, *Centrally extended mapping class groups from quantum Teichmüller theory*, 23p., arXiv:1003.5365.
- [21] S. Gervais, *Presentation and central extensions of mapping class groups*, Trans. Amer. Math. Soc. 348 (1996), 3097–3132.
- [22] P. Gilmer and G. Masbaum, *Integral lattices in TQFT*, Ann. Sci. École Norm. Sup. (4) 40 (2007), 815–844.
- [23] T. Goto, *The topological invariant of three-manifolds based on the U(1) gauge theory*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 39 (1992), 169–184.
- [24] E. Grossman, *On the residual finiteness of certain mapping class groups*, J. London Math. Soc. (2) 9 (1974/75), 160–164.
- [25] F. Grunewald, A. Jaikin-Zapirain and P.A. Zalesskii, *Cohomological goodness and the profinite completion of Bianchi groups*, Duke Math. J. 144 (2008), no. 1, 53–72.
- [26] S. Gurevich and R. Hadani, *The Weil representation in characteristic two*, Adv. in Math. 230 (2012), no. 3, 894–926.
- [27] S. Gurevich, R. Hadani and R. Howe, *Quadratic reciprocity and the sign of the Gauss sum via the finite Weil representation*, Int. Math. Res. Not. 2010, no. 19, 3729–3745.
- [28] J.H. Hannay and M.V. Berry, *Quantization of linear maps on a torus-Fresnel diffraction by a periodic grating*, Phys. D 1 (1980), no. 3, 267–290.
- [29] G. Hardy and E. Wright, An introduction to the theory of numbers, Oxford at the Clarendon Press, 1979.
- [30] J. Harer, *The second homology group of the mapping class group of an orientable surface*, Invent. Math. 72 (1983), 221–239.
- [31] R. Hain and M. Matsumoto, *Relative pro- ℓ completions of mapping class groups*, J. Algebra 321 (2009), 3335–3374.
- [32] A. J. Hahn and O. T. O’Meara, The classical groups and K-theory, *Grund. math. Wissenschaften* 291, Springer Verlag, 1989.
- [33] J. E. Humphreys, *Variations on Milnor’s computation of $K_2 Z$* , in Algebraic K-theory, II: Classical algebraic K-theory and connections with arithmetic, 304–307, Lecture Notes in Math. 342, 1973.
- [34] J.-I. Igusa, *On theta functions and Weil’s generalized Poisson summation formula*, Trans. Amer. Math. Soc. 141 (1969), 195–210.
- [35] J.-I. Igusa, *On the Graded Ring of Theta-Constants*, Amer. J. Math. 86 (1964), 219–246.
- [36] J.-I. Igusa, Theta functions, Springer, New York, 1972.
- [37] N. Kaiblanger and M. Neuhauser, *Metaplectic operators for finite abelian groups and \mathbb{R}^d* , Indag. Math. (N.S.) 20 (2009), 233–246.
- [38] H. D. Kloosterman, *The behaviour of general theta functions under the modular group and the characters of binary modular congruence groups. I.*, Ann. of Math. (2) 47 (1946), 317–375.
- [39] I. Kaplansky, *Projective modules*, Ann. of Math (2) 68 (1958), 372–377.
- [40] M. Korkmaz and A. I. Stipsicz, *The second homology groups of mapping class groups of oriented surfaces*, Math. Proc. Cambridge Philos. Soc. 134 (2003), 479–489.
- [41] S. Lang, Algebraic number theory, Addison-Wesley Comp., 1970.
- [42] T. Lam, Introduction to quadratic forms over fields, vol.67, Graduate Stud. Math., Amer. Math. Soc., 2004.
- [43] M. Larsen, Z. Wang, *Density of the $SO(3)$ TQFT representation of mapping class groups*, Commun. Math. Phys. 260 (2005), 641–658.
- [44] A. I. Malcev, *On the faithful representation of infinite groups by matrices*, Mat. Sb., 8(50) (1940), pp. 405–422.
- [45] G. Masbaum and J. D. Roberts, *On central extensions of mapping class groups*, Math. Ann. 302 (1995), 131–150.

- [46] G. Masbaum, *On representations of mapping class groups in integral TQFT*, Oberwolfach Reports, vol.5, issue 2, 2008, 1157–1232.
- [47] G. Masbaum and A. Reid, *All finite groups are involved in the Mapping Class Group*, Geom. Topol. 16 (2012) 1393 – 1411.
- [48] H. Matsumoto, *Sur les groupes arithmétiques des groupes semi-simples déployés*, Ann. Sci. École Norm. Sup. (4) 2 (1969), 1–62.
- [49] J. L. Mennicke, *Finite factor groups of the unimodular group*, Ann. of Math. (2) 81 (1965), 31–37.
- [50] J. L. Mennicke, *Zur Theorie der Siegelschen Modulgruppe*, Math. Ann. 159 (1965), 115–129.
- [51] F. Mezzadri, *On the multiplicativity of quantum cat maps*, Nonlinearity 15 (2002), 905–922.
- [52] J. Milnor, Introduction to algebraic K-theory, *Annals Math. Studies* 72, Princeton Univ. Press, 1971.
- [53] J. Milnor and D. Husemoller, Symmetric bilinear forms, *Ergeb. Math. Grenz.* 73, Springer, 1973.
- [54] C.C. Moore, *Group extensions of p -adic and adelic linear groups*, Inst. Hautes Etudes Sci. Publ. Math. No. 35, 1968, 157–222.
- [55] D. Mumford, Tata lectures on theta I,II, *Progress in Math.*, 1984.
- [56] M. Newman and J. R. Smart, *Symplectic modular groups*, Acta Arith. 9 (1964), 83–89.
- [57] W. Pitsch, *Un calcul élémentaire de $H_2(\mathcal{M}_{g,1}, \mathbb{Z})$ pour $g \geq 4$* , C. R. Acad. Sci. Paris Sér. I Math. 329 (1999), no. 8, 667–670.
- [58] A. Putman, *The Picard group of the moduli space of curves with level structures*, Duke Math. J. 161 (2012), 623–674.
- [59] M. S. Raghunathan, *Torsion in cocompact lattices in coverings of $\text{Spin}(2, n)$* , Math. Ann. 266 (1984), 403–419.
- [60] R. Ranga Rao, *On some explicit formulas in the theory of Weil representation*, Pacific J. Math. 157 (1993), 335–371.
- [61] J. Rosenberg, Algebraic K-theory and its applications, *Graduate Texts in Mathematics* 147, Springer-Verlag, New York, 1994.
- [62] M. Sato, *The abelianization of the level d mapping class group*, J. Topology 3 (2010), 847–882.
- [63] J.P. Serre, Cohomologie galoisienne, 5-th ed., Lect. Notes Math. vol. 5., Springer-Verlag, Berlin, 1994.
- [64] G. Shimura, *Moduli and fibre systems of abelian varieties*, Ann. of Math. 83 (1966), 294–338.
- [65] Michael R. Stein, *Surjective stability in dimension 0 for K_2 and related functors*, Trans. Amer. Math. Soc. 178 (1973), 165–191.
- [66] Michael R. Stein, *The Schur multipliers of $Sp_6(\mathbb{Z})$, $Sp_{10}(\mathbb{Z})$, $Spin_7(\mathbb{Z})$ and $F_4(\mathbb{Z})$* , Math. Annalen 215 (1975), 165–172.
- [67] Michael R. Stein, *Stability theorems for K_1 , K_2 and related functors modeled on Chevalley groups*, Japan. J. Math. (N.S.) 4(1978), 77–108.
- [68] A. Suslin, *Torsion in K_2 of fields*, K-theory 1(1987), 5–29.
- [69] V. G. Turaev, Quantum invariants of knots and 3-manifolds. *de Gruyter Studies in Mathematics*, 18, Walter de Gruyter & Co., Berlin, 1994.
- [70] A. Weil, *Sur certain groupes d'opérateurs unitaires*, Acta Math. 111 (1964), 143–211.