IRREDUCIBLE FACTORS OF WEIL REPRESENTATIONS AND TQFT

JULIEN KORINMAN

Communicated by Ştefan Papadima

We give the decomposition into irreducible factors of Weil representations of $Sp_{2g}(\mathbb{Z})$ at even levels, generalizing the decompositions in [8, 19] at odd levels. We then derive the decomposition of the quantum representations of $SL_2(\mathbb{Z})$ arising in the $SU(2)$ and $SO(3)$ TQFTs. As application we show that, when the level indexing the TQFT is not a multiple of 4, the universal construction of [5] applied to a cobordism category without framed links leads to the same TQFT.

AMS 2010 Subject Classification: 57M25, 57R56.

Key words: Weil representations, symplectic groups, Topological Quantum Field Theory.

1. INTRODUCTION AND STATEMENTS

1.1. A BRIEF HISTORY

In this paper, we study a family of unitary representations of the symplectic groups $Sp_{2g}(\mathbb{Z})$, indexed by some integer $p \geq 2$, which are related to number theory, mathematical physics and topology (see the next section for definitions). They first appeared in the work of Kloosterman in 1946 (see [19]) where they arise as modular transformations of spaces of theta functions. They were rediscovered independently by the physicist Shale [32] following Segal [30] in 1962 when the authors studied the Weyl quantization of the symplectic torus. Their construction has been generalized to arbitrary locally compact abelian groups by Weil in 1964 (see [34]). The ones we consider in this paper are associated to $\mathbb{Z}/p\mathbb{Z}$. They also appeared independently in the work of Igusa [18] and Shimura [33] on theta functions. See also [25] for another construction.

The mathematical physics community studied the semi-classical properties of the Weil representations associated to finite cyclic groups when the level p tends to infinity as a model for quantum chaotical behavior (see [3,6,11,21]).

Topologists began to study these representations because they fit into the framework of Topological Quantum Field Theories. Their definition for even levels and arbitrary genus first appeared in [13, 17] in relation with 3-manifold invariants which were studied in [26] and further explored in [9] in the more general context of abelian invariants.

The main motivation of the author for this paper was to obtain information on the Witten-Reshetikhin-Turaev representations of the mapping class groups, as defined in [35], using a relation between the two families of representations in the genus one case.

The construction we will use in this paper is related to knot and skein theory following the topological point of view of [15]. Though less standard that the number theoretical or geometrical construction, this point of view is more elementary, crucial in the proofs of Theorem 4.13 and makes more transparent the relation with the Witten-Reshetikhin-Turaev representations made in the last section.

1.2. STATEMENTS

Given two integers $p \geq 2$ and $g \geq 1$, the Weil representations are projective unitary representations of the symplectic group $Sp_{2g}(\mathbb{Z})$

$$\pi_{p,g} : Sp_{2g}(\mathbb{Z}) \to \mathrm{PGL}(U_p^{\otimes g})$$

where U_p is a free module of rank p over the ring:

$$\mathbf{k}_p := \begin{cases} \mathbb{Z}\left[A, \frac{1}{2p}\right] / (\phi_p(A)) \ , & \text{when } p \text{ is odd.} \\ \mathbb{Z}\left[A, \frac{1}{p}\right] / (\phi_{2p}(A)), & \text{when } p \text{ is even.} \end{cases}$$

where $\phi_p \in \mathbb{Z}[X]$ represents the cyclotomic polynomial of degree p.

In [19], Kloosterman gave a complete decomposition of the Weil representations when $g = 1$ and p is odd. His result was further generalized by Cliff, Mc Neilly and Szechtman in [8] to arbitrary genus still at odd levels (see also [27]).

The main result of this paper is the extension of these decompositions to even levels.

Let $a, b \geq 2$ be two coprime non negative integers with b odd, and let u and v be odd integers such that $au + bv = 1$ in the case where a is odd and such that $2au + bv = 1$ if a is even and b is odd. We define a ring isomorphism $\mu : \mathbf{k}_{ab} \to \mathbf{k}_a \otimes \mathbf{k}_b$ by $\mu(A) = (A^{vb}, A^{au})$ if a is odd and $\mu(A) = (A^{vb}, A^{2au})$ if a is even, which turns $U_a^{\otimes g} \otimes U_b^{\otimes g}$ into a $\mathbf{k}_{ab}$-module.

For r prime and $n \geq 1$, we define the ring homomorphism $\mu : \mathbf{k}_{r^n} \to \mathbf{k}_{r^{n+2}}$ by $\mu(A) = A^{r^2}$ which turns $U_{r^n}^{\otimes g}$ into a $\mathbf{k}_{r^{n+2}}$-module.

Set $\sigma(p)$ for the number of divisors of p including 1.

Theorem 1.1. *The level p Weil representation contains $\sigma(p)$ irreducible submodules, when p is odd and $\sigma(\frac{p}{2})$, when p is even. They decompose according to the following rules, where $\cong$ denotes an isomorphism of $Sp_{2g}(\mathbb{Z})$ projective modules:*

1. *If $a, b \geq 2$ are two coprime integers, then:*
$$U_a^{\otimes g} \otimes U_b^{\otimes g} \cong U_{ab}^{\otimes g}$$
2. *If r is prime and $n \geq 1$, then:*
$$U_{r^{n+2}}^{\otimes g} \cong U_{r^n}^{\otimes g} \oplus W_{r^{n+2}}^{\otimes g}$$
where $W_{r^{n+2}}$ is a free submodule of $U_{r^{n+2}}$.
3. *If r is an odd prime, then:*
$$U_{r^2}^{\otimes g} \cong \mathbb{1} \oplus W_{r^2}^{\otimes g}$$
where $\mathbb{1}$ denotes the trivial representation.
4. *Every factor $U_p^{\otimes g}, W_{r^n}^{\otimes g}$ for $p \geq 3$ decomposes into two invariant submodules,*
$$U_p^{\otimes g} \cong U_p^{g,+} \oplus U_p^{g,-}$$
$$W_{r^n}^{\otimes g} \cong W_{r^n}^{g,+} \oplus W_{r^n}^{g,-}$$
We call $U_p^{g,+}$ and $W_{r^n}^{g,+}$ the even modules and $U_p^{g,-}, W_{r^n}^{g,-}$ the odd modules.
5. *The application of the previous four rules decomposes any $U_p^{\otimes g}$ into a direct sum of modules of the form $B_{r_1} \otimes \ldots \otimes B_{r_k}$ with $r_1, \ldots, r_k$ distinct prime numbers and $B_{r_i} \in \{U_{r_i}^{g,\pm},\ W_{r_i^n}^{g,\pm}\}$. These modules are all irreducible and pairwise distinct.*

The Witten-Reshetikhin-Turaev representations V_p of $SL_2(\mathbb{Z})$ defined in [35] are projectively isomorphic to the odd submodule U_p^- of the Weil representations (see [12] when p is even, [22] when $p \equiv 1 \pmod 4$ and the last section of this paper for a general proof). We deduce the following:

Corollary 1.2. *We have the following decomposition into irreducible modules of the genus one $SO(3)$ and $SU(2)$ quantum representations at level p of $SL_2(\mathbb{Z})$:*

$$\begin{aligned} V_p &\cong \bigoplus_{B \in E, B_1 \in E_1, \ldots, B_k \in E_k} B \otimes B_1 \otimes \ldots \otimes B_k, \text{ when p is even;} \\ V_p &\cong \bigoplus_{B_1 \in E_1, \ldots, B_k \in E_k} B_1 \otimes \ldots \otimes B_k, \text{ when p is odd.} \end{aligned}$$

where $p = 2^m r_1^{n_1} \ldots r_k^{n_k}$ is the factorization into primes and:

- *If j is such that n_j is odd,*

$$E_j = \left\{ W^{+}_{r_j^{n_j-2a_j}}, W^{-}_{r_j^{n_k-2a_j}}, U^{+}_{r_j}, U^{-}_{r_j} \mid 0 \le a_j \le \left\lceil \frac{n_k}{2} \right\rfloor - 1 \right\}.$$

- *If j is such that n_j is even,*

$$E_j = \left\{ W^{+}_{r_j^{n_j-2a_j}}, W^{-}_{r_j^{n_k-2a_j}}, \mathbb{1} \mid 0 \le a_j \le \left\lceil \frac{n_k}{2} \right\rfloor - 1 \right\}.$$

- *If m is odd, $E = \left\{ W^{+}_{2^{m-2a}}, W^{-}_{2^{m-2a}}, U_2 \mid 0 \le a \le \left\lceil \frac{m}{2} \right\rfloor - 1 \right\}$.*
- *If m is even, $E = \left\{ W^{+}_{2^{m-2a}}, W^{-}_{2^{m-2a}}, U_4^{+}, U_4^{-} \mid 0 \le a \le \left\lceil \frac{m}{2} \right\rfloor - 1 \right\}$.*

with the condition that each summand $B \otimes B_1 \otimes \ldots \otimes B_k$ or $B_1 \otimes \ldots \otimes B_k$ contains an odd number of modules $U_p^{-}, W_{r^n}^{-}$.

Example 1. The Weil representation (π_{500}, U_{500}) at level 500 decomposes as follows:

$$\begin{aligned} U_{500} &\cong U_4 \otimes U_{125} \cong U_4 \otimes (U_5 \oplus W_{125}) \\ &\cong (U_4^{+} \otimes U_5^{+}) \oplus (U_4^{-} \otimes U_5^{+}) \oplus (U_4^{+} \otimes U_5^{-}) \oplus (U_4^{-} \otimes U_5^{-}) \\ &\quad \oplus (U_4^{+} \otimes W_{125}^{+}) \oplus (U_4^{+} \otimes W_{125}^{-}) \oplus (U_3^{-} \otimes W_{125}^{+}) \oplus (U_3^{-} \otimes W_{125}^{-}) \end{aligned}$$

In particular, we derive the following decomposition of the $SU(2)$-quantum representation (ρ_{500}, V_{500}) in genus one at level 500:

$$V_{500} \cong U_{500}^{-} \cong (U_4^{-} \otimes U_5^{+}) \oplus (U_4^{+} \otimes U_5^{-}) \oplus (U_4^{-} \otimes W_{125}^{+}) \oplus (U_4^{+} \otimes W_{125}^{-})$$

where each factor in parenthesis is an irreducible factor.

The previous decomposition has the following application. The TQFTs defined in [5] associate to each closed oriented surface Σ, a vector space $V_p(\Sigma)$. To a triple (M, ϕ, L), where M is a closed oriented 3 manifold, $\phi : \partial M \to \Sigma$ an orientation-preserving homeomorphism and $L \subset M$ an embedded framed link (possibly empty), the TQFT associates a vector $Z_p(M, \phi, L) \in V_p(\Sigma)$. Such vectors generate $V_p(\Sigma)$ by definition (see the last section). The following theorem was proved by Roberts in the particular case where p is prime (it results from Lemma 2 in [29]).

Theorem 1.3. *If 4 does not divides p, then in the $SU(2)$ and $SO(3)$ TQFTs (see [5] for definitions), the vectors $Z_p(M, \phi, \emptyset)$, associated to cobordisms without framed links, generate $V_p(\Sigma)$.*

It results that the universal construction of [5] applied to a cobordism category without framed links leads to the same TQFTs. In particular, these TQFTs are determined by their 3 manifolds invariants without framed links (see the last section for details). It contrasts with the usual constructions (see [5, 28]) where standard generating sets for $V_p(\Sigma)$ are constructed from the skein modules of Handlebodies.

2. DEFINITION OF THE PROJECTIVE WEIL REPRESENTATIONS

The following section closely follows the definitions from [15].

2.1. HEISENBERG GROUPS AND SCHRÖDINGER REPRESENTATIONS

Definition 2.1. 1. Let $p \geq 2$ and M be a compact oriented 3-manifold possibly with boundary. The *reduced abelian skein module* $\widetilde{\mathcal{T}}_p(M)$ is the $\mathbf{k}_p$-module generated by the isotopy classes of oriented banded links of ribbons in M quotiented by the relations given by the abelian skein relations of Fig. 1 and by the submodule generated by the links made of p parallel copies of the same ribbon.

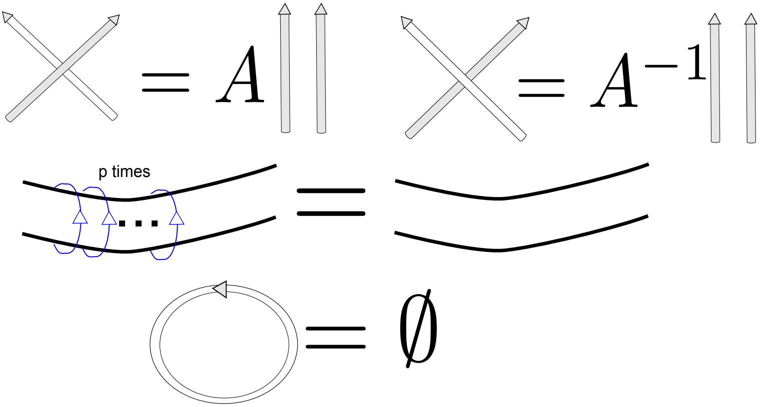


Fig. 1. Skein relations defining the reduced abelian skein modules.

The reduced abelian skein module of the sphere S^3 has rank one. The class of a link $L \subset S^3$ in this module is equal to the class of the empty link multiplied by $A^{lk(L)}$ where $lk(L)$ represents the self-linking number of L. This gives a natural isomorphism $\widetilde{\mathcal{T}}_p(S^3) \cong \mathbf{k}_p$.
It is classic, that if $M \cong \Sigma \times [0,1]$ is a thickened surface, then its reduced skein module $\widetilde{\mathcal{T}}_p(M)$ is isomorphic to $\mathbf{k}_p[H_1(\Sigma, \mathbb{Z}/p\mathbb{Z})]$.

2. Denote by H_g the genus g handlebody. Its abelian skein module is freely generated by the elements of $H_1(H_g, \mathbb{Z}/p\mathbb{Z})$. So, if we denote by U_p the module $\widetilde{\mathcal{T}}_p(S^1 \times D^2)$, we have a natural $\mathbf{k}_p$-isomorphism between $\widetilde{\mathcal{T}}_p(H_g)$ and $U_p^{\otimes g}$.

3. Let Σ_g be a closed oriented surface of genus g. The module $\widetilde{\mathcal{T}}_p(\Sigma_g \times [0,1])$ has an algebra structure with product induced by superposition, which appears to be the algebra of the following group.

We denote by $c \in \widetilde{\mathcal{T}}_p(\Sigma_g \times [0,1])$ the product of the class of the empty link by $A \in \mathbf{k}_p$. We call *Heisenberg group* and denote $\mathcal{H}_{p,g}$ the subgroup of $\widetilde{\mathcal{T}}_p(\Sigma_g \times [0,1])$ generated by c and $H_1(\Sigma_g, \mathbb{Z}/p\mathbb{Z})$. Denote by ω the intersection form $\omega : H_1(\Sigma_g, \mathbb{Z}/p\mathbb{Z}) \times H_1(\Sigma_g, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/p\mathbb{Z}$ when p is odd and $\omega : H_1(\Sigma_g, \mathbb{Z}/p\mathbb{Z}) \times H_1(\Sigma_g, \mathbb{Z}/p\mathbb{Z}) \to \mathbb{Z}/2p\mathbb{Z}$, when p is even. Then $\mathcal{H}_{p,g}$ is isomorphic to the group $H_1(\Sigma_g, \mathbb{Z}/p\mathbb{Z}) \times \mathbb{Z}/p\mathbb{Z}$, when p is odd and $H_1(\Sigma_g, \mathbb{Z}/2p\mathbb{Z}) \times \mathbb{Z}/2p\mathbb{Z}$ when p is even with group law given by:

$$(X, z) \bullet (X', z') = (X + X', z + z' + \omega(X, X'))$$

4. We choose a homeomorphism $\phi : \Sigma_g \to \Sigma_g$ so that $(\Sigma_g \times [0,1]) \bigcup_\phi H_g \cong H_g$. This gluing induces a linear action of the Heisenberg group on the reduced skein module $\widetilde{\mathcal{T}}_p(H_g) \cong U_p^{\otimes g}$. This representation is called *the Schrödinger representation* and will be denoted by $\mathrm{Add}_p : \mathcal{H}_{p,g} \to \mathrm{GL}(U_p^{\otimes g})$. Up to isomorphism, this representation does not depend on ϕ.

2.2. THE WEIL REPRESENTATIONS

Every element of the mapping class group $\mathrm{Mod}(\Sigma_g)$ acts on $H_1(\Sigma_g, \mathbb{Z})$ by preserving the intersection form. Choosing a basis of $H_1(\Sigma_g, \mathbb{Z})$ we obtain a surjective morphism $f : \mathrm{Mod}(\Sigma_g) \to Sp_{2g}(\mathbb{Z})$ whose kernel is called Torelli group.

Let $g \geq 1$, the module $\widetilde{\mathcal{T}}_p(\Sigma_g \times [0,1])$ is spanned by classes of links embedded in $\Sigma \times \{\frac{1}{2}\}$ with parallel framing whose class only depends on their homology class in Σ_g. The action in homology of the mapping class group $\mathrm{Mod}(\Sigma_g)$ induces, by passing through the quotient by the reduced skein relations, an action on the Heisenberg group. We denote by $\bullet$ this action. Let $\phi \in \mathrm{Mod}(\Sigma_g)$ and consider the representation $s^\phi : \mathcal{H}_{p,g} \to \mathrm{GL}(U_p^{\otimes g})$ defined by $s^\phi(h) := \mathrm{Add}_p(\phi \bullet h)$ for all $h \in \mathcal{H}_{p,g}$. It is a standard fact, referred as the Stone-Von Neumann theorem, that the Schrödinger representation is the unique irreducible representation of the Heisenberg group sending the central element c to the scalar operator $A \cdot \mathbb{1}$.

It results that the representation s^ϕ is conjugate to the Schrödinger representation. Thus there exists $\pi_{p,g}(\phi) \in \mathrm{GL}(U_p^{\otimes g})$, uniquely determined up to multiplication by an invertible scalar, so that:

$$\pi_{p,g}(\phi)\,\mathrm{Add}_p(h)\pi_{p,g}(\phi)^{-1} = \mathrm{Add}_p(\phi \bullet h), \text{ for any } h \in \mathcal{H}_{p,g} \tag{1}$$

The equation (1) is called the Egorov identity and we easily show that the elements $\pi_{p,g}(\phi)$ define a projective representation $\underline{\pi}_{p,g} : \mathrm{Mod}(\Sigma_g) \to \mathrm{PGL}(U_p^{\otimes g})$ called the Weil representation.

Since the action of $\mathrm{Mod}(\Sigma_g)$ on $\mathcal{H}_{p,g}$ factorizes through the Torelli group and through $Sp_{2g}(\mathbb{Z}/p\mathbb{Z})$ when p is odd and $Sp_{2g}(\mathbb{Z}/2p\mathbb{Z})$ when p is even, so do the Weil representations.

The previous definition of the Weil representations as intertwining operators is not explicit. To manipulate it more easily, we choose the generators of $Sp_{2g}(\mathbb{Z})$ consisting of the image through f of the Dehn twists X_i, Y_i, Z_{ij} of Fig. 2 (see [23] for a proof these Dehn twists generate the mapping class group). We define the basis $\{e_{a_1} \otimes \ldots \otimes e_{a_g} | a_1, \ldots, a_g \in \mathbb{Z}/p\mathbb{Z}\}$ of $U_p^{\otimes g}$ as in Fig. 3, that means that $e_{a_1} \otimes \ldots \otimes e_{a_g}$ is the class of a link made of a_i parallel copies of an unframed ribbon encircling the i^{th} hole of H_g one time. To express the image of the generators in the basis, we will first need to define Gauss sums.

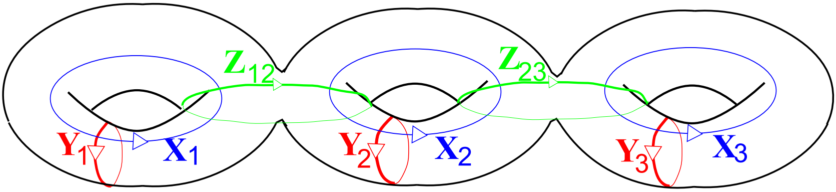


Fig. 2 – A set of Dehn twists generating the mapping class group and the symplectic group.

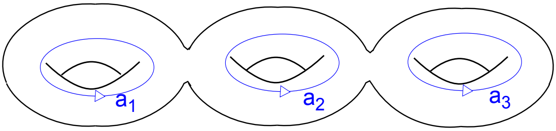
$e_{a_1} \otimes e_{a_2} \otimes e_{a_3} =$ 

Fig. 3 – A basis for the abelian skein module of the genus g handlebody. Here an integer i in front of a ribbon means that we take i parallel copies of it.

Definition 2.2. Let $p \geq 2$ and a, b be two integers. We define the Gauss sums by the formulas:

1. $G(a,b,p) := \sum_{k\in\mathbb{Z}/p\mathbb{Z}} A^{ak^2+bk} \in \mathbf{k}_p$ when p is odd.
2. $G(a,b,2p) := \sum_{k\in\mathbb{Z}/2p\mathbb{Z}} A^{ak^2+bk} = 2\sum_{k\in\mathbb{Z}/p\mathbb{Z}} A^{ak^2+bk} \in \mathbf{k}_p$ when p is even.

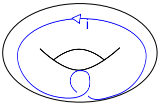
The computation of the Gauss sums is detailed in [2].

Proposition 2.3. *The expression of the matrices of the Weil representation on the generators X_i, Y_i and $Z_{i,j}$ in the basis $\{e_{a_1} \otimes \ldots \otimes e_{a_g} | a_1, \ldots, a_g \in \mathbb{Z}/p\mathbb{Z}\}$ of $U_p^{\otimes g}$ is given by the projective class of the following matrices:*

- $\pi_{p,1}(X) = (A^{2i^2}\delta_{i,j})_{i,j}$ *and* $\pi_{p,g}(X_i) = \mathbb{1}^{\otimes(i-1)} \otimes \pi_p^1(X) \otimes \mathbb{1}^{\otimes(g-i)}$.
- $\pi_{p,g}(Z_{i,j})(e_{a_1} \otimes \ldots \otimes e_{a_g}) = A^{(a_i-a_j)^2}(e_{a_1} \otimes \ldots \otimes e_{a_g})$.
- $\pi_{p,1}(Y) = \begin{cases} \frac{G(1,0,N)}{N}(A^{-(i-j)^2})_{i,j}, & \textit{when } p \textit{ is odd.} \\ \frac{G(1,0,2N)}{2N}(A^{-(i-j)^2})_{i,j}, & \textit{when } p \textit{ is even.} \end{cases}$
  $\pi_{p,g}(Y_i) = \mathbb{1}^{\otimes(i-1)} \otimes \pi_{p,1}(Y) \otimes \mathbb{1}^{\otimes(g-i)}$.

These generating matrices are unitary (they verify $\bar{U}^T U = \mathbf{1}$ *where* $\bar{U} = \left(\bar{U_{i,j}}\right)_{i,j}$ *is defined by the involution of* $\boldsymbol{k}_p$ *sending* A *to* A^{-1}*) so are the Weil representations.*

Proof. If $\phi \in \mathrm{Mod}(\Sigma_g)$ can be extended to a homeomorphism Φ of the handlebody H_g, the action of Φ on $\mathcal{T}_p(H_g) \cong U_p^{\otimes g}$ defines an operator which satisfies the Egorov identity (1) so is projectively equal to $\underline{\pi}_{p,g}(\phi)$. The generators X_i and $Z_{i,j}$ are such homeomorphisms and Fig. 4 shows how we compute their action on the basis.

$\pi_{p,1}(X) \cdot e_i =$  $= A^{i^2} e_i$

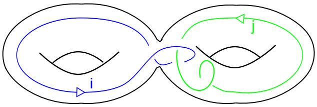
$\pi_{p,2}(Z_{1,2}) \cdot e_i \otimes e_j =$  $= A^{(i-j)^2} e_i \otimes e_j$

Fig. 4 – The computation of the matrices associated to $\pi_{p,1}(X)$ and $\pi_{p,2}(Z_{1,2})$.

Then choose a Heegaard splitting of the sphere $H_g \bigcup_\phi H_g \cong S^3$ with $\phi \in \mathrm{Mod}(\Sigma_g)$. This splitting determines a pairing $\widetilde{\mathcal{T}}_p(H_g) \times \widetilde{\mathcal{T}}_p(H_g) \rightarrow \widetilde{\mathcal{T}}_p(S^3) \cong k'_p$. The associated bilinear pairing $(\cdot,\cdot)_p^H : U_p^{\otimes g} \otimes U_p^{\otimes g} \rightarrow \mathbf{k}_p$ is called the *Hopf pairing.* Fig. 5 shows that:

$$\left(e_{a_1} \otimes \ldots \otimes e_{a_g}, e_{b_1} \otimes \ldots \otimes e_{b_g}\right)_p^H = A^{-2\sum_i a_i b_i}$$

Thus the Hopf pairing is non degenerate.

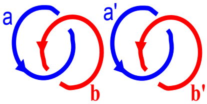
$\left(e_a \otimes e_b, e_{a'} \otimes e_{b'}\right)_p^H =$  $= A^{-2ab-2a'b'}$

Fig. 5 – The computation of the matrix associated to the Hopf pairing when $g = 2$.

The dual of $\pi_{p,g}(X_i)$ for $\langle\cdot,\cdot\rangle^H$ satisfies the Egorov identity (1), so is projectively equal to $\underline{\pi}_{p,g}(Y_i)$. If $\pi_{p,1}(Y)$ is the dual of $\pi_{p,1}(X)$ for $(\cdot,\cdot)^H$, the previous expression of $\pi_{p,g}(X_i)$ implies that its dual for the Hopf pairing is $\mathbb{1}^{\otimes(i-1)} \otimes \pi_{p,1}(Y) \otimes \mathbb{1}^{\otimes(g-i)}$.

To compute the matrix of $\pi_{p,1}(Y)$, we remark that the matrix $S = \left(A^{-2ij}\right)_{i,j}$ of the Hopf pairing has inverse $S^{-1} = \frac{1}{p}\bar{S} = \frac{1}{p}(A^{2ij})_{i,j}$. A direct computation gives:

$$\pi_{p,1}(Y) = S\pi_{p,1}(X)S^{-1}$$
$$= \begin{cases} \frac{G(1,2(j-i),p)}{p} = \frac{G(1,0,p)}{p}(A^{-(i-j)^2})_{i,j}, & \text{when p is odd;} \\ \frac{G(1,2(j-i),2p)}{2p} = \frac{G(1,0,2p)}{2p}(A^{-(i-j)^2})_{i,j}, & \text{when p is even.} \end{cases} \quad \square$$

Remark. 1. When p is even and $A = \exp\left(-\frac{i\pi}{p}\right)$, the projective representations we defined here coincide with the ones from [13] and [17] coming from theta functions.

2. When p is odd or when $g = 1$ and p is even, the Weil representations lift to linear representations of $SL_2(\mathbb{Z}/p\mathbb{Z})$ and $SL_2(\mathbb{Z}/2p\mathbb{Z})$ respectively (see [1] for a proof and [20] for a proof that the matrices $\pi_{p,g}(X_i), \pi_{p,g}(Y_i)$ and $\pi_{p,g}(Z_{i,j})$, defined in Proposition 2.3 define an explicit lift).

   When p is even and $g \geq 2$, they lift to linear representations of $\widetilde{Sp_{2g}(\mathbb{Z})}$ a central extension of $Sp_{2g}(\mathbb{Z}/2p\mathbb{Z})$ by $\mathbb{Z}/2\mathbb{Z}$ (see [14] for a proof and [20] for a proof that the matrices above define an explicit lift).

   We will now consider these linear lifted representations and denote them by $\pi_{p,g}$.

3. DECOMPOSITION OF THE WEIL REPRESENTATIONS

In this section, we prove the three first points of the Theorem 1.1. We first define:

$$U_p^{+,g} := \mathrm{Span}\{e_{a_1} \otimes \ldots \otimes e_{a_g} + e_{-a_1} \otimes \ldots \otimes e_{-a_g} | a_1, \ldots, a_g \in \mathbb{Z}/p\mathbb{Z}\}$$
$$U_p^{-,g} := \mathrm{Span}\{e_{a_1} \otimes \ldots \otimes e_{a_g} - e_{-a_1} \otimes \ldots \otimes e_{-a_g} | a_1, \ldots, a_g \in \mathbb{Z}/p\mathbb{Z}\}$$

LEMMA 3.1. *The submodules $U_p^{+,g}$ and $U_p^{-,g}$ are $\pi_{p,g}$-stable.*

Proof. A direct computation shows that the submodules $U_p^{g,+}$ and $U_p^{g,-}$ are stabilized by $\pi_{p,g}(X_i), \pi_{p,g}(Y_i)$ and $\pi_{p,g}(Z_{i,j})$. We can also remark that the involution acting on the reduced skein module by changing the orientation of a framed link, commutes with the image of π. The modules $U_p^{\pm,g}$ correspond to its two eigenspaces. $\square$

Let $a, b \geq 2$ be two coprime non negative integers with b odd, and let u and v be odd integers such that $au + bv = 1$ in the case where a is odd and such that $2au+bv=1$ if a is even and b is odd. We define a ring isomorphism $\mu : \mathbf{k}_{ab} \to \mathbf{k}_a \otimes \mathbf{k}_b$ by $\mu(A) = (A^{vb}, A^{au})$ if a is odd and $\mu(A) = (A^{vb}, A^{2au})$ if a is even, which turns $U_a^{\otimes g} \otimes U_b^{\otimes g}$ into a $\mathbf{k}_{ab}$-module. We also denote by $f : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \to \mathbb{Z}/ab\mathbb{Z}$ the bijection sending (x,y) to $xv+yu$ when a is odd and to $xv+2yu$ when a is even. The following lemma was shown in [21], we give a more explicit proof.

Lemma 3.2 ([21]). *The isomorphism of $\mathbf{k}_{ab}$-module $\psi : U_a^{\otimes g} \otimes U_b^{\otimes g} \to U_{ab}^{\otimes g}$ defined by*

$$\psi((e_{a_1} \otimes \ldots \otimes e_{a_g}) \otimes (e_{b_1} \otimes \ldots \otimes e_{b_g})) = e_{f(a_1,b_1)} \otimes \ldots \otimes e_{f(a_g,b_g)}$$

makes the following diagram commute for all $\phi \in Sp_{2g}(\mathbb{Z})$ (resp for all $\phi \in \widetilde{Sp_{2g}}(\mathbb{Z})$ when a is even):

$$\begin{tikzcd}
U_a^{\otimes g} \otimes U_b^{\otimes g} \arrow[r, "\psi"] & U_{ab}^{\otimes g} \\
U_a^{\otimes g} \otimes U_b^{\otimes g} \arrow[r, "\psi"] \arrow[u, "\pi_{a,g}(\phi)\otimes\pi_{b,g}(\phi)"] & U_{ab}^{\otimes g} \arrow[u, "\pi_{ab,g}(\phi)"']
\end{tikzcd}$$

Proof. We note $(A_1, A_2) := (A^{vb}, A^{au})$ when a and b are odd and $(A_1, A_2) = (A^{vb}, A^{2au})$ when a is even. It is enough to show the commutativity of the diagram for $\phi = X_i, Y_i$ and $Z_{i,j}$. For $\phi = X_i$, we compute:

$$\psi\left(\pi_{a,g}(X_i) \otimes \pi_{b,g}(X_i)((e_{a_1} \otimes \ldots \otimes e_{a_g}) \otimes (e_{b_1} \otimes \ldots \otimes e_{b_g}))\right) = \\ \psi\left(A_1^{a_i^2} A_2^{b_i^2}((e_{a_1} \otimes \ldots \otimes e_{a_g}) \otimes (e_{b_1} \otimes \ldots \otimes e_{b_g}))\right) = \\ A^{f(a_i,b_i)^2}(e_{f(a_1,b_1)} \otimes \ldots \otimes e_{f(a_g,b_g)})$$

Then for $\phi = Y_i$, we note $c_p = \frac{G(1,0,p)}{p}$ when p is odd and $c_p = \frac{G(1,0,2p)}{2p}$ when p is even:

$$\psi\left(\pi_{a,g}(Y_i) \otimes \pi_{b,g}(Y_i)((e_{a_1} \otimes \ldots \otimes e_{a_g}) \otimes (e_{b_1} \otimes \ldots \otimes e_{b_g}))\right) \\ = \psi\left(c_a c_b \right. \\ \left. \sum_{\substack{k\in\mathbb{Z}/a\mathbb{Z} \\ l\in\mathbb{Z}/b\mathbb{Z}}} A_1^{-(a_i-k)^2} A_2^{-(b_i-l)^2}((e_{a_1} \otimes \ldots \otimes e_k \otimes \ldots \otimes e_{a_g}) \otimes (e_{b_1} \otimes \ldots \otimes e_l \otimes \ldots \otimes e_{b_g}))\right) \\ = \psi(c_a c_b) \sum_{m\in\mathbb{Z}/ab\mathbb{Z}} A^{-(f(a_i,b_i)-m)^2}(e_{f(a_1,b_1)} \otimes \ldots \otimes e_m \otimes \ldots \otimes e_{f(a_g,b_g)})$$

where we made the change of variable $m = f(k,l)$ to pass to the last line. We conclude by noticing that $\psi(c_a c_b) = c_{ab}$ which is equivalent to $\psi(G(1,0,a)$

$G(1,0,b)) = G(1,0,ab)$ when a is odd and $\psi(G(1,0,2a)G(1,0,b)) = G(1,0,2ab)$ when a is even.

Finally, for $\phi = Z_{i,j}$:

$$\begin{aligned}
&\psi\left(\pi_{a,g}(Z_{i,j}) \otimes \pi_{b,g}(Z_{i,j})((e_{a_1} \otimes \ldots \otimes e_{a_g}) \otimes (e_{b_1} \otimes \ldots \otimes e_{b_g}))\right) \\
&\qquad = \psi\left(A_1^{(a_i-a_j)^2} A_2^{(b_i-b_j)^2}((e_{a_1} \otimes \ldots \otimes e_{a_g}) \otimes (e_{b_1} \otimes \ldots \otimes e_{b_g}))\right) \\
&\qquad\qquad = A^{f(a_i,b_i)^2}(e_{f(a_1,b_1)} \otimes \ldots \otimes e_{f(a_g,b_g)}) \quad \square
\end{aligned}$$

Remark. This lemma also follows from ([26], Proposition 2.3) where it is showed that the 3-manifold invariant coming from the abelian TQFT at level ab, with a coprime to b, is the product of the ones in level a and b. We can then conclude using the same argument as in [5].

Let r be a prime number and $n \geq 0$ if r is odd or $n \geq 1$ if $r = 2$. Let $\bar{U}_{r^n}^{\otimes g}$ be the submodule of $U_{r^{n+2}}^{\otimes g}$ spanned by the vectors $g_{a_1} \otimes \ldots \otimes g_{a_g}$ where $g_i := \sum_{0 \leq k \leq r-1} e_{r(i+kr^n)}$.

Lemma 3.3. *The submodule $\bar{U}_{r^n}^{\otimes g}$ is stabilized by $\pi_{r^{n+2},g}$. Moreover, the isomorphism of $\boldsymbol{k}_{r^{n+2}}$-modules $\psi : U_{r^n}^{\otimes g} \to \bar{U}_{r^n}^{\otimes g}$ sending $e_{a_1} \otimes \ldots \otimes e_{a_g}$ to $g_{a_1} \otimes \ldots \otimes g_{a_g}$ makes the following diagram commute for all $\phi \in Sp_{2g}(\mathbb{Z})$ (for all $\phi \in \widetilde{Sp_{2g}(\mathbb{Z})}$ when $r = 2$ respectively):*

$$\begin{tikzcd}
\mathrm{GL}(U_{r^{n+2}}^{\otimes g})^{\bar{U}_{r^n}^{\otimes g}} \arrow[r, "\pi_{r^{n+2},g}(\phi)"] & \mathrm{GL}(U_{r^{n+2}}^{\otimes g})^{\bar{U}_{r^n}^{\otimes g}} \\
\mathrm{GL}(U_{r^n}^{\otimes g}) \arrow[r, "\pi_{r^n,g}(\phi)"] \arrow[u, hook] & \mathrm{GL}(U_{r^n}^{\otimes g}) \arrow[u, hook]
\end{tikzcd}$$

Proof. We generalize an argument of [8] to even levels to show that $\bar{U}_{r^n}^{\otimes g}$ is $\pi_{r^{n+2},g}$-stable. Denote by I the principal ideal $I := r^{n+1}H_1(\Sigma^g, \mathbb{Z}/r^{n+2}\mathbb{Z})$ of $H_1(\Sigma^g, \mathbb{Z}/r^{n+2}\mathbb{Z})$ and by D the subgroup $D := (I \times I, 0)$ of $\mathcal{H}_{r^{n+2},g}$. Since $I^2 = \{0\}$ and I is an ideal, D is a subgroup of $\mathcal{H}_{r^{n+2},g}$ stable under the action of $Sp_{2g}(\mathbb{Z})$. We deduce from the Egorov identity that the space $\{v \in U_{r^{n+2}}^{\otimes g} | \operatorname{Add}_p(\phi)v = v, \forall \phi \in D\}$ is preserved by $\pi_{r^{n+2},g}$. We now easily show that this space is $\bar{U}_{r^n}^{\otimes g}$.

We then verify the commutativity of the diagram for $\phi = X_i, Y_i$ and $Z_{i,j}$. When $\phi = X_i$ we have:

$$\pi_{r^{n+2},g}(X_i)(g_{a_1} \otimes \ldots \otimes g_{a_g}) = A^{(ri)^2}(g_{a_1} \otimes \ldots \otimes g_{a_g}) = \mu(A)^{i^2}(g_{a_1} \otimes \ldots \otimes g_{a_g})$$

When $\phi = Y_i$ we have:

$$\pi_{r^{n+2},g}(Y_i)(g_{a_1} \otimes \ldots \otimes g_{a_g})$$

$$= c_{r^{n+2}} \sum_{x\in\mathbb{Z}/r^{n+2}} \sum_{k\in\mathbb{Z}/r\mathbb{Z}} A^{-(r(a_i+kr^n)-x)^2} g_{a_1}\otimes\ldots\otimes e_x\otimes\ldots\otimes e_{a_g}$$

$$= c_{r^{n+2}} \sum_{x\in\mathbb{Z}/r^{n+2}\mathbb{Z}} A^{-x^2-xra_i-r^2a_i^2}\left(\sum_{k\in\mathbb{Z}/r\mathbb{Z}} (A^{2r^{(}n+1)x})^k\right) g_{a_1}\otimes\ldots\otimes e_x\otimes\ldots\otimes g_{a_g}$$

$$= rc_{r^{n+2}} \sum_{y\in\mathbb{Z}/r^{n+1}\mathbb{Z}} (A^{r^2})^{-(y-a_i)^2} g_{a_1}\otimes\ldots\otimes e_{ry}\otimes\ldots\otimes g_{a_g}$$

$$= rc_{r^{n+2}}(\mu(A))^{-(z-a_i)^2} \sum_{z\in\mathbb{Z}/r^n\mathbb{Z}} g_{a_1}\otimes\ldots\otimes g_z\otimes\ldots\otimes g_{a_k}$$

We verify that $\mu(c_{r^n}) = rc_{r^{n+2}}$ to conclude in this case. Finally when $\phi = Z_{i,j}$:

$$\pi_{r^{n+2},g}(Z_{i,j})(g_{a_1}\otimes\ldots\otimes g_{a_g})$$

$$= \sum_{k,l\in\mathbb{Z}/p\mathbb{Z}} A^{(r(a_i+kr^n)-p(a_j+lr^n))^2}(g_{a_1}\otimes\ldots e_{r(a_i+kr^n)}\otimes\ldots\otimes e_{r(a_j+lr^n)}\otimes\ldots\otimes g_{a_g})$$

$$= \sum_{k,l\in\mathbb{Z}/p\mathbb{Z}} (A^{r^2})^{(a_i-a_j)^2}(g_{a_1}\otimes\ldots e_{r(a_i+kr^n)}\otimes\ldots\otimes e_{r(a_j+lr^n)}\otimes\ldots\otimes g_{a_g})$$

$$= (\mu(A)^{(a_i-a_j)^2}(g_{a_1}\otimes\ldots\otimes g_{a_g}) \quad \square$$

Let $W_{r^{n+2}}$ be the submodule of U_{r^n} orthogonal for the invariant form turning $\{e_0,\ldots,e_{r^{n+2}-1}\}$ into an orthogonal basis. It is freely generated by the vectors e_i when r does not divide i and by the vectors $e_{ri-r(i+k+r^n)}$ for $i\in\{0,\ldots,r^n-1\}$ and $k\in\{1,\ldots,r-1\}$.

The orthogonal of $\bar{U}_{r^n}^{\otimes g}$ in $U_{r^{n+2}}^{\otimes g}$ is isomorphic to $W_{r^{n+2}}^{\otimes g}$ and is stabilized by $\pi_{r^{n+2},g}$. So are the two submodules $W_{r^{n+2}}^{g,\pm} := W_{r^{n+2}}^{\otimes g}\bigcap U_{r^{n+2}}^{g,\pm}$.

4. **IRREDUCIBILITY OF THE FACTORS**

4.1. THE GENUS ONE CASES

The goal of this section is to extend Kloosterman's work [19] to even levels.

When $g = 1$ the strategy for the proof lies on the computation of the following Kloosterman's sums:

(2) $\quad \mathbf{S}_p := \frac{1}{|SL_2(\mathbb{Z}/p\mathbb{Z})|}\sum_{\phi\in SL_2(\mathbb{Z}/p\mathbb{Z})}|\operatorname{Tr}(\pi_p(\phi))|^2,\quad$ when p is odd.

(3) $\quad \mathbf{S}_{2p} := \frac{1}{|SL_2(\mathbb{Z}/2p\mathbb{Z})|}\sum_{\phi\in SL_2(\mathbb{Z}/2p\mathbb{Z})}|\operatorname{Tr}(\pi_p(\phi))|^2,\quad$ when p is even.

It is a classical fact that if this sum is equal to the number of component in a decomposition of π_p then each factors appearing in this decomposition are irreducible and they are pairwise distinct (see [31], chapter 2).

LEMMA 4.1. *If a is prime to b then $\boldsymbol{S}_{ab} = \boldsymbol{S}_a \times \boldsymbol{S}_b$ if they are both odd and $\boldsymbol{S}_{2ab} = \boldsymbol{S}_{2a} \times \boldsymbol{S}_b$ if a is even.*

Proof. This follows from the fact that we have a group isomorphism $SL_2(\mathbb{Z}/ab\mathbb{Z}) \cong SL_2(\mathbb{Z}/a\mathbb{Z}) \times SL_2(\mathbb{Z}/b\mathbb{Z})$ together with Proposition 3.2. □

In [19] Kloosterman showed that for an odd prime r and $n \geq 1$ then $\mathbf{S}_{r^n} = n + 1$. Thus, to complete the proof of Theorem 1.1 it remains to show the following:

PROPOSITION 4.2. *For $n \geq 1$, we have:*

$$\boldsymbol{S}_{2^n} = n - 1$$

Since the summand $|\operatorname{Tr}(\pi_{2^n}(\phi))|^2$ only depends on the conjugacy class of ϕ we will first make a complete study of the conjugacy classes of $SL_2(\mathbb{Z}/2^n\mathbb{Z})$. Then we will compute the characters of the Weil representations on representatives of each conjugacy classes.

4.1.1. Conjugacy classes of $SL_2(\mathbb{Z}/2^n\mathbb{Z})$

We begin by defining three invariants of the conjugacy classes which almost classify the conjugacy classes:

Definition 4.3. For $A \in SL_2(\mathbb{Z}/2^n\mathbb{Z})$ there exists a unique integer $l \in \{0, \ldots, n\}$ and $x \in \{0, \ldots, 2^l - 1\}$ such that:

$$A \equiv x\mathbb{1} + 2^l U_1 \pmod{2^n}$$

for some matrix U_1 which reduction modulo 2 is neither the identity, nor the null matrix. We define a third integer

$$\tau := \begin{cases} \operatorname{Tr}(A) \in \mathbb{Z}/2^n\mathbb{Z}, & \text{when } l = 0. \\ \det(U_1) \in \mathbb{Z}/2^{n-l}\mathbb{Z}, & \text{when } l \geq 1. \end{cases}$$

Note that $\det(U) = 1 (\text{mod } 2^n)$ implies that $x^2 = 1 (\text{mod } 2^l)$ hence if $l = 1$ then $x = 1$, when $l = 2$ then $x = 1$ or 3, when $l \geq 3$ we have four choices: $x = 1, 2^l - 1, 2^{l-1} + 1$ or $2^{l-1} - 1$.

Let us denote by $C(x, l, \tau)$ the set of matrices of $SL_2(\mathbb{Z}/2^n\mathbb{Z})$ having x, l and τ as invariants. Clearly $C(-1, l, \tau) = -C(1, l, \tau)$ and $C(2^{l-1} - 1, l, \tau) = -C(2^{l-1}+1, l, \tau)$, thus we only need to study the conjugacy classes of $C(x, l, \tau)$ when $x = 1$ or $x = 2^{l-1} + 1$.

As example, the matrices with $l = 0$ are the matrices which are not equal to the identity matrix modulo 2 whereas those with $l = n$ are the four scalar matrices.

Definition 4.4. We define the following representatives of $C(x, l, \tau)$, where c_1 will denote an odd number:

- $l = 0$, $A_0(\tau, c_1) := \begin{pmatrix} 1 & c_1^{-1}(\tau - 2) \\ c_1 & \tau - 1 \end{pmatrix}$.
- $l \geq 1$, $x = 1$, $A_l(\tau, c_1) := \begin{pmatrix} 1 & c_1^{-1} 2^l \tau \\ c_1 2^l & 1 + 2^l \tau \end{pmatrix}$.
- $l \geq 3$, $x = 1 + 2^{l-1}$,
  $B_l(\tau, c_1) := \begin{pmatrix} 1 + 2^{l-1} & -c_1^{-1} 2^l \tau \\ 2^l c_1 & 1 + 2^{l-1} - (1 + 2^{l-1})^{-1}(2^l + 2^{2l-2} + 2^{2l}\tau) \end{pmatrix}$.

Similar representative for $x = -1$ and $x = 2^{l-1} - 1$ are given by taking $-A_l$ and $-B_l$.

Proposition 4.5. *Each set $C(x, l, \tau)$ contains $1, 2$ or 4 conjugacy classes each containing a matrix $\pm A_l(\tau, c_1)$ or $\pm B_l(\tau, c_1)$ for a suitable choice of c_1. The following table gives for every l, x, τ a set of $1, 2$ or 4 representatives and the cardinal $m(A)$ of the corresponding conjugacy classes:*

l and x	τ	*Representatives of $C(x, l, \tau)$*	$m(A)$
$l = 0$	$\mathrm{Tr}(U) = \tau$ *is odd*	$A_0(\tau, 1)$	2^{2n-1}
	$\mathrm{Tr}(U) = \tau = 2 \pmod 4$	$A_0(\tau, 1), A_0(\tau, 3), A_0(\tau, 5), A_0(\tau, 7)$	$3 \cdot 2^{2n-4}$
	$\mathrm{Tr}(U) = \tau = 0 \pmod 4$	$A_0(\tau, 1), A_0(\tau, 3)$	$3 \cdot 2^{2n-3}$
$l = 1$ *and* $x = 1$	$\tau = 1 \pmod 8$	$A_1(\tau, 1), A_1(\tau, 3), A_1(\tau, 5), A_1(\tau, 7)$	$3 \cdot 2^{2n-6}$
	$\tau = 3, 5, 7 \pmod 8$	$A_1(\tau, 1), A_1(\tau, \tau)$	$3 \cdot 2^{2n-5}$
	$\tau = 2, 4, 6 \pmod 8$	$A_1(\tau, 1), A_1(\tau, 3)$	$3 \cdot 2^{2n-5}$
	$\tau = 0 \pmod 8$	$A_1(\tau, 1), A_1(\tau, 3), A_1(\tau, 5), A_1(\tau, 7)$	$3 \cdot 2^{2n-6}$
$2 \leq l \leq n - 3$ *and* $x = 1$	$\tau = 1, 4, 5 \pmod 8$	$A_l(\tau, 1), A_l(\tau, 3)$	$3 \cdot 2^{2n-2l-3}$
	$\tau = 3, 7 \pmod 8$	$A_l(\tau, 1)$	$3 \cdot 2^{2n-2l-2}$
	$\tau = 2 \pmod 8$	$A_l(\tau, 1), A_l(\tau, 5)$	$3 \cdot 2^{2n-2l-3}$
	$\tau = 0 \pmod 8$	$A_l(\tau, 1), A_l(\tau, 3), A_l(\tau, 5), A_l(\tau, 7)$	$3 \cdot 2^{2n-2l-4}$
$l = n - 2$ *and* $x = 1$	$\tau = 0, 1 \pmod 4$	$A_{n-2}(\tau, 1), A_{n-2}(\tau, 3)$	6
	$\tau = 2, 3 \pmod 4$	$A_{n-2}(\tau, 1)$	12
$l = n - 1$ *and* $x = 1$	$\tau = 0 \pmod 2$	$A_{n-1}(0, 1)$	3
	$\tau = 1 \pmod 2$	$A_{n-1}(1, 1)$	3
$3 \leq l \leq n - 1$ *and* $x = 1 + 2^{l-1}$	τ *odd*	$B_l(\tau, 1)$	$2^{2n-2l-1}$
	τ *even*	$B_l(\tau, 1)$	$3 \cdot 2^{2n-2l-1}$
$l = n$		$\mathbb{1}, -\mathbb{1}, (2^{n-1} + 1)\mathbb{1}$ *and* $(2^{n-1} - 1)\mathbb{1}$	1

Proposition 4.5 gives the complete description of the conjugacy classes of $SL_2(\mathbb{Z}/2^n\mathbb{Z})$. The exact information needed for computing $\mathbf{S}_{2^n}$ is summarized in the following:

Corollary 4.6. *For $A \in SL_2(\mathbb{Z}/2^n\mathbb{Z})$ we define $s(A) \in \{2l, \dots, l+n\}$ to be the maximal s for which 2^{s-l} divides τ. Let $N(l,x)$, resp. $N(l,x,s)$, be the number of matrices having l, x (resp s) as invariants. We deduce from Theorem 4.5 the following:*

1. $N(0,1,0) = 2^{3n-2}$.
2. *For* $1 \leq s \leq n-1$, $N(0,1,s) = 3 \cdot 2^{3n-s-3}$.
3. $N(0,1,n) = 3 \cdot 2^{2n-2}$.
4. *For* $l \geq 1$, $N(l,1,s) = 3.2^{3n-l-s-3}$ *if* $s \neq l+n$ *and* $N(l,1,n+l) = 3 \cdot 2^{2n-2l-2}$.
5. *For* $l \geq 2$, $N(l,-1) = 3 \cdot 2^{3n-3l-2}$.
6. *For* $l \geq 3$, $N(l, 1+2^{l-1}) = N(l, 2^{l-1}-1) = 2^{3n-3l}$.
7. $N(n,x) = 1$.

The proof of Proposition 4.5 will be deduced from the following:

Lemma 4.7. *Let $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $U' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ be two matrices of $C(x,l,\tau)$. If $l=0$, we suppose that c and c' are odd. If $l \geq 1$, writing $U = x\mathbb{1} + \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}$ we suppose that c_1 and c'_1 are odd. Note that each conjugacy class contains an element satisfying these conditions. We define $E_{U,U'}$ the following equation:*

$$c_1x^2 + (a_1 - d_1)xy - b_1y^2 \equiv c'_1 \pmod{2^{n-l}}, \quad \text{when l} \geq 1;$$
$$cx^2 + (a-d)xy - by^2 \equiv c' \pmod{2^n}, \quad \text{when l} = 0.$$

Then we have the two following properties:

1. *The matrix U is conjugate to U' if and only if $E_{U,U'}$ has solutions.*
2. *If k is the number of solutions of $E_{U,U}$ then the conjugacy class of U has $m(U) = \frac{1}{k}3 \cdot 2^{3n-3l-2}$ elements.*

Once this Lemma proved, the proof of Theorem 4.5 will follows from the study of the equations $E_{U,U'}$. We will need the Hensel's Lemma (see [7], section 3.2) which states that if $n \geq 1$, $x_0 \in \mathbb{Z}/2^n\mathbb{Z}$ and $P \in \mathbb{Z}[x]$ is a polynomial such that $P(x_0) \equiv 0 \pmod{2^n}$ and $P'(x_0)$ is odd, then there exists a unique element $\tilde{x_0} \in \mathbb{Z}/2^{n+1}\mathbb{Z}$ such that $\tilde{x_0} \equiv x_0 \pmod{2^n}$) and $P(\tilde{x_0}) \equiv 0 \pmod{2^{n+1}}$.

Lemma 4.8. *Let $A \in SL_2(\mathbb{Z}/2^n\mathbb{Z})$, then there exist exactly 8 matrices $\tilde{A} \in SL_2(\mathbb{Z}/2^{n+1}\mathbb{Z})$ such that $\tilde{A} \equiv A \pmod{2^n}$.*

Proof. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then at least one entry of A must be odd. Suppose c is odd. There are exactly 8 ways to lift a, c and d into elements $\tilde{a}, \tilde{c}, \tilde{d}$ in $\mathbb{Z}/2^{n+1}\mathbb{Z}$. Using Hensel's Lemma to the polynomial $P(b) := -\tilde{c}b + \tilde{a}\tilde{d} - 1$ we show that for each of these 8 choices, there is exactly one way to lift b in $\mathbb{Z}/2^{n+1}\mathbb{Z}$ such that the corresponding matrix $\tilde{A}$ lies in $SL_2(\mathbb{Z}/2^{n+1}\mathbb{Z})$. □

Note that this lemma easily implies by induction that the cardinal of $SL_2(\mathbb{Z}/2^n\mathbb{Z})$ is $3 \cdot 2^{3n-2}$.

Proof of Lemma 4.7. Suppose that $X = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \in SL_2(\mathbb{Z}/2^n\mathbb{Z})$ is such that $XUX^{-1} = U'$. A simple computation shows that XUX^{-1} has the form $XUX^{-1} = \begin{pmatrix} * & * \\ cy_2^2 + (a-d)x_2y_2 - bx_2^2 & * \end{pmatrix}$. Thus (y_2, x_2) is solution of $E_{U,U'}$.

Conversely, let (y_2, x_2) be solution of $E_{U,U'}$. The equality $XU = U'X$ is equivalent to the following equations:

$$x_1 a + cy_1 = a'x_1 + b'x_2 \tag{4}$$

$$x_1 b + y_1 d = a'y_1 + b'y_2 \tag{5}$$

$$x_2 a + cy_2 = c'x_1 + d'x_2 \tag{6}$$

$$x_2 b + dy_2 = c'y_1 + d'y_2 \tag{7}$$

The equations (6) and (7) completely determine the values of x_1 and y_1, so of X, modulo 2^{n-l}. Direct computations show that this X is in $SL_2(\mathbb{Z}/2^{n-l}\mathbb{Z})$ and verifies (4) and (5).

Thus an element X in the stabilisator $\mathrm{Stab}(U)$ of U is completely determined modulo 2^{n-l} by a solution of $E_{U,U}$. Using Lemma 4.8, we see that there are exactly 2^{3l} ways to lift such a matrix in $SL_2(\mathbb{Z}/2^n\mathbb{Z})$. So, if k is the number of solutions of $E_{U,U}$ then $|\mathrm{Stab}(U)| = k2^{3l}$. The class formula concludes the proof. □

It remains to compute the number of solutions of the equations $E_{U,U'}$.

Lemma 4.9. *Let $n \geq 1$ and A, B, C, D four integers so that ABD is odd. Let E_n be the following equation:*

$$Ax^2 + Bxy + Cy^2 \equiv D \pmod{2^n}$$

Then E_n has 2^{n-1} solutions if C is even and $3 \cdot 2^{n-1}$ solutions if C is odd.

Proof. We show the result by induction on n using Hensel's Lemma. □

Lemma 4.10. *Let $n \geq 1$ and A, B, C, D be integers such that A and D are *odd. Let* (E) *be the following equation with variables* (x, y) *both in* $SL_2(\mathbb{Z}/p\mathbb{Z})$*:*

$$Ax^2 + 2Bxy + Cy^2 \equiv D \pmod{2^n}$$

We note $\Delta := AC - B^2$*. Then:*

(1) *If* $n = 1$*,* (E) *has* 2 *solutions.*

(2) *If* $n = 2$*, when* $\Delta \equiv 2, 3 \pmod 4$ *then* (E) *has* 4 *solutions. When* $\Delta \equiv 0, 1 \pmod 4$ *then* (E) *has* 8 *solutions if* $AD \equiv 1 \pmod 4$ *and* 0 *otherwise.*

(3) *If* $n \geq 3$*, we have the following cases:*

- **(a)** *If* $\Delta \equiv 0 \pmod 8$ *then* (E) *has* 2^{n+2} *solutions if* $AD \equiv 1 \pmod 8$ *and* 0 *otherwise.*
- **(b)** *If* $\Delta \equiv 2, 4, 6 \pmod 8$ *then* (E) *has* 2^{n+1} *solutions if* $AD \equiv 1 \pmod 8$ *or* $AD \equiv 1 + \Delta \pmod 8$ *and* 0 *otherwise.*
- **(c)** *If* $\Delta \equiv 1, 5 \pmod 8$ *then* (E) *has* 2^{n+1} *solutions if* $AD \equiv 1 \pmod 8$ *or* $AD \equiv 5 \pmod 8$ *and* 0 *otherwise.*
- **(a)** *If* $\Delta \equiv 3, 7 \pmod 8$ *then* (E) *has* 2^n *solutions.*

Proof. First we put $z = Ax + By$. The map from $\mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$ to itself sending (x, y) to (z, y) is bijective as A is odd and we remark that (x, y) is solution of (E) if and only if (z, y) is solution of the following equation, say (E'):

$$z^2 + \Delta y^2 \equiv AD \pmod{2^n}$$

Thus (E) and (E') have the same number of solutions. The number of solutions of (E') is easily computed using the fact (see [10], proposition 5.13) that if a is an odd number and $n \geq 3$, then the equation $x^2 \equiv a \pmod{2^n}$ has 4 solutions modulo 2^n if $a \equiv 1 \pmod 8$ and 0 otherwise. □

End of the Proof of Theorem 4.5. We fix three invariants l, x and τ and study the conjugacy classes of $C(l, x, \tau)$. Let us take two matrices $U, U' \in C(l, x, \tau)$. We can always conjugate them so that they verify the hypothesis of Lemma 4.7. These two matrices are conjugate if and only if the set of solutions of $E_{U,U'}$ is not empty and the number of elements in the conjugacy class of U is computed by using Lemmas 4.7, 4.10 and 4.9. □

4.1.2. **Computation of the characters**

Proposition 4.11. *Let* $A \in SL_2(\mathbb{Z}/2^n\mathbb{Z})$ *and* x, l, s *be its associated invariants. The definition of* s *has been given in Corollary* 4.6 *and will make sense now. The trace* $\mathrm{Tr}(\pi_{2^{n-1}}(A))$ *is given by:*

1. *If* $l = 0$*,* $|\mathrm{Tr}(\pi_{2^{n-1}}(A))|^2 = 2^s$ *if* $0 \leq s \leq n-2$*,* $\mathrm{Tr}(\pi_{2^{n-1}}(A)) = 0$ *if* $s = n-1$ *and* $|\mathrm{Tr}(\pi_{2^{n-1}}(A))|^2 = 2^{n-1}$ *if* $s = n$*.*

2. *If $1 \leq l \leq n-2$ and $x = 1$ then $|\operatorname{Tr}(\pi_{2^{n-1}}(A))|^2 = 2^s$ when $2l \leq s \leq n+l-2$, $\operatorname{Tr}(\pi_{2^{n-1}}(A)) = 0$ when $s = n+l-1$ and $|\operatorname{Tr}(\pi_{2^{n-1}}(A))|^2 = 2^{n+l-1}$ if $s = n+l$.*
3. *If $l = n-1$ and $x = 1$ then $\operatorname{Tr}(\pi_{2^{n-1}}(A)) = 0$.*
4. *If $l = n$ and $x = 1$ ($A = I_2$) then $|\operatorname{Tr}(\pi_{2^{n-1}}(A))|^2 = 2^{2n-2}$.*
5. *If $2 \leq l \leq n$ and $x = -1$ then $|\operatorname{Tr}(\pi_{2^{n-1}}(A))|^2 = 4$.*
6. *If $3 \leq l \leq n$ and $x = 2^{l-1}+1$ then $|\operatorname{Tr}(\pi_{2^{n-1}}(A))|^2 = 2^{2l-2}$.*
7. *If $3 \leq l \leq n$ and $x = 2^{l-1}-1$ then $|\operatorname{Tr}(\pi_{2^{n-1}}(A))|^2 = 4$.*

LEMMA 4.12. *Let a be an odd integer and $D_a := \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in SL_2(\mathbb{Z}/2^n\mathbb{Z})$. Then we have $\pi_{2^{n-1}}(D_a) = \epsilon(\delta_{ai,j})_{i,j}$ where ϵ is a scalar such that $|\epsilon|^2 = 1$.*

Proof. It is proved by a direct computation using the fact that $D_a = T^{-a}ST^{-a^{-1}}ST^{-a}S$. □

Proof of Proposition 4.11. First when $l = 0$ or when $x = 1$, we can suppose that $A = \begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} = ST^cS^{-1}T^{-b}$ with $b = 2^{s-l}b_1$, $c = 2^lc_1$ where b_1 and c_1 are odd.

A simple computation gives:

$$\pi_{2^{n-1}}(A) = \beta^{\pm 3+x}\frac{G(-1,0,2^n)^2}{2^{2n}}\left(\sum_k A^{ck^2+2(j-i)k-bj^2}\right)_{i,j}$$

So:

$$|\operatorname{Tr}(\pi_{2^{n-1}}(A))| = \left|\left(\frac{G(-1,0,2^n)}{2^n}\right)^2\frac{G(c,0,2^n)}{2}\frac{G(-b,0,2^n)}{2}\right|$$

We conclude by using the fact that, if x is odd and $s \in \{0,\dots,n\}$ then (see [2]):

$$|G(x2^s,0,2^n)|^2 = \begin{cases} 2^{s+n}, & \text{when } s \leq n-2; \\ 0, & \text{when } s = n-1; \\ 2^n, & \text{when } s = n. \end{cases}$$

Then when $x = -1$ we can suppose $A = -\begin{pmatrix} 1 & b \\ c & 1+bc \end{pmatrix} = S^{-1}T^cS^{-1}T^{-b}$ with $b = 2^{s-l}b_1$, $c = 2^lc_1$ where b_1 and c_1 are odd. A similar computation gives:

$$\pi_{2^{n-1}}(A)_{i,i} = \epsilon\left(\frac{G(-1,0,2^n)}{2^n}\right)^2 A^{-bi^2}\frac{G(c,4i,2^n)}{2}$$

where $\epsilon = \beta^{c-b-6}$ is a norm one scalar. The Gauss sum $G(c,4i,2^n)$ is not null if and only if $i \in \{0, 2^{n-2}\}$ when $l = n$, 2^{n-3} divides i and 2^{n-2} does not when $l = n-1$ and 2^{l-1} divdes i when $2 \le l \le n-3$.

We conclude by summing $\pi_{2^{n-1}}(A)_{i,i}$ over these i.

Now to compute the traces when $x = 2^{l-1} \pm 1$, we write $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with a odd and $c = 2^l c_1$ with c_1 odd. We use the decomposition $A = ST^{ca^{-1}}SD_{-a}T^{-a^{-1}b}$ and Lemma 4.12 to find that:

$$(\pi_{2^{n-1}}(A))_{i,i} = \epsilon' \left(\frac{G(-1,0,2^n)}{2^n} \right)^2 \frac{G(ca^{-1}, 2(a^{-1}-1)i, 2^n)}{2} A^{a^{-1}bi^2}$$

where ϵ' is a norm one scalar. We conclude by summing $\pi_{2^{n-2}}(A)_{i,i}$ over every i and taking the norm. □

4.1.3. The computation of the sum $\mathbf{S}_{2^n}$

Proof of Proposition 4.2. Set $\mathbf{S}(x,l) := \sum_{A \in C(x,l)} |T(A)|^2$ and $\mathbf{S}(l) := \sum_{A \in C(l)} |T(A)|^2$. By using Propositions 4.6 and 4.11 together, we compute the following sums:

1. $\mathbf{S}(0) = 2^{3n-2} + 3 \cdot 2^{3n-3}(n-1)$.
2. $\mathbf{S}(1,l) = 3 \cdot 2^{3n-l-3}(n-l)$ if $1 \le l \le n-2$.
3. $\mathbf{S}(-1,l) = 3 \cdot 2^{3n-3l}$ if $2 \le l \le n-1$.
4. $\mathbf{S}(1+2^{l-1},l) = 2^{3n-l-2}$ if $3 \le l \le n-1$.
5. $\mathbf{S}(-1+2^{l-1},l) = 2^{3n-3l+2}$ if $3 \le l \le n-1$.
6. $\mathbf{S}(1) = \mathbf{S}(1,1) = 3 \cdot 2^{3n-4}(n-1)$.
7. $\mathbf{S}(2) = \mathbf{S}(1,2) + \mathbf{S}(-1,2) = 3 \cdot 2^{3n-5}(n-2) + 3 \cdot 2^{3n-6}$.
8. $\mathbf{S}(l) = 3 \cdot 2^{3n-l-3}(n-l) + 3 \cdot 2^{3n-3l} + 2^{3n-l-2} + 2^{3n-3l+2}$ if $3 \le l \le n-2$.
9. $\mathbf{S}(n-1) = 3 \cdot 2^3 + 2^5 + 2^{2n-1}$.
10. $\mathbf{S}(n) = 2^3 + 2^{2n-1}$.

We conclude by computing:

$$\begin{aligned} |SL_2(\mathbb{Z}/2^n\mathbb{Z})|\mathbf{S}_{2^n} &= \mathbf{S}(0) + \mathbf{S}(1) + \mathbf{S}(2) + \sum_{l=3}^{n-2} \mathbf{S}(l) + \mathbf{S}(n-1) + \mathbf{S}(n) \\ &= 3 \cdot 2^{3n-2}(n-1) = |SL_2(\mathbb{Z}/2^n\mathbb{Z})| \times (n-1) \quad \square \end{aligned}$$

4.2. HIGHER GENUS FACTORS

The following theorem was shown in [8] when r is odd. We give a different argument and deal with the case $r = 2$ by using the results on the genus one representations.

Theorem 4.13. *If r is prime, the modules $U_r^{g,\pm}$ and $W_{r^n}^{g,\pm}$ are irreducible.*

Proof. First let us handle the $U_r^{g,\pm}$ modules, when r is prime. Denote by $\mathcal{A}$ the $\mathbf{k}_r$-subalgebra of $\mathrm{End}(U_r)$ generated by the operators $\pi_r(\phi)$ for $\phi \in SL_2(\mathbb{Z})$ and by $\mathcal{B}$ the $\mathbf{k}_r$-subalgebra of $\mathrm{End}(U_r^{\otimes g})$ generated by the operators $\pi_{r,g}(\phi)$ for $\phi \in Sp_{2g}(\mathbb{Z})$, when r is odd, and $\phi \in \widetilde{Sp_{2g}}(\mathbb{Z})$, when r is even.

We denote by $\mathcal{A}'$ and $\mathcal{B}'$ their commutant in $\mathrm{End}(U_r)$ and $\mathrm{End}(U_r^{\otimes g})$, respectively. We know from the genus one study that $\mathcal{A}'$ is generated by $\mathbb{1}$ and the symmetry $\theta \in \mathrm{GL}(U_r)$ sending e_i to e_{-i}. There is a natural injection $i : \mathcal{A} \otimes \ldots \otimes \mathcal{A} \hookrightarrow \mathcal{B}$. Now using the fact that the commutant of a tensor product is the tensor product of the commutant we get:

$$\mathcal{B}' \subset i((\mathcal{A} \otimes \ldots \otimes \mathcal{A})') = i(\mathcal{A}' \otimes \ldots \otimes \mathcal{A}')$$

Note that when $r = 2$ then $\theta = \mathbb{1}$ so $\mathcal{B}'$ consists of scalar elements and $\pi_{2,g} = \pi_{2,g}^+$ is irreducible. We can thus suppose that r is odd.

A generic element of $i(\mathcal{A}' \otimes \ldots \otimes \mathcal{A}')$ has the form:

$$C = \sum_{i \in I} \lambda_i a_{i_1} \otimes \ldots \otimes a_{i_g}, \text{ with } I \subset \{1, \ldots, p\}^g \text{ and } a_{i_k} = \mathbb{1} \text{ or } \theta$$

To conclude, we must show that $\mathcal{B}'$ is generated by $\mathbb{1}\otimes\ldots\otimes\mathbb{1}$ and $\theta\otimes\ldots\otimes\theta$, that is, show that if $C \in \mathcal{B}'$ then $a_{i_u} = a_{i_v}$ for all $i \in I$ and $u \neq v$.

Let us choose u, v and set $e := e_1 \otimes \ldots \otimes e_1$. We compute the commutator:

$$[C, \pi_{r,g}(Z_{u,v})](e) = \sum_{i \in I} \lambda_i (A^{4\epsilon_i} - 1)(a_{i_1} \otimes \ldots \otimes a_{i_g})(e)$$

where $\epsilon_i = 0$ if $a_{i_u} = a_{i_v}$ and $\epsilon_i = 1$ elsewhere. Since $A^4 \neq 1$ and the family $\{(a_{i_1} \otimes \ldots \otimes a_{i_g})(e), i \in I\}$ is free, the fact that C is in the commutant of $\mathcal{B}$ implies that $\epsilon_i = 0$ for all i so the two eigenspaces of $\theta \otimes \ldots \otimes \theta$ are irreducible.

Denote by $\mathcal{C}$ the $\mathbf{k}_{r^n}$-subalgebra of $\mathrm{End}(U_{r^n})$ generated by the operators $\pi_r(\phi)$ for $\phi \in SL_2(\mathbb{Z})$ and by the $\mathbf{k}_{r^n}$-subalgebra of $\mathrm{End}(U_{r^n}^{\otimes g})$ generated by the operators $\pi_{r,g}(\phi)$ for $\phi \in Sp_{2g}(\mathbb{Z})$, when r is odd, and $\phi \in \widetilde{Sp_{2g}}(\mathbb{Z})$, when r is even.

We denote by $\mathcal{C}'$ and $\mathcal{D}'$ their commutant in $\mathrm{End}(U_{r^n})$ and $\mathrm{End}(U_{r^n}^{\otimes g})$, respectively. We know from the genus one study that $\mathcal{A}'$ is generated by $\mathbb{1}$ and θ. The natural injection $i : \mathcal{C} \otimes \ldots \otimes \mathcal{C} \hookrightarrow \mathcal{D}$ implies that:

$$\mathcal{D}' \subset i((\mathcal{C} \otimes \ldots \otimes \mathcal{C})') = i(\mathcal{C}' \otimes \ldots \otimes \mathcal{C}')$$

Again we choose a generic element $C = \sum_{i \in I} \lambda_i a_{i_1} \otimes \ldots \otimes a_{i_g} \in i(\mathcal{C}' \otimes \ldots \otimes \mathcal{C}')$ with $I \subset \{1, \ldots, p^n\}^g$ and $a_{i_k} = \mathbb{1}$ or θ and suppose that $C \in B'$. Now remember that W_{r^n} is defined as the orthogonal of $\bar{U}_{r^{n-2}} = \mathrm{Span}(g_i)$ in U_{r^n} and since e_1 is orthogonal to all g_i we deduce that $e = e_1 \otimes \ldots \otimes e_1 \in W_{r^n}^{\otimes g}$.

So the fact that the commutator $[C, \pi_{r^{n+2},g}(Z_{u,v})](e)$ is null if and only if C is a linear combination of $\mathbb{1} \otimes \ldots \otimes \mathbb{1}$ and $\theta \otimes \ldots \otimes \theta$ permits us to conclude. □

Finally, the irreducibility of the factors coming from the decomposition at composite levels $p = r_1^{n_1} \ldots r_k^{n_k}$ follows, using the decomposition (1) from Theorem 1.1, exactly as in the genus one case:

Corollary 4.14. *All the modules of the form $B_{r_1} \otimes \ldots \otimes B_{r_k}$ with $r_1, \ldots,$ r_k distinct prime and $B_{r_i} = U_{r_i}^{g,\pm}$ or $W_{r_i^n}^{g,\pm}$, are irreducible and pairwise distinct.*

Proof. Let $p = 2^\alpha r_1^{n_1} \ldots r_k^{n_k}$ with r_i some distinct odd primes. There is a group isomorphism between $\widetilde{Sp_{2g}}(\mathbb{Z}/2p\mathbb{Z})$ and $\widetilde{Sp_{2g}}(\mathbb{Z}/2^{\alpha+1}\mathbb{Z}) \times Sp_{2g}(\mathbb{Z}/r_1^{n_1}\mathbb{Z}) \times \ldots \times Sp_{2g}(\mathbb{Z}/r_k^{n_k}\mathbb{Z})$, if p is even, and between $Sp_{2g}(\mathbb{Z}/p\mathbb{Z})$ and $Sp_{2g}(\mathbb{Z}/r_1^{n_1}\mathbb{Z}) \times \ldots \times Sp_{2g}(\mathbb{Z}/r_k^{n_k}\mathbb{Z})$, if p is odd.

Denote by $\mathcal{A}_{p,g}$ the subalgebra of $\mathrm{End}(U_p^{\otimes g})$ generated by the operators $\pi_{p,g}(\phi)$. Using the first point of Theorem 1.1, we get an algebra isomorphism:

$$\mathcal{A}_{p,g} \cong \mathcal{A}_{2^\alpha,g} \otimes \mathcal{A}_{r_1^{n_1},g} \otimes \ldots \otimes \mathcal{A}_{r_k^{n_k},g}$$

We conclude using the fact that the commutant of a tensor product is the tensor product of the commutant and use Theorem 4.13. □

5. RELATION WITH THE WITTEN-RESHETIKHIN-TURAEV GENUS ONE REPRESENTATIONS

We now give explicit isomorphisms between the submodules U_p^- and the $SL_2(\mathbb{Z})$-modules V_p defined in [5] extending the relations in [12, 22] to the case where $p \equiv 3 \pmod 4$. We include also their proof for self-completeness of the paper. Corollary 1.2 follows.

Denote by $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ the two generators of $SL_2(\mathbb{Z})$.

Using the basis $\{u_i, i \in I_p\}$ of V_p defined in [5], where

$$I_p := \begin{cases} \{0, 1, 2, \ldots, r-2\}, & \text{if } p = 2r \text{ is even.} \\ \{0, 2, 4, \ldots, p-3\}, & \text{if } p \text{ is odd.} \end{cases}$$

The Reshetikhin-Turaev representations in genus one are characterized by the projective class of the matrices:

$$\rho_p(T) = \left(A^{i(i+2)}\delta_{i,j}\right)_{i,j} \quad \rho_p(S) = c_p\left((-1)^{i+j}[(i+1)(j+1)]\right)_{i,j}$$

where we used the ring $\mathbf{k'}_p := \mathbb{Z}\left[A, \frac{1}{p}\right]/(\phi_{2p}(A))$, so A is always a $2p$-th root of unity, and $c_p := \frac{G(-1,0,2p)}{2p}$ when p is even and $c_p := \frac{G(-1,0,p)}{p}$ when p is odd.

The following theorem was shown in [12] when p is even and in [22] when $p \equiv 1 \pmod 4$. We extend their proofs for $p \equiv 3 \pmod 4$.

Theorem 5.1. *For $p \geq 3$, the $SL_2(\mathbb{Z})$ projective modules U_p^- and V_p are projectively equivalent.*

When p is odd, the module U_p is defined on the ring $\mathbf{k}_p$, where A is a primitive p-th root of unity, whereas V_p is defined on $\mathbf{k'}_p$, where A is a primitive $2p$-th root of unity. In the preceding theorem, we turned U_p^- into a $\mathbf{k'}_p$-module using the ring morphism $\mu : \mathbf{k'}_p \to \mathbf{k}_p$ defined by $\mu(A) = A^4$.

Proof. When $p = 2r$ is even, we define an isomorphism of $\mathbf{k'}_p$-modules $\Psi : V_p \to U_p^-$ by $\Psi(u_i) = e_{r-i-1} - e_{r+i+1}$. We then compute the matrices of π_p^- in the basis $(\Psi(u_i), i = 0, 1, \dots r-2)$:

$$\begin{aligned}
\left\langle \Psi(u_j), \pi_p^-(T)\Psi(u_i) \right\rangle &= A^{(r-i-1)^2}\delta_{i,j} \\
&= A^{(r-1)^2} \cdot A^{-2ri} \cdot A^{i(i+2)} \\
&= A^{(r-1)^2}\rho_p(T)_{i,j}
\end{aligned}$$

$$\begin{aligned}
\left\langle \Psi(u_j), \pi_p^-(S)\Psi(u_i) \right\rangle &= c_p\left(A^{-2(r-i-1)(r-j-1)} - A^{2(r-i-1)(r-j-1)}\right) \\
&= c_p \cdot A^{2r(i+j)}\left(A^{-2(i+1)(j+1)} - A^{2(i+1)(j+1)}\right) \\
&= -\rho_p(S)_{i,j}
\end{aligned}$$

So π_p^- and ρ_p are projectively equivalent when p is even.

Then when $p \geq 3$ is odd, we turn U_p^- into a $\mathbf{k'}_p$-module via the ring morphism $\mu : \mathbf{k'}_p \to \mathbf{k}_p$ defined by $\mu(A) := A^4$. We define an isomorphism $\Psi : V_p \to U_p^-$ of $\mathbf{k'}_p$-modules *via* $\Psi(u_i) := e_{\frac{p-1-i}{2}} - e_{\frac{p+i+1}{2}}$. We then compute the matrices of π_p^- in the basis $(\Psi(u_i), i = 0, 2, 4, \dots p-3)$:

$$\begin{aligned}
\left\langle \Psi(u_j), \pi_p^-(T)\Psi(u_i) \right\rangle &= \mu(A)^{\left(\frac{p-1-i}{2}\right)^2}\delta_{i,j} \\
&= A^{(p-i-1)^2}\delta_{i,j} \\
&= (-A) \cdot \rho_p(T)_{i,j}
\end{aligned}$$

$$\begin{aligned}
\left\langle \Psi(u_j), \pi_p^-(S)\Psi(u_i) \right\rangle &= c_p\left(\mu(A)^{-2(\frac{p-1-i}{2})(\frac{p-1-j}{2})} - \mu(A)^{2(\frac{p-1-i}{2})(\frac{p-1-j}{2})}\right) \\
&= c_p\left(A^{-2(p-i-1)(p-1-j)} - A^{2(p-i-1)(p-1-j)}\right) \\
&= -\rho_p(S)_{i,j}
\end{aligned}$$

And the proof is completed. □

6. THE WITTEN-RESHETIKHIN-TURAEV TQFTS ARE DETERMINED BY 3-MANIFOLDS INVARIANTS WITHOUT FRAMED LINKS

In this section, we briefly review the universal construction of TQFTs of [5] and prove Theorem 1.3. For simplicity, we omit the complications due to the presence of an anomaly for it does not change the proof and refer to [5, 16] for more complete discussion. We also only write the proof when p is even for the odd case easily follows using Theorem 1.5 of [5].

Let $\mathcal{M}^{links}$ denotes the set of classes (M, L) of closed oriented 3 manifolds M equipped with an embedded framed link $L \subset M$, modulo preserving-orientation homeomorphisms. In [4,24], the authors define a map $\tau_p : \mathcal{M}^{links} \to \mathbb{C}$ multiplicative for connected sums and sending the manifold M with opposite orientation to the complex conjugate of the image of M.

Let Σ be a closed oriented surface and $\mathcal{V}(\Sigma)$ be the complex vector space freely generated by (homeomorphism classes of) elements (M, ϕ, L) where M is a compact oriented three manifold, $\phi : \partial M \to \Sigma$ an orientation-preserving homeomorphism and $L \subset M$ is an embedded framed link (possibly empty). The space $\mathcal{V}(\Sigma)$ is naturally equipped with a bilinear form $\langle \cdot, \cdot \rangle_p$ associated to τ_p defined as follows. If $\mathbb{M}_1 = (M_1, \phi_1, L_1)$ and $\mathbb{M}_2 = (M_2, \phi_2, L_2)$ are two cobordisms in $\mathcal{V}(\Sigma)$, we can glue them to obtain $\mathbb{M}_1 \cup \mathbb{M}_2 := (M_1 \cup_{\phi_1^{-1} \circ \phi_2} M_2, L_1 \cup L_2) \in \mathcal{M}^{links}$. We then define $\langle \mathbb{M}_1, \mathbb{M}_2 \rangle_p := \tau_p(\mathbb{M}_1 \cup \mathbb{M}_2)$ and extend the form to $\mathcal{V}(\Sigma)$ by bi-linearity.

Eventually define the vector space:

$$V_p(\Sigma) := \mathcal{V}(\Sigma) \Big/ \ker(\langle \cdot, \cdot \rangle_p)$$

By definition, any cobordism $\mathbb{M} \in \mathcal{V}(\Sigma)$ defines a vector $Z_p(\mathbb{M}) \in V_p(\Sigma)$ by passing to the quotient. Moreover if $\mathbb{M}$ is a cobordism between to surfaces Σ_1 and Σ_2, we can associate a linear map $V_p(\mathbb{M}) : V_p(\Sigma_1) \to V_p(\Sigma_2)$ by sending $Z_p(\mathbb{M}')$ to $Z_p(\mathbb{M} \circ \mathbb{M}')$. Such a functorial assignation $\Sigma \to V_p(\Sigma)$ and $\mathbb{M} \to V_p(\mathbb{M})$ is what is called a TQFT. Note that the spaces $U_{p,g}$ of the Weil representations also fit into this framework (see [15, 20]).

Denote by $X_p(\Sigma) \subset V_p(\Sigma)$ the subspace generated by classes of cobordisms with an empty link. Theorem 1.3 states that whenever 4 does not divide p, then $X_p(\Sigma) = V_p(\Sigma)$.

By construction the subspace $X_p(\Sigma)$ is determined by the restriction of the three manifolds invariant τ_p to the subset $\mathcal{M} \subset \mathcal{M}^{links}$ of closed oriented three manifolds without framed links.

We now turn to the proof of Theorem 1.3. Simply denote by V_p the space $V_p(S^1 \times S^1)$ as in the previous section. Let $u_1 := Z_p(D^2 \times S^1, id, L) \in V_p$ be the vector associated to the manifold $D^2 \times S^1$ with trivial boundary identification and the link $L = \{0\} \times S^1 \subset D^2 \times S^1$ with parallel framing. Theorem 1.3 easily follows from the following:

Lemma 6.1. *If* 4 *does not divide* p, *then* $u_1 \in X_p(S^1 \times S^1)$.

Proof of Theorem 1.3 using Lemma 6.1. The following argument is the same as Robert's argument in [29] who proved Theorem 1.3 when p is prime. We briefly reproduce it for self-completeness of the paper. Let $\mathbb{M} = (M, \phi, L) \in \mathcal{V}(\Sigma)$ be a cobordism and $Z_p(\mathbb{M}) \in V_p(\Sigma)$ its class in the quotient. We have to show that $Z_p(\mathbb{M})$ is a linear combination of vectors associated to cobordisms without links, so we suppose that L is not empty.

Let $L_i \subset L$ be a connected component and choose N_i a tubular neighborhood of L_i in M homeomorphic to $D^2 \times S^1$. Writing $\mathbb{M} \setminus N_i = (M \setminus N_i, \phi \cup \phi_{N_i}, L \setminus L_i) \in \mathcal{V}(\Sigma \bigsqcup S^1 \times S^1)$, we have $(\mathbb{M} \setminus N_i) \cup_{\partial N_i} (N_i, \phi_{N_i}, L_i) = \mathbb{M}$.

Passing to the quotient, we get $Z_p(\mathbb{M}) = V_p(\mathbb{M} \setminus N_i) \circ Z_p(N_i, \phi_{N_i}, L_i)$, where $V_p(\mathbb{M} \setminus N_i)$ is a linear map from V_p to $V_p(\Sigma)$ and $Z_p(N_i, \phi_{N_i}, L_i)$ is the vector $u_1 \in V_p$. Lemma 6.1 implies the existence of three manifolds $\mathbb{M}_1, \ldots, \mathbb{M}_k$ bounding $S^1 \times S^1$ without framed links embedded and scalars $\lambda_1, \ldots, \lambda_k$ in $\mathbb{C}$ such that $u_1 = \sum_i \lambda_i Z_p(M_i)$. It follows that:

$$Z_p(\mathbb{M}) = \sum_i \lambda_i Z_p((\mathbb{M} \setminus N_i) \circ \mathbb{M}_i))$$

Thus $Z_p(\mathbb{M})$ is a linear combination of vectors associated to cobordisms with one component less than L. We conclude by induction on the number of components of L. □

The proof of Lemma 6.1 relies on the fact that $X_p \subset V_p$ is invariant under the action of $SL_2(\mathbb{Z})$ on V_p. Let $u_0 \in V_p$ denotes the vector associated to $D^2 \times S^1$ without framed links embedded and let $\Lambda_0, \Lambda_1 \subset V_p$ be the $SL_2(\mathbb{Z})$ cyclic subspaces associated to u_0 and u_1, respectively.

Lemma 6.2. *If* 4 *does not divide* p, *then* $\Lambda_0 = \Lambda_1$.

Proof. Since Λ_0 and Λ_1 are $SL_2(\mathbb{Z})$ invariant subspaces by definition, we have to show that for any irreducible subspace $B \subset V_p \cong U_p^-$, we have $\Lambda_0 \cap B = \Lambda_1 \cap B$. Note that $\Lambda_i \cap B$ is either $\{0\}$ or B.

Using the identification $\Psi : V_p \cong U_p^-$ of (the proof of) Theorem 5.1 and Corollary 1.2, we know explicit basis for such irreducible modules. Denote by $\Lambda_i' := \Psi(\Lambda_i) \subset U_p^-$ and remark that if $p = 2r$, we have:

$$\psi(u_0) = e_{r-1} - e_{r+1} \quad \psi(u_1) = e_{r-2} - e_{r+2} \ .$$

Note $p = 2r_1^{n_1} \ldots r_k^{n_k}$ the decomposition of p in primes numbers, and choose $B = U_2 \otimes B_1 \otimes \ldots \otimes B_k \subset U_p^-$ an irreducible submodule as in Corollary 1.2. We have to study whether the projection of $\psi(u_i)$ on B is null or not.

First consider the case where there exists in index i such that $n_i \geq 2$ and $B_i \neq W^{\pm}_{r_i^{n_i}}$. Then $B_i \subset U^{\pm}_{r_i^{n_i-2}}$ which is included in the subspace spanned by vectors e_k such that r_i divides k. But clearly r_i does not divide $r-1, r+1, r-2$ nor $r+2$ thus the projection of both $\psi(u_0)$ and $\psi(u_1)$ on B is null and we have $\Lambda'_0 \cap B = \Lambda'_1 \cap B = \{0\}$.

Next suppose that for each i such that $n_i \geq 2$, we have $B_i = W^{\epsilon_i}_{r_i^{n_i}}$ where ϵ_i is either -1 or $+1$. Given two integers x and n, we will denote by $[x]_n \in \mathbb{Z}/n\mathbb{Z}$ the class of x modulo n. Let x be any integer such that none of the r_i divides x. Set:

$$v_B := e_{[x]_2} \otimes e^{\epsilon_1}_{[x]_{r_1^{n_1}}} \otimes \ldots \otimes e^{\epsilon_k}_{[x]_{r_k^{n_k}}} \in B$$

where we used the notation $e_i^{\pm} := e_i \pm e_{-i}$. By using the fact that $< e_i, e_i^{\epsilon} >= 1$ and $< e_{-i}, e_i^{\epsilon} >= (-1)^{\frac{1-\epsilon}{2}}$, we compute:

$$\begin{aligned} < v_B, e_x - e_{-x} > &= \left\langle e_{[x]_2} \otimes e^{\epsilon_1}_{[x]_{r_1^{n_1}}} \otimes \ldots \otimes e^{\epsilon_k}_{[x]_{r_k^{n_k}}}, e_{[x]_2 \otimes e_{[x]_{r_1^{n_1}}}} \otimes \ldots \otimes e_{[x]_{r_k^{n_k}}} \right\rangle \\ &\quad - \left\langle e_{[x]_2} \otimes e^{\epsilon_1}_{[x]_{r_1^{n_1}}} \otimes \ldots \otimes e^{\epsilon_k}_{[x]_{r_k^{n_k}}}, e_{[-x]_2} \otimes e_{[-x]_{r_1^{n_1}}} \right. \\ &\qquad \left. \otimes \ldots \otimes e_{[-x]_{r_k^{n_k}}} \right\rangle \\ &= 1 - (-1)^{\sum_i \frac{1-\epsilon_i}{2}} = 2 \neq 0 \end{aligned}$$

where we used in the last line the fact that there is an odd number of i such that $\epsilon_i = -1$ for $B \subset U_p^-$. In particular the orthogonal projection of e_x^- on B is non-trivial whenever none of the r_i divides x. Applying this to $x = r-1$ and $x = r-2$, we get that $\Lambda'_0 \cap B = \Lambda'_1 \cap B = B$. □

Proof of Lemma 6.1. Since u_0 belongs to X_p by definition and that X_p is invariant under the action of $SL_2(\mathbb{Z})$, we have $\Lambda_0 \subset X_p$. Now Lemma 6.2 implies that $\Lambda_1 \subset X_p$ thus $u_1 \in X_p$. □

Acknowledgements. The author is thankful to R. Bacher, C. Blanchet, F. Costantino, L. Funar, and J. Marché for valuable discussions and to G.Masbaum for pointed him the reference [27]. The author acknowledges support from the grant ANR 2011 BS 0102001 ModGroup, the GDR Tresses, the GDR Platon and the GEAR Network.

REFERENCES

[1] A. Adler and S. Ramanan, *Moduli of abelian varieties.* Lecture Notes in Mathematics **1644**, Springer-Verlag, Berlin 1996.

[2] B.C. Berndt and R.J. Evans, *The determination of Gauss sums.* Bull. Amer. Math. Soc. (N.S.) **5** (1981), *2*, 107–129.

[3] M.V. Berry and J.H. Hannay, *Quantization of linear maps on a torus-Fresnel diffraction by a periodic grating.* Phys. D **1** (1980), *3*, 267–290.

[4] C. Blanchet, N. Habegger, G. Masbaum and P. Vogel, *Three-manifold invariants derived from the Kauffman bracket.* Topology **31** (1992), *4*, 685–699.

[5] C. Blanchet, N. Habegger, G. Masbaum and P. Vogel, *Topological quantum field theories derived from the Kauffman bracket.* Topology **34** (1995), *4*, 883–927.

[6] A. Bouzouina and S. De Bièvre, *Equipartition of the eigenfunctions of quantized ergodic maps on the torus.* Comm. Math. Phys. **178** (1996), 83–105.

[7] T. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable.* Math. Surveys **VI**, Amer. Math. Soc. New York, 1951.

[8] G. Cliff, D. McNeilly and F. Szechtman, *Weil representations of symplectic groups over rings.* J. Lond. Math. Soc. (2), **62** (2000), *2*, 423–436.

[9] F. Deloup and C. Gille, *Abelian quantum invariants indeed classify linking pairings.* J. Knot Theory Ramifications **10** (2001), *2*, 295–302.

[10] M. Demazure, *Cours d'algèbre. Primalité. Divisibilité. Codes.* Nouv. Bibl. Math. **1**, Cassini, Paris, 1997.

[11] F. Faure, S. Nonnenmacher and S. De Bièvre, *Scarred eigenstates for quantum cat maps of minimal periods.* Comm. Math. Phys. **239** (2003), *3*, 449–492.

[12] M. Freedman and V. Krushkal, *On the asymptotics of quantum* SU(2) *representations of mapping class groups.* Forum Math. **18** (2006), *2*, 293–304.

[13] L. Funar, *Some abelian invariants of 3-manifolds.* Rev. Roumaine Math. Pures Appl. **45** (2000), *5*, 825–861.

[14] L. Funar and W. Pitsch, *Finite quotients of symplectic groups vs. mapping class groups.* 2011.

[15] R. Gelca and A. Uribe, *From classical theta functions to topological quantum field theory.* In: L. Katzarkov *et al.* (Eds.), *The influence of Solomon Lefschetz in Geometry and Topology.* Contemp. Math. **621**, Amer. Math. Soc., Providence, 35–68, 2014.

[16] P.M. Gilmer and G. Masbaum, *Maslov index, lagrangians, mapping class groups and TQFT.* Forum Math. **25** (2013), *5*, 1067–1106.

[17] T. Gocho, *The topological invariant of three-manifolds based on the* U(1) *gauge theory.* J. Fac. Sci. Univ. Tokyo Sect. IA Math. **39** (1992), *1*, 169–184.

[18] J. Igusa, *On the graded ring of theta-constants. II.* Amer. J. Math. **88** (1966), 221–236.

[19] 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.

[20] J. Korinman, *On some quantum representations of the mapping class groups of surfaces.* PhD thesis, Institut Fourier, 2014.

[21] P. Kurlberg and Z. Rudnick, *Hecke theory and equidistribution for the quantization of linear maps of the torus.* Duke Math. J. **103** (2000), *1*, 47–77.

[22] M. Larsen and Z. Wang, *Density of the SO(3) TQFT representation of mapping class groups.* Comm. Math. Phys. **260** (2005), *3*, 641–658.

[23] W.B.R. Lickorish, *A finite set of generators for the homeotopy group of a* 2*-manifold.* Proc. Cambridge Philos. Soc. **60** (1964), 769–778.

[24] W.B.R. Lickorishi, *Invariants for* 3*-manifolds from the combinatorics of the Jones polynomial.* Pacific J. Math. **149** (1991), *2*, 337–347.

[25] G. Lion and M. Vergne, *The Weil representation, Maslov index and theta series.* Progr. Math. **6**, Birkhäuser, Boston, 1980.

[26] H. Murakami, T. Ohtsuki and M. Okada, *Invariants of three-manifolds derived from linking matrices of framed links.* Osaka J. Math. **29** (1992), *3*, 545–572.

[27] T. Calamoneri, *On character values and decomposition of the Weil representation associated to a finite abelian group.* J. Anal. **17** (2009), 73–85.

[28] J. Roberts, *Skeins and mapping class groups.* Math. Proc. Cambridge Philos. Soc. **115** (1994), 53-77.

[29] J. Roberts, *Irreducibility of some quantum representations of mapping class groups.* J. Knot Theory Ramifications **10** (2001), *5*, 763–767.

[30] I.E. Segal, *Lectures at the* 1960 *Boulder summer seminar*, 1962.

[31] J-P. Serre, *Linear representations of finite groups.* Grad. Texts in Math. **42**, Springer Verlag, New-York–Heidelberg–Berlin, 1977.

[32] D. Shale, *Linear symmetries of free boson fields.* Trans. Amer. Math. Soc. **103** (1962), 149–167.

[33] G. Shimura, *Moduli and fibre systems of abelian varieties.* Ann. of Math. (2) **83** (1966), 294–338.

[34] A. Weil, *Sur certains groupes d'opérateurs unitaires.* Acta Math. **111** (1964), 143–211.

[35] E. Witter, *Quantum field theory and the Jones polynomial.* Comm. Math. Phys. **121** (1989), *3*, 351–399.

Received 23 January 2017

Universidade Federal de São Carlos
Rodovia Washington Luís, Km 235, s/n
São Carlos - SP, 13565-905
julienkorinman@dm.ufscar.br