ANNALES DE L'I. H. P., SECTION A

E. BUFFENOIR
A. COSTE
J. LASCOUX
P. DEGIOVANNI
A. BUHOT

Precise study of some number fields and Galois actions occurring in conformal field theory

Annales de l'I. H. P., section A, tome 63, n° 1 (1995), p. 41-79
<http://www.numdam.org/item?id=AIHPA_1995__63_1_41_0>

Ann. Inst. Henri Poincaré,

Vol. 63, n° 1, 1995, p. 41-79. *Physique théorique*

Precise study of some number fields and Galois actions occurring in conformal field theory

by

E. BUFFENOIR, A. COSTE ([1]), J. LASCOUX

Centre de Physique Théorique, Ecole Polytechnique,
91128 Palaiseau Cedex, France.

and

P. DEGIOVANNI, A. BUHOT

Laboratoire de Physique Théorique, ENSLAPP ([2])
ENS Lyon, 46, allée d'Italie, 69364 Lyon Cedex 07, France.

ABSTRACT. – We present a detailed study of some number fields and Galois groups occurring in two dimensional models built from Wess-Zumino-Novikov-Witten (WZNW) and $\mathbb{Z}/N\mathbb{Z}$ theories. The observed structures may be relevant for the classification of rational conformal theories (RCFT) and for the understanding of links and three manifolds invariants.

More precisely we look at M, the number field generated by the modular matrix elements S_{ij} [1], [2] and at L, the subfield generated by the quotients $S_{ij}/S_{\rho j}$, introduced in ref. [3], following [4] and even, for $\mathbb{Z}/N\mathbb{Z}$ theories [5], at the field generated by Moore and Seiberg data.

RÉSUMÉ. – Nous étudions l'action galoisienne de certains corps de nombres apparaissant dans les théories conformes des champs dites rationelles en approfondissant les théorèmes de [3], [4], [5]. Cette étude est illustrée par les exemples des modèles de Wess-Zumino-Novikov-Witten et

([1]) On leave till Oct. 94 from CPT CNRS Luminy.

([2]) URA 1436 du CNRS, associée à l'ENS de Lyon et au LAPP(IN2P3) Annecy Le Vieux.

des théories $\mathbb{Z}/N\mathbb{Z}$. Ces structures présentent un intérêt pour la classification des théories conformes bidimensionnelles rationnelles et la compréhension des invariants topologiques d'entrelacs et de variétés tridimensionnelles que l'on en déduit.

---

0. INTRODUCTION

Since the development of Conformal Field Theory the modular aspects of Rational Conformal Field Theories (RCFT) have become an important aspect of the subject. For example, Cardy showed in [1] how to use modular properties of genus one characters to obtain the operator content of the theory. In particular he noticed the importance of the genus one S and T matrices which also play a central role in the present paper.

These considerations were systematized by Moore and Seiberg in 1988 ([6], [7]) who introduced a finite number of matrices, called Moore and Seiberg's data, which satisfy the so-called Moore and Seiberg's polynomial equations. These data represent the modular properties of conformal blocks for the following values of the genus g and number of punctures n: $(0,3)$, $(0,4)$ and $(1,0)$, $(1,1)$. They also examined the modular invariance problem and formulated the "naturality argument" which gives the form of the genus one partition function in terms of characters relative to the maximal symmetry algebra of the RCFT. This result has also been obtained independently by R. Dijkgraaf and E. Verlinde [8].

Starting from first principles, A. Cappelli, C. Itzykson and J. B. Zuber [2], followed by A. Kato [9], T. Gannon and Q. Ho Kim [10], Ph. Ruelle, E. Thiran, J. Weyers [11], impressively succeeded in classifying the genus one physical modular invariants built from Kac Moody algebras associated with $su(2)$ and $su(3)$ and the corresponding coset models.

Later, the modular aspects of 2D RCFTs were connected to three dimensional topological field theories by E. Witten in his paper on the Jones polynomial [12]. Various constructions of three dimensional topological field theories were produced, either from the representation theory of some quasi-Hopf algebras [13], [14] or from solutions to Moore and Seiberg's equations [15], [16]. It finally appeared that, from any solution to Moore and Seiberg's equations, one can construct a topological field theory in three dimensions.

An interesting question is then to understand the structure of this set of invariants. This is a kind of preliminary to the classification of RCFTs. It may help understanding how powerful the invariants are for solving problems in knot/link or three-manifold theory. A possible strategy is to find some kind of "symmetry" which relates various invariants.

In fact, a proposal in this direction has been made in [5], [17] using the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The basic idea dates back to Grothendieck [18] and is the following: let us consider the system of all modular multiplicities $\mathfrak{M}_{g,n}$ together with a few fundamental operations such as the "sewing of surfaces", the "forgetting of marked points" and so on. These operations should have a counter part in the system of all fundamental groupoids ([3]) $\widehat{T}_{g,n}$ in the sense of algebraic geometry, which we will not define here. Moreover, there is a natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on this tower of groupoids. Then, conjecturing that RCFTs provide projective representations of the $\widehat{T}_{g,n}$'s, one is naturally led to conjecture the existence of an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ o n these representations, or on solutions to Moore and Seiberg's equations, or on 3D topological theories. One may also think of reconstructing as much as possible of a rational theory from some algebraic (collections of number fields) or geometric data.

In [3], this action was shown to be responsible of the so called "parity rule" (or "arithmetical symmetry") recently discovered among torus partition functions. In [18], it is also conjectured that for a certain class of RCFTs, this Galois action is nothing but the usual Galois action (Galois acting on algebraic numbers) on Moore and Seiberg's matrices (coefficient by coefficient).

These reasons motivated the study of some particular examples. It also appeared that the analysis was simpler on the "genus one data", that is to say the S matrix, the phases $(\exp(2\pi i h_j))_j$ and $\exp(2\pi i c/8)$. In the case of the S matrix, one can show that all matrix elements belong to some cyclotomic extension of $\mathbb{Q}$ [4] and that the Galois action transforms one matrix element of S into another one, up to a sign [3]. The aim of this paper is to illustrate these facts on a few examples.

In the first section, we recall the general facts concerning the Galois action on S. We also discuss the structure of $\mathrm{Gal}(\mathbb{Q}(S_{ij})_{i,j})/\mathbb{Q})$ and compare it with $\mathrm{Gal}(\mathbb{Q}(\lambda_i^{(j)})_{i,j})/\mathbb{Q})$ where the $\lambda_i^{(j)}$'s are the fusion eigenvalues. In section 2, we shall consider the case of WZW models and give a

([3]) With respect to suitable families of base points.

complete list of the number fields generated by S's matrix elements in the case of $su(2)$ and $su(3)$ models at any level as well as some deep relationship between these number fields and the polynomial presentations of the Pasquier-Verlinde algebra.

We shall also discuss the $\mathbb{Z}/N\mathbb{Z}$ theories. The genus one data have been computed in [19] and we shall explicitly compute the Galois action on them. Since the partition function of any boundaryless compact oriented three-manifold without any decoration ([4]) can be computed in terms of these data, we will discuss the Galois effect on these invariants (*see* sections 3 and 4). Let us mention that they can be computed using some Gauss sums.

1. GALOIS ACTION ON RATIONAL THEORIES

For convenience of the reader, let us recall in this first section some notations and results of ref. [3], [4].

The Hilbert space H of a RCFT admits a decomposition into a finite number of blocks:

$$H = \bigoplus_{a,b\in B} \mathcal{N}_{ab} \bar{V}_a \otimes_I V_b \tag{1}$$

Let us denote by $a = \rho$ the index of the identity block, corresponding to the unit of the fusion ring. We exclude here the heterotic case and assume V_b and $\bar{V}_a$ are irreducible representations of isomorphic algebras $A, \bar{A}$; ($\otimes_I$ means that central extension parts of A and $\bar{A}$ are identified). B is the finite set of such representations occuring in (1). $\mathcal{N}_{ab}$ is the non negative integral matrix encoding multiplicities of isotypic blocks. The partition function on modulus τ torus reads:

$$Z(\tau) = \sum_{a,b\in B} \chi_a^* \mathcal{N}_{ab} \chi_b \tag{2}$$

The $SL(2,\mathbb{Z})$ modular invariance of $Z(\tau)$ requires commutation of $\mathcal{N}$ with the unitary symmetric S and T matrices satisfying

$$S^2 = (ST)^3 = C, \quad C^2 = I \tag{3}$$

([4]) No graph embedded in it.

where C is called the conjugation involution.

In [4], De Boer and Goeree have discovered a lot of deep properties satisfied by RCFT's. In their Appendix B they consider the Galois group [20] of the number field L generated by the quotients of S matrix elements $(S_{aj}/S_{\rho j})_{a,j\in B}$. They proved that this group is abelian and these quotients are sums of roots of unity with integer coefficients. Furthermore, for a fixed, these quotients are the eigenvalues of the left regular representation of the fusion ring, *i.e.* roots of the characteristic polynomial $\det(\lambda - N_a)$, where N_a is the fusion matrix between A-primary fields:

$$(N_a)_b^c = N_{ab}^c\ , \qquad \Phi_a\Phi_b = \sum_c N_{ab}^c\ \Phi_c \tag{4}$$

A striking result stemming out of [4] and pointed out in [3], is that one has a group morphism from Galois automorphisms σ of the number field M generated by the modular matrix elements S_{ij} to permutations $j \to j^\sigma$ of B and for each such σ a collection of signs $\varepsilon_\sigma(i) = \pm 1$ such that

$$\sigma(S_{ij}) = \varepsilon_\sigma(j) S_{i,j^\sigma} = \varepsilon_\sigma(i) S_{i^\sigma,j} \tag{5}$$

Commutativity of $\mathrm{Gal}(M/\mathbb{Q})$ has also been proved. Equation (5) immediately implies the cocycle relation:

$$\varepsilon_{\sigma\sigma'}(i) = \varepsilon_\sigma(i)\ \varepsilon_{\sigma'}(i^\sigma) = \varepsilon_{\sigma'}(i)\ \varepsilon_\sigma(i^{\sigma'}) \tag{6}$$

1.1. Galois symmetry of torus matrix

Since $\mathcal{N}$ has integer elements, applying any automorphism σ to $(S\mathcal{N})_{ik} = (\mathcal{N}S)_{ik}$ leads to

$$\begin{aligned}\sum_j \mathcal{N}_{ij}\ \varepsilon_\sigma(j)\ S_{j^\sigma\ k} &= \varepsilon_\sigma(i) \sum_j S_{i^\sigma\ j}\ \mathcal{N}_{jk} \\ &= \varepsilon_\sigma(i)\ \sum_j \mathcal{N}_{i^\sigma\ j}\ S_{jk} \\ &= \varepsilon_\sigma(i)\ \sum_j \mathcal{N}_{i^\sigma\ j^\sigma}\ S_{j^\sigma\ k}\end{aligned}$$

Invertibility of S brings the conclusion:

$$\mathcal{N}_{i^\sigma\ j^\sigma} = \varepsilon_\sigma(i)\varepsilon_\sigma(j)\mathcal{N}_{ij} \tag{7}$$

which is a very powerful selection rule, recently discovered and exploited in ([10], [11]).

1.2. Symmetry of fusion rules

As a start, apply any σ to Verlinde's formula:

$$\frac{S_{aj}}{S_{\rho j}}\,\frac{S_{bj}}{S_{\rho j}} = \sum_{c\in B} N_{ab}^{c}\,\frac{S_{cj}}{S_{\rho j}} \tag{8}$$

Image of the l.h.s. is:

$$\varepsilon_\sigma(a)\varepsilon_\sigma(b)\,\frac{S_{a^\sigma\, j}S_{b^\sigma\, j}}{(S_{\rho^\sigma\, j})^2} = \varepsilon_\sigma(a)\varepsilon_\sigma(b)\sum_c N_{a^\sigma\, b^\sigma}^{c}\,\frac{S_{cj}}{S_{\rho j}}\left(\frac{S_{\rho j}}{S_{\rho^\sigma j}}\right)^2$$

$$= \varepsilon_\sigma(a)\varepsilon_\sigma(b)\sum_c N_{a^\sigma\, b^\sigma}^{c^\sigma}\,\frac{S_{c^\sigma\, j}}{S_{\rho j}}\left(\frac{S_{\rho j}}{S_{\rho^\sigma j}}\right)^2$$

whereas image of the r.h.s. is:

$$\sum_c N_{ab}^{c}\,\frac{\varepsilon_\sigma(c)}{\varepsilon_\sigma(\rho)}\,\frac{S_{c^\sigma\, j}}{S_{\rho^\sigma\, j}}$$

Equating these two images gives

$$\sum_c \left(\frac{\varepsilon_\sigma(c)\varepsilon_\sigma(\rho)}{\varepsilon_\sigma(a)\varepsilon_\sigma(b)}\,N_{ab}^{c}\,\frac{S_{\rho^\sigma\, j}}{S_{\rho j}} - N_{a^\sigma b^\sigma}^{c^\sigma}\right) S_{c^\sigma\, j} = 0 \tag{9}$$

Contract finally with $(S^{-1})_{j\, d^\sigma}$ in order to obtain the interesting rule:

$$N_{a^\sigma b^\sigma}^{d^\sigma} = \sum_{c,j}\frac{\varepsilon_\sigma(c)\varepsilon_\sigma(\rho)}{\varepsilon_\sigma(a)\varepsilon_\sigma(b)}\,N_{ab}^{c}\,S_{c^\sigma\, j}\,\frac{S_{\rho^\sigma\, j}}{S_{\rho j}}(S^{-1})_{j\, d^\sigma} \tag{10}$$

$$= \sum_{c\in B}\frac{\varepsilon_\sigma(c)\varepsilon_\sigma(\rho)}{\varepsilon_\sigma(a)\varepsilon_\sigma(b)}\,N_{ab}^{c}\,N_{c^\sigma\ \rho^\sigma}^{d^\sigma}$$

Setting

$$(G_\sigma)_b{}^c = \varepsilon_\sigma(b)\,\delta_{b^\sigma}^{c} \tag{11}$$

we get:

$$G_1 = I, \qquad G_{\sigma\sigma'} = G_\sigma G_{\sigma'} \tag{12}$$

which tells us that we have a representation of $\mathrm{Gal}(M/\mathbb{Q})$ defined over $\mathbb{Q}$. Setting $a = \rho^{\sigma^{-1}}$, one sees that N_{ρ^σ} is invertible (and its inverse has integral matrix elements). Furthermore if one sets

$$M_{\sigma,a} = \varepsilon_\sigma(a)\varepsilon_\sigma(\rho)N_{a^\sigma}\,(N_{\rho^\sigma})^{-1} \tag{13}$$

Equation (10) is equivalent to

$$M_{\sigma,a} = (G_\sigma)^{-1} N_a G_\sigma \tag{14}$$

so that $\Phi_a \longrightarrow M_{\sigma,a}$ is a set of $\mathbb{Q}$-representations of the fusion algebra equivalent to the regular representation.

When $\rho^\sigma = \rho$,

$$\Phi_a \longrightarrow \varepsilon_\sigma(a)\varepsilon_\sigma(\rho)\Phi_{a^\sigma} \tag{15}$$

is an algebraic automorphism of the fusion algebra.

1.3. Lines of study

Let us describe some tracks one may follow if one were to study any rational conformal field theory where the Verlinde formula holds :

1. Start for instance from the fusion ring Fus generated by the matrices N_a , look at their characteristic and minimal polynomials (over $\mathbb{Q}$). As shown by Di Francesco and Zuber [21], if one of the N_a , say N_1, is non degenerate, the fusion algebra (that is to say Fus considered as a vector space over the field $\mathbb{Q}$) is generated by N_1.

2. The arithmetic field $L = \mathbb{Q}((\lambda_a^{(j)}))$ is then the splitting field of these minimal polynomials.

One may determine its Galois group $\mathrm{Gal}(L/\mathbb{Q})$ (which is abelian) and its faithful image into the permutation group $\mathrm{Perm}\,(B)$ determined by

$$\sigma(\lambda_a^{(j)}) = \lambda_a^{(j^\sigma)} \tag{16}$$

where the λ_a^j 's are the eigenvalues of N_a, adequately ordered.

3. Of course the existence and unicity (up to a global permutation) of this ordering comes from the existence of the invertible modular S matrix, such that

$$\lambda_a^{(j)} = S_{aj} \,/ S_{\rho j} \tag{17}$$

so that when one explicitly knows S one may as well start from (17).

4. $S_{\rho\rho}$ is then the real positive constant such that the symmetric matrix

$$S_{aj} = \frac{\lambda_a^{(j)}}{\lambda_j^{(\rho)}} \, S_{\rho\rho} \tag{18}$$

is unitary. Or, taking into account the symmetry of S:

$$S_{\rho\rho} = \sqrt{\frac{1}{\sum_j |\lambda_a^{(j)}/\lambda_j^{(\rho)}|^2}} \tag{19}$$

valid for any $a \in B$.

5. In view of (18) and (19) $M = L((S_{aj})_{a,j}) = L(S_{\rho\rho})$ is at most a quadratic extension of L.

6. The signs $\varepsilon_\sigma(\rho)$, $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ are determined by

$$\sigma(S_{\rho\rho}) = \varepsilon_\sigma(\rho)\, S_{\rho^\sigma\ \rho} \tag{20}$$

7. From which all the $\varepsilon_\sigma(a)$'s can be obtained by

$$\varepsilon_\sigma(a) = \varepsilon_\sigma(\rho)\, \frac{S_{a\ \rho^\sigma}}{S_{\rho\ a^\sigma}} \tag{21}$$

More generally, for any j

$$\varepsilon_\sigma(a)\, \lambda_{a^\sigma}^{(j)} = \varepsilon_\sigma(\rho)\, \lambda_a^{(j^\sigma)}\, \lambda_{\rho^\sigma}^{(j)} \tag{22}$$

8. When M is a quadratic extension of L one has the group isomorphism

$$\begin{aligned} \mathrm{Gal}(M/\mathbb{Q}) &\sim \mu_2 \bowtie_\eta \mathrm{Gal}(L/\mathbb{Q}) \\ \sigma &\longrightarrow (\varepsilon_\sigma(\rho)\ ,\ \sigma_{|L}) \end{aligned} \tag{23}$$

with the group law

$$\sigma\sigma' \sim (\varepsilon\ ,\ \sigma_{|L}) *_\eta (\varepsilon'\ ,\ \sigma'_{|L}) = (\varepsilon\varepsilon'\, \eta_{\sigma\sigma'}\ ,\ \sigma\sigma'_{|L}) \tag{24}$$

$$\eta_{\sigma\sigma'} = \frac{\varepsilon_\sigma(\rho^{\sigma'})}{\varepsilon_\sigma(\rho)} = \frac{\varepsilon_{\sigma\sigma'}(\rho)}{\varepsilon_\sigma(\rho)\, \varepsilon_{\sigma'}(\rho)} \tag{25}$$

In order to study this extension, one can ask whether it is split, *i.e.* does there exists a group morphism

$$\gamma : \quad \mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathrm{Gal}(M/\mathbb{Q})$$

which is a right inverse of the restriction, *i.e.* $\gamma(g)_{|L} = g$ for all $g \in \mathrm{Gal}(L/\mathbb{Q})$.

Since $M = L(S_{\rho\rho})$ and $[M : L] = 2$, $\sigma = \gamma(g)$ is uniquely determined by a choice of sign $\varepsilon_g(\rho) = \varepsilon_\sigma(\rho)$ defining $\sigma(S_{\rho\rho}) = \varepsilon_\sigma(\rho) S_{\rho\, g(\rho)}$ (we will use notation $g(\rho)$ instead of ρ^g, which will be more pleasant when iterating). Therefore $\mathrm{Gal}(M/\mathbb{Q})$ is split if one can choose consistently the signs $\varepsilon_g(\rho)$ for all $g \in \mathrm{Gal}(L/\mathbb{Q})$.

But this abelian Galois group is isomorphic to a direct product of cyclic groups:

$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \mu_{m_1} \times \cdots \times \mu_{m_l} \tag{26}$$

Let $(g_i)_{i=1,\ldots,l}$ be a choice of generators corresponding to this factorization. Since

$$\sigma\, \sigma'(S_{\rho\rho}) = \varepsilon_g(\rho)\, \varepsilon_{g'}(\rho)$$
$$S_{g(\rho)\, g'(\rho)} = \sigma'\, \sigma(S_{\rho\rho})$$

commutativity is satisfied and we can consider each cyclic factor independently . For such a factor the only condition is to insure that the image σ_i of g_i satisfies $(\sigma_i)^{m_i} = \mathrm{Id}_M$. This is equivalent to :

$$\varepsilon_{\sigma_i}(\rho)\, \varepsilon_{\sigma_i}(g_i(\rho)) \cdots \varepsilon_{\sigma_i}(g_i^{m_i-1}(\rho)) = 1 \tag{27}$$

Since

$$\varepsilon_\sigma(g^k(\rho)) = \varepsilon_\sigma(\rho)\, \frac{S_{g(\rho)\, g^k(\rho)}}{S_{\rho\, g^{k+1}(\rho)}} = \varepsilon_\sigma(\rho)\, \lambda_{g(\rho)}^{g^k(\rho)}\, \frac{S_{\rho\, g^k(\rho)}}{S_{\rho\, g^{k+1}(\rho)}}$$

it is also equivalent to :

$$(\varepsilon_{\sigma_i}(\rho))^{m_i} \prod_{k=0}^{m_i-1} \lambda_{g_i(\rho)}^{(g_i^k(\rho))} = 1 \tag{28}$$

Therefore this extension is **not a direct product** if and only if there exists such an even m_i with

$$\prod_{k=0}^{m_i-1} \lambda_{g_i(\rho)}^{(g_i^k(\rho))} = -1. \tag{29}$$

On the contrary, when such a splitting holds, we can define $\tau = \sigma\, \gamma(\sigma_{|L})^{-1} \in \mathrm{Gal}(M/L)$ so that since the groups are abelian one has the direct product factorization

$$\begin{array}{c} \sigma \longrightarrow (\tau, \sigma_{|L}) \\ \mathrm{Gal}(M/\mathbb{Q}) \simeq \mathrm{Gal}(M/L) \times \mathrm{Gal}(L/\mathbb{Q}) \simeq \mu_2 \times \mathrm{Gal}(L/\mathbb{Q}) \end{array} \tag{30}$$

and the cocycle (25) is a coboundary.

A more efficient criterion is

(31) $\mathrm{Gal}(M/\mathbb{Q})$ is split if and only if there exists α such that $\alpha^2 \in \mathbb{Q}$ and $M = L(\alpha)$

If this holds, any element of M is uniquely written $x+y\alpha$ with $x, y \in L$ and

$$\sigma(x + y\alpha) = \sigma_{|L}(x) + \sigma_{|L}(y)\eta_\sigma \alpha\ , \qquad \eta_\sigma = \pm 1 \tag{32}$$

so that

$$\sigma \longrightarrow (\eta_\sigma\ , \sigma_{|L})$$
$$\mathrm{Gal}(M/\mathbb{Q}) \longrightarrow \mu_2 \times \mathrm{Gal}(L/\mathbb{Q})$$

is a group isomorphism. Conversely, if there exists a section γ : $\mathrm{Gal}(L/\mathbb{Q}) \longrightarrow \mathrm{Gal}(M/\mathbb{Q})$ set

$$M' = \{x \in M / \gamma(\sigma)(x) = x \text{ for all } \sigma \in \mathrm{Gal}(L/\mathbb{Q})\} \tag{33}$$

Then Galois fundamental theorem gives

$$\mathrm{Gal}(M/M') = \gamma(\mathrm{Gal}(L/\mathbb{Q})) \tag{34}$$

which implies $[M : M'] = [L : \mathbb{Q}]$ and

$$[M' : \mathbb{Q}] = \frac{[M : \mathbb{Q}]}{[M : M']} = [M : L] = 2 \tag{35}$$

insuring the existence of $\alpha \in M'$ such that

$$M' = \mathbb{Q}(\alpha)\ , \qquad \alpha^2 \in \mathbb{Q} \tag{36}$$

But α does not belong to L , because otherwise if one had M' included into L, the restrictions to L of elements of $\mathrm{Gal}(M/M')$ would cover only $\mathrm{Gal}(L/M')$, which contradicts (34) ; this ends the proof of (31).

This criterion can even be expressed in terms of $S_{\varrho\varrho}$. Write $S_{\varrho\varrho} = r + \alpha s$ with $r, s \in L$. Since De Boer and Goeree have proved that $S^2_{\varrho\varrho} = r^2 + \alpha^2 s^2 + 2\alpha r s \in L$ and since α and $S_{\varrho\varrho}$ do not belong to L, one has necessarily $r = 0$, *i.e.*

(37) $\mathrm{Gal}(M/\mathbb{Q})$ is split if and only if there exists $s \in L$ and an integer a such that a is not a square and $S_{\varrho\varrho} = \sqrt{a}\ s$

9. One may also think of using this Galois structure at best for building modular invariants of the form (2) , for instance by using $[G + G^{-1}, S] = 0$

(G defined in (11)), as noticed independently in [24]. We will rather here, as a first step, try to get some insights into classical situations.

10. One may even look at bigger number fields, such as the one generated by diagonal elements T_j of the modular T matrix. Their Galois action may bring us outside the category of usually considered rational theories. Nevertheless the transformed data can still be used to define topological invariants. We will adopt this broader point of view when presenting the examples of topological $\mathbb{Z}/N\mathbb{Z}$ three dimensional theories. Following [17], the relevant field in this context is the extension K generated by the S_{ij} elements, the $(\exp(2i\pi h_j)\ )_j$ and $\exp(2i\pi c/8)$. We will call such data

(38) $(S_{ij}, \exp(2i\pi h_j),\ \exp(2\pi ic/8)\ )$ solution of $(ST)^3 = C,\ S^4 = I$

"Moore and Seiberg" data and will consider in section 3 the orbits of Galois action on such collections of algebraic numbers.

2. KAC MOODY SITUATION

Let us consider the case of a WZNW model based on a compact simple Lie algebra $\mathcal{G}$.

2.1. General case

As pointed out by Gepner [25], the formal Weyl character formula [26] allows one to express the S matrix elements (which we index by shifted weights $p = \lambda + \rho$) in terms of values of characters for the related compact Lie group:

$$(39)\quad S_{p\,p'} = \frac{i^{|\Delta_+|}}{n^{r/2}\sqrt{|R^V|}} \sum_{w\in W} \varepsilon(w)\ \exp\left(\frac{-2i\pi w(p)\cdot p'}{n}\right)$$

$$(40)\quad = \frac{2^{|\Delta_+|}}{n^{r/2}\sqrt{|R^V|}} \prod_{\alpha\in\Delta_+} \sin\left(\frac{\pi}{n}\alpha(H_{p'})\right) \mathrm{ch}_\lambda\left(\exp\left(-\frac{2i\pi\ H_{p'}}{n}\right)\right.$$

$$(41)\quad = S_{\rho\,p'}\ \mathrm{ch}_\lambda\left(\exp -\frac{2i\pi\ H_{p'}}{n}\right)$$

where Δ_+ is the set of positive roots, $\rho = \frac{1}{2}\sum_{\alpha\in\Delta_+}$, r is the rank, $|R^V| = |R^{V*}/R^V|$ is the determinant of the coroot lattice, $n = k + h^V$, h^V dual Coxeter number. $H_{p'}$ is the matrix in the Cartan subalgebra of $\mathcal{G}$ such

that $\lambda \cdot p' = \lambda(H_{p'})$ for any weight λ. We normalize the scalar product as in Bourbaki and Humphreys [26].

If we express any root in terms of the simple roots α_i as

$$\alpha = \sum_{i=1}^{r} a_i \ \alpha_i \tag{42}$$

we have

$$S_{\rho\rho} = \frac{2^{|\Delta_+|}}{n^{r/2}\sqrt{|R^V|}} \prod_{\alpha\in\Delta_+} \sin\left(\frac{\pi \sum_{i=1}^{r} a_i \ (\alpha_i \cdot \alpha_i)}{2n} \right) \tag{43}$$

2.2. $su(N)$ case

For these algebras the matrices corresponding to the fundamental weights are

$$H_{\mu_j} = \sum_{m=1}^{j} \delta_m - \frac{j}{N} \sum_{m=1}^{N} \delta_m \tag{44}$$

where δ_m is the diagonal matrix with only 1 at element $m \times m$. Furthermore $n = k + N$, $\sqrt{|R^V|} = \sqrt{N}$, $|\Delta_+| = N(N-1)/2$. Rather than writing redundant formulae, let us look directly at the lowest rank algebras :

2.3. $\widehat{su(2)}_k$ case

Horizontal parts of integrable $\widehat{su(2)}_k$ integrable highest weights are $\Lambda = \Lambda_1\mu_1$ where $\Lambda_1 = 2j \in \{0, 1, \cdots, k\}$ is the number of boxes in the corresponding Young tableau ($\Lambda_1 = 0$ being the trivial $su(2)$ representation), j is the spin of the representation, μ_1 is the fundamental weight. Let us set $p = \Lambda_1 + 1$.

The relevant finite Fourier transform matrix is

$$\begin{aligned} S_{pq} &= \frac{i}{\sqrt{2n}} \left(e^{-i\pi pq/n} - e^{i\pi pq/n}\right) \\ &= \sqrt{\frac{2}{n}} \sin\left(\frac{\pi pq}{n}\right) \end{aligned} \tag{45}$$

It satisfies $S^2 = I_{n-1}$.

Identification of the number fields L, M

$$L = \mathbb{Q}\Big(\Big(\frac{S_{pq}}{S_{1q}}\Big)\Big) = \mathbb{Q}\Big(\cos\Big(\frac{\pi}{n}\Big)\Big) = \mathbb{Q}_{2n} \cap \mathbb{R} \tag{46}$$

This is due to the fact that $\cos(\pi/n) = S_{2\,1}/2S_{1\,1} \in L$ and these quotients can be expressed in terms of Chebyshev polynomials T and U which have integer coefficients:

$$\sin(pq\theta)/\sin(q\theta) = U_{p-1}(\cos(q\theta)) = U_{p-1}(T_q(\cos(\theta))). \tag{47}$$

This field is well known, its Galois group consists of the $\varphi(2n)/2$ automorphisms g_l for $1 \leq l \leq n-1$ and l coprime with $2n$ such that

$$g_l\Big(\cos\Big(\frac{\pi}{n}\Big)\Big) = \cos\Big(\frac{l\pi}{n}\Big). \tag{48}$$

Notice that $\varphi(2n)/2$ equals $\varphi(n)$ when n is even and $\varphi(n)/2$ when n is odd, $\varphi(n)$ being the number of integers between 1 and n, coprime with n (1 being coprime with anything !). This group is isomorphic to $(\mathbb{Z}/2n\mathbb{Z})^*, \times) / (\{1,-1\}, \times)$. It is clearly cyclic when n is prime.

It is straightforward to check directly that L is normal: since

$$U_{n-1}(x) = 2^{n-1}\prod_{j=1}^{n-1}\Big(x - \cos\Big(\frac{j\pi}{n}\Big)\Big) \tag{49}$$

has rational coefficients, any $\mathbb{Q}$-automorphism sends $\cos(\pi/n)$ into a $\cos(l\pi/n) = T_l(\cos(\pi/n)) \in L$.

Let us now study

$$M = \mathbb{Q}\Big(\cos\Big(\frac{\pi}{n}\Big), \sqrt{\frac{2}{n}}\,\sin\Big(\frac{\pi}{n}\Big)\Big). \tag{50}$$

In fact, let us prove that

$$n = 2m \quad \text{is even implies } M = L \tag{51}$$

In this case,

$$\begin{aligned}\sin\Big(\frac{\pi}{n}\Big) &= \sin\Big(\frac{\pi}{2} - \frac{(m-1)\pi}{2m}\Big) \\ &= \cos\Big(\frac{(m-1)\pi}{2m}\Big) = T_{m-1}\Big(\cos\Big(\frac{\pi}{n}\Big)\Big)\end{aligned} \tag{52}$$

So that in this case equation (50) simplifies into

$$M = \mathbb{Q}\Big(\cos\Big(\frac{\pi}{n}\Big), \sqrt{m}\Big) = L(\sqrt{m})$$

Let p be a prime divisor of m :

- If $p = 2$, n is a multiple of 4 and

$$\frac{1}{\sqrt{2}} = \cos\Big(\frac{\pi n/4}{n}\Big) = T_{n/4}\Big(\cos\Big(\frac{\pi}{n}\Big)\Big) \in L$$

- If $p \equiv 1 \pmod 4$ we have the following Gauss sum formula [28]:

$$\begin{aligned} \sqrt{p} &= \sum_{j=1}^{p-1} \Big(\frac{j}{p}\Big) \exp\Big(\frac{2i\pi j}{p}\Big) \\ &= 2 \sum_{j=1}^{(p-1)/4} \Big(\frac{j}{p}\Big) \cos\Big(\frac{2j\pi}{p}\Big) \\ &\quad - 2\Big(\frac{-2}{p}\Big) \sum_{j=0}^{(p-5)/4} \Big(\frac{2j+1}{p}\Big) \cos\Big(\frac{(2j+1)\pi}{p}\Big) \end{aligned} \tag{53}$$

where $\Big(\frac{j}{p}\Big)$ is the Legendre symbol, equal to ± 1. $\Big(\frac{-2}{p}\Big) = +1$ if $p \equiv 1 \pmod 8$, and $= -1$ if $p \equiv 5 \pmod 8$. Equation (53) implies that

$$\sqrt{p} \in \mathbb{Q}_p \bigcap \mathbb{R} \subset \mathbb{Q}_{2n} \bigcap \mathbb{R} = \mathbb{Q}\Big(\cos\Big(\frac{\pi}{n}\Big)\Big)$$

- If $p \equiv 3 \pmod 4$ one has similarly ([5])

$$\sqrt{p} = 2 \sum_{j=1}^{(p-1)/2} \Big(\frac{j}{p}\Big) \sin\Big(\frac{2\pi j}{p}\Big) \tag{54}$$

and $\sin\left(\frac{2\pi j}{p}\right) = \cos\left(\frac{\pi(p-4)j}{2p}\right)$ belongs to $\mathbb{Q}_{4p} \bigcap \mathbb{R}$ which is included into

$$\mathbb{Q}_{2n} \bigcap \mathbb{R} = \mathbb{Q}\left(\cos\left(\frac{\pi}{\aleph}\right)\right).$$

This ends the proof of proposition (51).

The converse is true, *i.e.*

$$n \text{ is odd implies } [M : L] = 2 \tag{55}$$

To prove this, let us use some results on cyclotomic fields detailed in Appendix B: For n odd, we have:

$$\begin{aligned} \mathbb{Q}_n = \mathbb{Q}_{2n} &= \mathbb{Q}\left(\cos\left(\frac{\pi}{n}\right),\ i\ \sin\left(\frac{\pi}{n}\right)\right) \\ \mathbb{Q}_{4n} &= \mathbb{Q}\left(\cos\left(\frac{\pi}{n}\right),\ \sin\left(\frac{\pi}{n}\right),\ i\right) \\ \mathbb{Q}_{8n} &= \mathbb{Q}\left(\cos\left(\frac{\pi}{n}\right),\ \sin\left(\frac{\pi}{n}\right),\ \sqrt{2},\ i\right) \end{aligned} \tag{56}$$

Using $[\mathbb{Q}_l : \mathbb{Q}] = \varphi(l)$, one shows that for n odd i doesn't belong to $\mathbb{Q}_n$ and $\sqrt{2}$ doesn't belong to $\mathbb{Q}_{4n}$. On the other hand Gauss' sum formulae seen above show that either $\sqrt{n}$ or $i\sqrt{n} \in \mathbb{Q}_n$. Therefore $\sqrt{n}$ and $\sin\left(\frac{\pi}{n}\right)$ do belong to $\mathbb{Q}_{4n}$.

Now, if we had $M = L$, *i.e.* $\sqrt{\frac{2}{n}}\ \sin\left(\frac{\pi}{n}\right) \in L \subset \mathbb{Q}_n$, this would imply $\sqrt{2} \in \mathbb{Q}_{4n}$. This ends the proof of (55).

As seen above, our Galois group can, for n odd, be identified with the extension

$$\begin{aligned} \mathrm{Gal}(M/\mathbb{Q}) &\longrightarrow \mu_2 \rtimes \mathrm{Gal}(L/\mathbb{Q}) \\ \sigma &\longrightarrow (\varepsilon_\sigma\ , \sigma_l\ ) \end{aligned} \tag{57}$$

with group law

$$(\varepsilon, \sigma_l) \cdot (\varepsilon', \sigma_{l'}) = \left(\varepsilon\,\varepsilon' \mathrm{sign}\left(\sin\left(\frac{ll'\,\pi}{n}\right)\right), \sigma_l\,\sigma_{l'}\right) \tag{58}$$

([5]) For practical use, let us also mention

$$\sqrt{p} = 2\sum_{j=1}^{(p-3)/4}\left(\frac{j}{p}\right)\sin\left(\frac{2j\pi}{p}\right) + 2\left(\frac{-2}{p}\right)\sum_{j=0}^{(p-3)/4}\left(\frac{2j+1}{p}\right)\sin\left(\frac{(2j+1)\pi}{p}\right)\left(\frac{-2}{p}\right) = 1$$

if $p \equiv 3 \bmod 8$ and $= -1$ if $p \equiv 7 \bmod 8$ for instance $\sqrt{7} = 2\left(\sin\left(\frac{2\pi}{7}\right) + \sin\left(\frac{3\pi}{7}\right) - \sin\left(\frac{\pi}{7}\right)\right)$.

The splitting criterion (37) reads here for n odd:

$$S_{\varrho\varrho} = \sqrt{\frac{2}{n}} \sin\left(\frac{\pi}{n}\right) = \sqrt{a}\, s$$

with $s \in \mathbb{Q}(\cos(\pi/n)) = \mathbb{Q}(\exp(2i\pi/2n)) \cap \mathbb{R}$ and a a positive integer which is not a square. This condition is equivalent to the existence of a positive integer m such that $2nm$ is not a square and

$$\sqrt{m} \sin(\pi/n) \in \mathbb{Q}(\exp(2i\pi/2n)) = \mathbb{Q}(\exp(2i\pi/n))$$

But since $i \sin(\pi/n) \in \mathbb{Q}(\exp(2i\pi/n))$, for $su(2)$ one has the equivalent criterion:

(59) Gal$(M/\mathbb{Q})$ is split if and only if there exists a positive integer m such that $2nm$ is not a square and $i\sqrt{m} \in \mathbb{Q}(\exp(2i\pi/n))$

As a consequence

(60) When n has at least one prime factor $p \equiv 3 \pmod 4$, Gal$(M/\mathbb{Q}) \simeq \mu_2 \times$ Gal$(L/\mathbb{Q})$

As a counter example, note that in the case $n = 5$, studied in details in [3], Gal$(M/\mathbb{Q}) \simeq \mu_4$ is **not** split, in agreement with (29)!

One can sum up some of these facts in the following table.

Fusion rules for $\widehat{su(2)}_k$. – The fusion rules are:

$$\Phi_p\, \Phi_q = \sum_{r=|p-q|+1}^{n-1-|n-p-q|} \Phi_r = \sum_{r=|p-q|+1}^{p+q-1-2\eta(p+q-n)} \Phi_r \tag{61}$$

where $p, q, r \in B = \{1, \cdots, n-1\}$, $n = k+2$, the sum is only on $r \equiv p - q + 1 \ mod\ 2$ and

$$\begin{cases} \eta = 0 & \text{if} \quad p+q < n \\ \eta = 1 & \text{if} \quad 2n > p+q \geq n \end{cases} \tag{62}$$

TABLE 1. – *Fields L, M, Galois group of M, some cyclotomic field K containing M. μ_m denotes the multiplicative cyclic group of order m.*

k	$n = k+2$	$L = \mathbb{Q}(\{S_{ij}/S_{\rho j}\})$	$M = \mathbb{Q}(\{S_{ij}\})$	$\mathrm{Gal}(M/\mathbb{Q})$	K
1	3	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{2})$	μ_2	$\mathbb{Q}_8$
2	4	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{2})$	μ_2	$\mathbb{Q}_8$
3	5	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{5-\sqrt{5}})$	μ_4	$\mathbb{Q}_{40}$
4	6	$\mathbb{Q}(\sqrt{3})$	$\mathbb{Q}(\sqrt{3})$	μ_2	$\mathbb{Q}_{12}$
6	8	$\mathbb{Q}(\sqrt{2-\sqrt{2}})$	$\mathbb{Q}(\sqrt{2-\sqrt{2}})$	μ_4	$\mathbb{Q}_{16}$
10	12	$\mathbb{Q}(\sqrt{2},\sqrt{3})$	$\mathbb{Q}(\sqrt{2},\sqrt{3})$	$\mu_2 \times \mu_2$	$\mathbb{Q}_{24}$
16	18	$\mathbb{Q}(\cos(\pi/18))$	$\mathbb{Q}(\cos(\pi/18))$	μ_6	$\mathbb{Q}_{36}$
28	30	$\mathbb{Q}(\cos(\pi/30))$	$\mathbb{Q}(\cos(\pi/30))$	$\mu_4 \times \mu_2$	$\mathbb{Q}_{60}$
$2m-2$	$2m$	$\mathbb{Q}(\cos(\pi/(2m)))$	$\mathbb{Q}(\cos(\pi/(2m)))$	$\frac{(\mathbb{Z}/4m\mathbb{Z})^*}{\{\pm 1\}}$	$\mathbb{Q}_{4m}$
$2m-1$	$2m+1$	$\mathbb{Q}(\cos(\pi/(2m+1)))$	$L\left(\sqrt{\frac{2}{n}}\sin\left(\frac{\pi}{n}\right)\right)$	see text	$\mathbb{Q}_{16m+8}$

As shown in [21], the fusion algebra is isomorphic to $\mathbb{Q}[x]/U_{n-1}(x/2)$, U_{n-1} being a Chebyshev polynomial. For completeness, let us give the factorized form of these polynomials $P_n(x) = U_{n-1}(x/2)$ for $\widehat{su(2)}_{n-2}$. The interpretation will be discussed after deriving similar expressions for $\widehat{su(3)}_{n-3}$.

2.4. $\widehat{su(3)}_k$ case

The diagonal matrix corresponding to a shifted weight

$$p = p_1\mu_1 + p_2\mu_2, \qquad p_1 + p_2 \leq n-1 \tag{63}$$

$$\text{is} \quad H_p = \frac{1}{3}\,\mathrm{diag}\left(2p_1+p_2,\ p_2-p_1,\ -(p_1+2p_2)\right) \tag{64}$$

TABLE 2. – *The characteristic polynomials of the fundamental generator $x = \Phi_2$ of the fusion algebra.*

$$
\begin{aligned}
P_3 &= (x-1)(x+1)\\
P_4 &= x(x^2-2)\\
P_5 &= (x^2+x-1)(x^2-x-1)\\
P_6 &= x(x-1)(x+1)(x^2-3)\\
P_7 &= (x^3-x^2-2x+1)(x^3+x^2-2x-1)\\
P_8 &= x(x^2-2)(x^4-4x^2+2)\\
P_9 &= (x-1)(x+1)(x^3-3x+1)(x^3-3x-1)\\
P_{10} &= x(x^2+x+1)(x^2-x-1)(x^4-5x^2+5)\\
P_{11} &= (x^5-x^4-4x^3+3x^2+3x-1)\cdot(x^5+x^4-4x^3-3x^2+3x+1)\\
P_{12} &= x(x-1)(x+1)(x^2-2)(x^2-3)(x^4-4x^2+1)\\
P_{18} &= x(x-1)(x+1)(x^2-3)\cdot(x^3-3x+1)(x^3-3x-1)(x^6-6x^4+9x^2-3)\\
P_{30} &= x(x-1)(x+1)(x^2-3)(x^2-x-1)(x^2+x-1)\\
&\quad\times(x^4-5x^2+5)(x^4+x^3-4x^2-4x+1)(x^4-x^3-4x^2+4x+1)\\
&\quad\times(x^8-7x^6+14x^4-8x^2+1)
\end{aligned}
$$

One also has

$$S_{\rho\rho} = \frac{4\sqrt{3}}{3n}\left(1-\cos\left(\frac{2\pi}{n}\right)\right)\sin\left(\frac{2\pi}{n}\right) \tag{65}$$

The character of the fundamental representation $p = \mu_1$ being simply the trace, the eigenvalues of N_f are:

$$\lambda_f^{(p)} = \lambda_f^{(p_1,p_2)} = \zeta^{-2p_1-p_2} + \zeta^{p_1-p_2} + \zeta^{p_1+2p_2}, \quad \text{with } \zeta = \exp\left(\frac{2i\pi}{3n}\right) \tag{66}$$

Since

$$\cos\left(\frac{2\pi}{n}\right) = \frac{\lambda_f^{(\rho)}-1}{2} \in L = \mathbb{Q}((\lambda_f^{(p)})) \tag{67}$$

we have:

$$M = L(S_{\rho\rho}) = L\Big(\sqrt{3}\ \sin\Big(\frac{2\pi}{n}\Big)\Big) \tag{68}$$

Furthermore,

$$i\sqrt{3}\ \in\ L. \tag{69}$$

because if we set $p_3 = n - p_1 - p_2$, we have

$$\lambda_f^{(p_3,\ p_1)} = \exp\Big(\frac{2i\pi}{3}\Big)\ \lambda_f^{(p_1,\ p_2)}. \tag{70}$$

In particular $\exp\Big(\frac{2i\pi}{3}\Big) = \lambda_f^{(n-2,1)}/\lambda_f^{(1,1)}$. Thus, if we set $c = \cos\Big(\frac{2\pi}{n}\Big)$ and $s = \sin\Big(\frac{2\pi}{n}\Big)$, (68) is equivalent to

$$M\ =\ L(is) \tag{71}$$

But for $n \geq 6$, we can consider ([6])

$$\lambda_f^{(1,4)} = \zeta^{-6} + \zeta^{-3} + \zeta^{9} = 4c^3 + 2c^2 - 2c - 1 + 2i\ s\ (2c+1)(c-1) \tag{72}$$

which shows that $is \in L$. We have thus proved: $\zeta^3 = c + is \in L$ and $\mathbb{Q}\Big(\exp\Big(\frac{2i\pi}{n}\Big)\Big) \subset L = M \subset \mathbb{Q}\Big(\exp\Big(\frac{2i\pi}{3n}\Big)\Big)$.

But $\zeta = \lambda_f^{(1,3)}/(\zeta^{-6} + \zeta^{-3} + \zeta^{6}\ ) \in L$ showing that

$$\text{for}\ \ n \geq 6 \qquad L = M = \mathbb{Q}\Big(\exp\Big(\frac{2i\pi}{3n}\Big)\Big) \tag{73}$$

Fusion rules for $\widehat{su(3)}_k$. – In a very dense paper [25], Gepner has shown that Fus is isomorphic to the polynomial algebra in two variables x, y which satisfy relations

$$\frac{\partial V_n}{\partial x} = \frac{\partial V_n}{\partial y} = 0 \tag{74}$$

where

$$V_n = \frac{1}{n}\Big(\ q_1^n + q_2^n + \frac{1}{q_1^n q_2^n}\Big) \tag{75}$$

([6]) The idea of this proof is due to T. Gannon , whom we warmly thank.

is reexpressed in terms of the characters

$$x = q_1 + q_2 + \frac{1}{q_1 q_2} \qquad y = q_1 q_2 + \frac{1}{q_1} + \frac{1}{q_2} \tag{76}$$

Another theorem, due to Di Francesco, Zuber and Bauer [21], asserts that Fus is isomorphic to $\mathbb{Q}[x]/P_n(x)$ where $P_n(x)$ is the characteristic polynomial of N_f, of degree $(n-1)(n-2)/2$, whose roots are the $\lambda_{\mu_1}^{(p)}$'s.

We have checked for $n \leq 12$ using the Gröbner bases package available on Maple algebraic system (*see* the program below) that the ideal of $\mathbb{Q}[x, y]$ generated by $\dfrac{\partial V_n}{\partial x}$ and $\dfrac{\partial V_n}{\partial y}$ is equal to the ideal generated by $P_n(x)$ and an element of the form $y - Y(x)$, which form a "Gröbner basis" [27] of it. For instance at $n = 7$ the following polynomial lies in this ideal:

$$\begin{aligned} 46228\ y\ &- 59833\ x^2\ - 157075\ x^5 \\ +120859\ x^8\ &- 30564\ x^{11}\ + 1865\ x^{14} \end{aligned}$$

This seems to us a striking property of these polynomial algebras !

One can even prove:

$$P_n(x) \text{ is of the form } P(x^3) \text{ or } xP(x^3) \text{ or } x^2P(x^3) \tag{77}$$

This is because multiplication in $SU(3)$ by the center element $j\mathrm{Id}$ ($j = \exp(2i\pi/3)$) corresponds to the transformation $x \mapsto x' = jx$, $y \mapsto y' = j^2 y$, and $V_n(x', y') = j^n\ V_n(x, y)$.

Therefore $\dfrac{\partial V_n}{\partial x} = \dfrac{\partial V_n}{\partial y} = 0$ implies

$$\frac{\partial V_n}{\partial x}(jx, j^2 y) = \frac{\partial V_n}{\partial y}(jx, j^2 y) = 0$$

and

$$P_n(jx) = 0 \quad \text{in } \mathbb{Q}[x]/P_n(x)\ . \tag{78}$$

Similarly

$$P_n(j^2 x) = 0\ . \tag{79}$$

Writing $P_n(x) = P_n^{(0)}(x^3) + xP_n^{(1)}(x^3) + x^2 P_n^{(2)}(x^3)$, linear combinations of $P_n = 0$, (78) and (79) give

$$P_n^{(0)} = xP_n^{(1)} = x^2 P_n^{(2)} = 0 \quad \text{in } \mathbb{Q}[x]/P_n(x)$$

But if two of these three polynomials were non zero their greatest common divisor would be a generator of degree smaller than $P_n(x)$, which ends the proof of (77).

Example: $\widehat{su(3)}_2$. – The characteristic polynomial of N_f is

$$(80) \quad P_5(x) = x^6 - 4x^3 - 1 \; = \; (x^2 - x - 1)(x^4 + x^3 + 2x^2 - x + 1)$$

For $\zeta = \exp(2i\pi/15)$, it is a funny exercise to check by use of the cyclotomic polynomials $\Phi_{15}(\zeta) = \zeta^8 - \zeta^7 + \zeta^5 - \zeta^4 + \zeta^3 - \zeta + 1 \; = 0$ and $\Phi_5(t)$ $(t = \zeta^3$ here), that $\lambda_f^{(2,1)} = \zeta^{-5} + \zeta + \zeta^4$ (and therefore its Galois conjugates), are roots of $x^4 + x^3 + 2x^2 - x + 1$. Since the roots of $x^6 - 4x^3 - 1$ are

$$(81) \qquad x = \exp(2i\pi l/3) \quad \left(\frac{1 \pm \sqrt{5}}{2}\right)$$

one can identify easily $L = \mathbb{Q}(\sqrt{5},\ i\sqrt{3})$, and

$$(82) \qquad M = \mathbb{Q}(\exp(2i\pi/15)\ ) = \mathbb{Q}\left(\sqrt{5},\ i\sqrt{3},\ \sqrt{3}\sqrt{5-\sqrt{5}}\ \right).$$

For the lowest values of n, let us list the characteristic polynomials $P_n(x)$ of N_f.

These polynomials have been obtained with help of the following Maple program:

```
with(grobner);
w(1,x,y)  :=  x;
w(2,x,y)  :=  x^{2}-2*y;
w(3,x,y)  :=  x^{3}-3*x*y+3;
for n from 4 to 12 do
w(n,x,y) := simplify(x*w(n-1,x,y)-y*w(n-2,x,y)+w(n-3,x,y));
vx(n,x,y) := simplify( simplify(diff(w(n,x,y),x))/n);
vy(n,x,y) := simplify( simplify(diff(w(n,x,y),y))/n);
gb(n) := gbasis([vx(n,x,y),vy(n,x,y)], [y,x],plex);
p(n ,x) := sort(simplify(gb(n)[2]));
pf(n,x) :=factor(");
solve({ vx(n,x,y)=0,vy(n,x,y)=0},{x,y});
od;
latex({p(7,x),pf(7,x),...}, 'grobnerf.tex' );
```

There is a one to one correspondence between the irreducible factors of these polynomials and the orbits of B under $\mathrm{Gal}(L/\mathbb{Q})$: Let O be such

TABLE 3. – *For the lowest values of n, characteristic polynomials $P_n(x)$ of N_f with their decomposition into irreducible polynomials over the rationals.*

$$P_4 = x^3 - 1 = (x^2 + x + 1)(x - 1)$$

$$P_5 = x^6 - 4x^3 - 1 = (x^4 + x^3 + 2x^2 - x + 1)(x^2 - x - 1)$$

$$P_6 = x^{10} - 9x^7 + 9x^4 - 8x$$
$$= (x^6 - x^3 + 1)(x^2 + 2x + 4)(x - 2)x$$

$$P_7 = x^{15} - 16x^{12} + 59x^9 - 67x^6 - 37x^3 + 8$$
$$= (x^2 + x + 2)(x^3 - 2x^2 - x + 1)(x^6 + 2x^5 + 5x^4 + 3x^2 + x + 1)$$
$$\times (x^4 - x^3 - x^2 - 2x + 4)$$

$$P_8 = x^{21} - 25x^{18} + 191x^{15} - 559x^{12} + 531x^9 - 507x^6 + 341x^3 + 27$$
$$= (x - 1)(x^2 + x + 1)(x^2 + 2x + 3)(x^2 + 1)(x^2 - 2x - 1)$$
$$\times (x^4 - x^2 + 1)(x^4 + 2x^3 + 5x^2 - 2x + 1)(x^4 - 2x^3 + x^2 - 6x + 9)$$

$$P_9 = x^{28} - 36x^{25} + 459x^{22} - 2655x^{19} + 7290x^{16} - 9801$$
$$x^{13} + 3429x^{10} + 6075x^7 - 1458x^4 + 729x$$
$$= x(x^3 - 3x^2 + 3)(x^6 + 3x^5 + 9x^4 + 6x^3 + 9x^2 + 9)$$
$$\times (x^{18} - 18x^{15} + 108x^{12} - 252x^9 + 324x^6 - 81x^3 + 27)$$

$$P_{10} = x^{36} - 49x^{33} + 929x^{30} - 8865x^{27} + 46315x^{24} - 136058x^{21} + 219202x^{18}$$
$$- 198802x^{15} + 189535x^{12} - 152085x^9 + 62341x^6 + 20851x^3 - 1331$$
$$= (x^2 - x - 1)(x^2 - 3x + 1)$$
$$\times (x^4 - x^3 + x^2 - x + 1)(x^4 + 4x^3 + 11x^2 + 14x + 11)$$
$$\times (x^4 + 3x^3 + 8x^2 + 3x + 1)(x^4 + x^3 + 2x^2 - x + 1)$$
$$\times (x^8 + x^7 - x^5 - x^4 - x^3 + x + 1)$$
$$\times (x^8 - 4x^7 + 5x^6 - 16x^5 + 54x^4 - 66x^3 + 75x^2 - 154x + 121)$$

$$P_{11} = x^{45} - 64x^{42} + 1679x^{39} - 23699x^{36} + 198636x^{33} - 1031272x^{30} + 3360456x^{27}$$
$$- 6855112x^{24} + 8542281x^{21} - 5062167x^{18} - 1959023x^{15} + 4912958x^{12}$$
$$- 1335971x^9 + 1092507x^6 - 375746x^3 - 12167$$
$$= (x^5 - 4x^4 + 2x^3 + 5x^2 - 2x - 1)$$
$$\times (x^{10} + 4x^9 + 14x^8 + 18x^7 + 26x^6 + 7x^5 + 25x^4 + 6x^3 + 9x^2 - 2x + 1)$$
$$\times (x^{10} + 3x^9 + 9x^8 + 5x^7 + 4x^6 - 21x^5 + 3x^4 - 2x^3 + 38x^2 + 4x + 23)$$
$$\times (x^{20} - 3x^{19} - 17x^{17} + 62x^{16} + 58x^{14} - 405x^{13} + 44x^{12} + 26x^{11} + 1088x^{10}$$
$$- 41x^9 - 352x^8 - 1721x^7 + 158x^6 + 583x^5 + 1383x^4$$
$$- 244x^3 - 858x^2 - 92x + 529)$$

TABLE 3 (continued).

$$
\begin{aligned}
P_{12} &= x^{55} - 81x^{52} + 2799x^{49} - 54447x^{46} + 662742x^{43} - 5311422x^{40} + 28737907x^{37} \\
&\quad - 106030035x^{34} + 266507370x^{31} - 451720778x^{28} + 518828787x^{25} \\
&\quad - 462789387x^{22} + 436171797x^{19} - 357754725x^{16} + 197274672x^{13} \\
&\quad - 12009616x^{10} - 55706688x^{7} + 4315968x^{4} - 1124864x \\
&= x(x-1)(x-2)(x^2+2x+4)(x^2+x+1)(x^2-2x-2)(x^2+2x+2) \\
&\quad \times (x^4-2x^3+2x^2-4x+4)(x^4+2x^3+6x^2-4x+4) \\
&\quad \times (x^6-x^3+1)(x^6+x^3+1) \\
&\quad \times (x^{12}-34x^9+381x^6-1564x^3+2197)(x^{12}-14x^9+53x^6-4x^3+1)
\end{aligned}
$$

an orbit and $j_o \in O$. By definition $j \in O$ if and only if there exists a $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $j = j_o^\sigma$ in the sense of (16).

Consider the polynomials

$$P_{a,O,n}(x) = \prod_{j \in O} (x - \lambda_a^{(j)}) \tag{83}$$

For any σ , $j \to j^\sigma$ induces a permutation of O , so that

$$\prod_{j \in O} \left(x - \sigma(\lambda_a^{(j)})\right) = \prod_{j \in O} \left(x - \lambda_a^{(j^\sigma)}\right) = P_{a,O,n}(x)$$

which implies that $P_{a,O,n}(x)$ has rational coefficients.

Using the non degeneracy of its roots $\lambda_f^{(j)}$, let us showthat $P_{f,O,n}$ is irreducible: a factorization $P_{f,O,n} = P^{(1)} P^{(2)}$ in $\mathbb{Q}[x]$ would correspond to a splitting of its complex roots into two disjoint subsets, $O = O_1 \bigcup O_2$ separately stable under Galois morphisms. For any σ and $j \in O_1$, j^σ , determined by $\sigma(\lambda_f^{(j)}) = \lambda_f^{(j^\sigma)}$ would belong to O_1 *i.e.* O_1 would be an orbit in itself, which is absurd.

Furthermore one can consider the subfield corresponding to any orbit O

$$L_O = \mathbb{Q}\left((\lambda_f^{(j)})_{j \in O}\right) \simeq \frac{\mathbb{Q}[x]}{P_{f,O,n}(x)} \tag{84}$$

Since any $\lambda_a^{(j)}$ is a polynomial in $\lambda_f^{(j)}$, they generate L. By the chinese remainder theorem, the direct product of these fields is isomorphic to the

fusion algebra (alternatively Fus is isomorphic to a block diagonal matrix algebra, each block being isomorphic to the corresponding field L_O) :

$$Fus \simeq \frac{\mathbb{Q}[x]}{P_{f,n}(x)} \simeq \times_O L_O \tag{85}$$

The stabilizer of the orbit O clearly equals the relative Galois group:

$$H_O = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q})/j = j^\sigma for\ j \in O\} = \mathrm{Gal}(L/L_O) \tag{86}$$

(note that since $\mathrm{Gal}(L/\mathbb{Q})$ is abelian, if $j = j^\sigma$ holds for one $j \in O$, it holds for all of them).

The order $[L : \mathbb{Q}]$ is a multiple of the greatest common multipleof the degrees $[L_O : \mathbb{Q}] = \deg(P_{f,O,n})$.

To our knowledge the idea to consider the factorization of these polynomials first appeared in [29].

3. $\mathbb{Z}/N\mathbb{Z}$ THEORIES

We shall now compute the Galois action on S, $(\exp(2\pi i h_j))_j$and $\exp(2\pi i c/8)$ of RCFTs with fusion rules of $\mathbb{Z}/N\mathbb{Z}$ type. These data have been determined in [19] and we recall here the results ([7]). Primary fields are labelled by an element of $\mathbb{Z}/N\mathbb{Z}$ and the S matrix is determined by the residue mod N of an integer a coprime with N and we have:

$$S_{n\ m} = \frac{1}{\sqrt{N}} \exp\left(-2\pi i a \frac{nm}{N}\right) \tag{87}$$

This matrix is denoted by $S(a)$. In the case of $(\exp(2\pi i h_j))_j$ and $\exp(2\pi i c/8)$, two cases must be distinguished according to N's parity:

• When N is even, a is odd. In this case, we should fix a modulo $2N$ and we have:

$$\begin{cases} \exp(2\pi i h_k) = \exp(2\pi i a k^2/2N) \\ \exp(2\pi i c(a)/8) = \dfrac{1}{\sqrt{2}} S_{2N}(a) \end{cases} \tag{88}$$

([7]) In fact, in [19], the equations solved were $S^2 = C$ and $(ST)^3 = \mathbf{1}$. It is easy to infer from that the solution to $S^2 = (ST)^3 = C$.

TABLE 4. – *Fields L, M, Galois group of M, some cyclotomic field K containing M for* $su(3)_k$. μ_m *denotes the multiplicative cyclic group of order* m.

k	$n = k+3$	$L = \mathbb{Q}(\{S_{ij}/S_{\rho j}\})$	$M = \mathbb{Q}(\{S_{ij}\})$	$\mathrm{Gal}(M/\mathbb{Q})$	K
1	4	$\mathbb{Q}\left(i\sqrt{3}\right)$	$\mathbb{Q}(\sqrt{3},\ i)$	$\mu_2 \times \mu_2$	$= M$
2	5	$\mathbb{Q}(\sqrt{5},\ i\sqrt{3})$	$\mathbb{Q}\left(\exp\left(\frac{2i\pi}{15}\right)\right)$	$\mu_2 \times \mu_4$	$= M$
3	6	$\mathbb{Q}\left(\exp\left(\frac{i\pi}{9}\right)\right)$	$= L$	μ_6	$= L$
4	7	$\mathbb{Q}\left(\exp\left(\frac{2i\pi}{21}\right)\right)$	$= L$	$\mu_2 \times \mu_6$	$= L$
5	8	$\mathbb{Q}\left(\exp\left(\frac{i\pi}{12}\right)\right)$	$= L$	$\mu_2 \times \mu_2 \times \mu_2$	$= L$
6	9	$\mathbb{Q}\left(\exp\left(\frac{2i\pi}{27}\right)\right)$	$= L$	μ_{18}	$= L$
7	10	$\mathbb{Q}\left(\exp\left(\frac{i\pi}{15}\right)\right)$	$= L$	$\mu_2 \times \mu_4$	$= L$
8	11	$\mathbb{Q}\left(\exp\left(\frac{2i\pi}{33}\right)\right)$	$= L$	$\mu_2 \times \mu_{10}$	$= L$
9	12	$\mathbb{Q}\left(\exp\left(\frac{i\pi}{18}\right)\right)$	$= L$	$\mu_2 \times \mu_6$	$= L$
$n-3$	n	$\mathbb{Q}\left(\left(\frac{i\pi}{18}\right)\right)$	$= L$	$(\mathbb{Z}/3n\mathbb{Z})^*$	$= L$

The Gauss sum $S_N(a)$ is defined by equation (122) in Appendix A.

• When N is odd, a must be taken even and we write $a = 2b$ where $b \wedge N = 1$, b being taken modulo N and we have:

$$\begin{cases} \exp(2\pi i h_k) = \exp(2\pi i b k^2/N) \\ \exp(2\pi i c(b)/8) = S_N(b) \end{cases} \tag{89}$$

As advocated in [17], and as we will recall in section, these numbers completely determine partition functions of boundaryless three-manifolds without any decoration in the topological theory deduced from a solution to Moore and Seiberg's equations.

3.1. Determination of the number fields

In this section, we shall determine the number field generated by all matrix elements of S, the $(\exp(2\pi i h_j))_j$ and $\exp(2\pi i c/8)$. Let us denote by K the field generated by S's matrix elements, the $(\exp(2\pi i h_j))_j$ and $\exp(2\pi i c/8)$. We have the following table:

(90)

N	K
$N \equiv 0 \pmod 4$	$\mathbb{Q}_{2N}$
$N \equiv 1 \pmod 4$	$\mathbb{Q}_N$
$N \equiv 2 \pmod 4$	$\mathbb{Q}_{4N}$
$N \equiv 3 \pmod 4$	$\mathbb{Q}_{4N}$

3.2. Explicit Galois action

The aim of this section is to prove the following result:

(91)
$$\begin{cases} \text{When } N \equiv 0,1 \pmod 4, \text{ there exist exactly two orbits} \\ \text{of } \mathbb{Z}/N\mathbb{Z} \text{ data.} \\ \text{When } N \equiv 2,3 \pmod 4 \text{ there is only one such orbit.} \end{cases}$$

In order to prove it, we shall examine both cases by giving explicit formulae for the Galois action on all these numbers. As we have seen before, the S matrix, $(\exp(2\pi i h_j))_j$ and $\exp(2\pi i c/8)$ are determined by the a or b parameter appearing in formulae (88) and (89). In all cases, the Galois action on $S_{n\ m}/S_{0\ 0}$ is determined through the cyclotomic character $\chi_N : \mathrm{Gal}(\mathbb{Q}_N/\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^*$. There exists a sign $\varepsilon_{N,a}(\sigma) = \pm 1$ such that, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ one has

$$\sigma(S(a)) = \varepsilon_N(\sigma) S(a\chi_N(\sigma)) \tag{92}$$

In all cases the $(\exp(2\pi i h_n))_n$ are N-th or $2N$-th roots of unity. The Galois action on them is therefore defined by χ_{2N}. For $\exp(2\pi i c/8)$ we will use explicit expressions of Gauss' sums. Let us go into the details of each case:

Case $N \equiv 0 \pmod 4$. – The Galois action on the $(\exp(2i\pi h_j))_j$ is completely determined by the cyclotomic character χ_{2N}. The central charge $c(a) \pmod 8$ depends on $a \bmod 2N$ and therefore using the fact that

$(ST)^3 = C$ has integer coefficients, we show that $\exp(2\pi ic/8)$ transforms as

$$\exp(2\pi ic(a)/8) \longrightarrow \varepsilon_N(\sigma)\exp(2\pi ic(\chi_{2N}(\sigma)a)/8) \tag{93}$$

Of course, $\varepsilon_N(\sigma)$ is such that:

$$\sqrt{N} \longrightarrow \varepsilon_N(\sigma)\sqrt{N} \tag{94}$$

Let us introduce the following notation: $N = 2^{\nu_2(N)}N'$ where N' is odd as well as $\mathcal{E}(x)$ defined in (128) in Appendix A. Then, one has:

$$\exp\left(2\pi i\frac{c(a)}{8}\right) = \frac{\mathcal{E}(N'a)}{\mathcal{E}(N')}\left(\frac{-1}{a}\right)\left(\frac{2^{1+\nu_2(N)}}{a}\right)\left(\frac{a}{N'}\right)\xi_8 \tag{95}$$

The explicit expression for $\varepsilon_N(\sigma)$ can be found using formulae (93), (131) and

$$\frac{\mathcal{E}(N'\chi_4(\sigma))}{\mathcal{E}(N')}\xi_8^{\chi_8(\sigma)-1} = (-1)^{(\chi_8^2-1)/8}(-1)^{\frac{N'-1}{2}\times\frac{(\chi_4-1)}{2}}$$

(96)

$$\varepsilon_N(\sigma) = \left(\frac{\chi_N(\sigma)}{N'}\right)\exp\left(i\pi\left(\frac{N'-1}{2}\,\frac{\chi_4(\sigma)-1}{2} + \nu_2(N)\frac{\chi_8(\sigma)^2-1}{8}\right)\right)$$

Here, $2N \equiv 0 \pmod 8$ and therefore, $\chi_{2N}(\sigma)$ specifies $\chi_8(\sigma)$ by reduction modulo 8. Henceforth, the sign $\varepsilon_N(\sigma)$ is completely determined. Therefore, there are two orbits through the Galois action on Moore-Seiberg data. Representatives of each orbit are found by fixing a and simultaneously changing $S_{0\,0}$ and $\exp(2\pi ic/8)$ into their opposite.

Case $N \equiv 1 \pmod 4$. – This is the simplest case since

$$\exp(2\pi ic(b)/8) = \left(\frac{b}{N}\right) \qquad \exp(2\pi ih_n) = \exp\left(2\pi i\frac{b}{N}n^2\right) \tag{97}$$

In this case, we immediately get:

$$\begin{aligned} \exp(2\pi ibn^2/N) &\longrightarrow \exp(2\pi ib\,\chi_N(\sigma)n^2/N) \\ \exp(2\pi ic(b)/8) &\longrightarrow \exp(2\pi ic(b)/8) \in \mathbb{Q} \\ \sqrt{N} &\longrightarrow \varepsilon_N(\sigma)\times\sqrt{N} \end{aligned} \tag{98}$$

where

$$\varepsilon_N(\sigma) = \left(\frac{\chi_N(\sigma)}{N}\right) \tag{99}$$

According to this equation, there are exactly two orbits for the Galois action. Representatives of each orbit are easily found by fixing b and simultaneously changing $S_{0\,0}$ and $\exp(2\pi ic/8)$ into their opposite.

Case $N \equiv 3 \pmod 4$. – This case is as simple as the $N \equiv 1 \pmod 4$ case since

$$\exp(2\pi ic/8) = i\left(\frac{b}{N}\right) \qquad \exp(2\pi ih_n) = \exp\left(2\pi i\frac{b}{N}n^2\right) \tag{100}$$

and therefore:

$$\begin{aligned} \exp(2\pi ibn^2/N) &\longrightarrow \exp(2\pi ib\chi_N(\sigma)n^2/N) \\ \exp(2\pi ic(b)/8) &\longrightarrow \varepsilon_N(\sigma)\exp(2\pi ic(\chi_N(\sigma)b)/8) \\ \sqrt{N} &\longrightarrow \varepsilon_N(\sigma)\sqrt{N} \end{aligned} \tag{101}$$

with

$$\varepsilon_N(\sigma) = (-1)^{(\chi_4(\sigma)-1)/2}\left(\frac{\chi_N(\sigma)}{N}\right) \tag{102}$$

Let us show that there is only one Galois orbit: let (b, b') be two invertible elements of the ring $\mathbb{Z}/N\mathbb{Z}$ and $(\alpha, \alpha') \in \{\pm 1\}^2$, there exists a unique $\chi_N \in (\mathbb{Z}/N\mathbb{Z})^*$ and a unique $\chi_4 \in (\mathbb{Z}/4\mathbb{Z})^*$ such that

$$b' \equiv b\,\chi_N \pmod N \qquad \alpha' = \alpha\,(-1)^{(\chi_4-1)/2} \tag{103}$$

Bezout's theorem shows that (χ_N, χ_4) arises from a unique $\chi_{4N} \in (\mathbb{Z}/4N\mathbb{Z})^*$ by reduction modulo N and 4 respectively. Moreover, there exists a unique $\sigma \in \mathrm{Gal}(\mathbb{Q}_{4N}/\mathbb{Q})$ satisfying $\chi_{4N}(\sigma) = \chi_{4N}$ and this proves that we have only one orbit under the Galois action.

Case $N \equiv 2 \pmod 4$. – In this case, since $\sqrt{N} \in \mathbb{Q}_{4N}$, the Galois action is defined through the cyclotomic character χ_{4N}, or equivalently χ_{2N} and χ_8. The transformation laws are:

$$\begin{aligned} \exp(2\pi ian^2/2N) &\longrightarrow \exp(2\pi ia\chi_{2N}(\sigma)n^2/2N) \\ \exp(2\pi ic(a)/8) &\longrightarrow \varepsilon_N(\sigma)\exp(2\pi ic(\chi_{2N}(\sigma)a)/8) \\ \sqrt{N} &\longrightarrow \varepsilon_N(\sigma)\sqrt{N} \end{aligned} \tag{104}$$

where $\varepsilon_N(\sigma)$ is given by formula (99) with $\nu_2(N) = 1$. The method used in the previous case – $N \equiv 3 \pmod 4$ – shows that there is exactly one orbit under the Galois action: since $N \equiv 2 \pmod 4$, 8 does not divide

$2N$. Henceforth, fixing $\chi_{2N}(\sigma)$ does not fix $\chi_8(\sigma)$. This concludes our proof of (91).

4. ON $\mathbb{Z}/N\mathbb{Z}$ TOPOLOGICAL INVARIANTS

In this section, we shall see how the Galois action on S and T matrices deduced from $\mathbb{Z}/N\mathbb{Z}$ fusion rules enables us to relate various topological invariants of a boundaryless three-manifold M without any decoration. We shall compare them to the ones described by Kohno in [34]. We shall see that these invariants only depend on the a (or b parameter) introduced in section 3 and of a sign. Such an invariant will be denoted by $Z_{\pm,a}$ (or $Z_{\pm,b}$). As explained by theorem 91, at fixed a (or b) parameter, the sign distinguishes between the two orbits under the Galois action.

We shall show the following relation between $Z_{+,a}$ and $Z_{-,a}$:

$$\frac{Z_{+,a}[M]}{Z_{-,a}[M]} = (-1)^{1+\dim(H^1(M,\mathbb{Z}))} \tag{105}$$

which shows that the quotient $Z_{+,a}/Z_{-,a}$ is a Galois invariant and is also related to the "classical" topological invariant $\dim(H^1(M,\mathbb{Z}))$.

Notations. – Here, we follow the notations of [15]. Let M be an oriented boundaryless compact oriented three-manifold without any decoration. In this paragraph, we shall use surgery presentations for computing $Z[M]$, a complex valued topological invariant of M. Let L be a framed oriented link in S_3, $\sharp(L)$ denotes the number of components of L. The Gauss linking number of two components L_i and L_j of L is denoted by $\langle L_i, L_j\rangle$:

$$\langle L_i, L_j\rangle = \frac{1}{4\pi}\int_{L_i}\int_{L_j}\frac{dx\wedge dy\wedge(x-y)}{\|x-y\|^3} \tag{106}$$

The framing of the i-th component is noted n_i. Let A_L be the intersection matrix of L, *i.e.*:

$$\begin{gathered}\forall(i,j)\in\{1,\cdots,\sharp(L)\}^2,\\ (i\neq j\Rightarrow(A_L)_{i,j}=\langle L_i,L_j\rangle)\qquad\text{and}\qquad(A_L)_{i,i}=n_i\end{gathered} \tag{107}$$

It is a symmetric matrix and σ_L is the signature (number of positive minus number of negative eigenvalues) of the associated quadratic form. It can be degenerated and we call $\ker(A_L)$ its kernel.

A coloring of L is completely specified by $J=(j_1,\ldots j_{\sharp(L)})\in(\mathbb{Z}/N\mathbb{Z})^{\sharp(L)}$and L_J denotes the link L colored by J.

Explicit expressions for $Z[M]$. – Here, we shall give explicit expressions for $Z[M]$ using the S matrix, the $(\exp(2\pi i h_j))_j$ and $\exp(2\pi i c/8)$ computed in [19]. In particular, we have $S_{00} > 0$. As we have recalled in section, these matrices depend on one parameter denoted by a.

Let L be a framed link in S_3 such that $[S_3, L]$ is a surgery presentation for M, the partition function of M can be computed using the algorithm given in [15]. First of all, using

$$Z[M] = \exp\left(-2\pi i \frac{c\sigma_L}{8}\right) \sum_{J \in (\mathbb{Z}/N\mathbb{Z})^{\sharp(L)}} \left(\prod_{l=1}^{\sharp(L)} S_{0j_l}\right) Z[S_3, L_J] \tag{108}$$

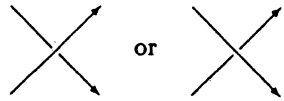
one brings the computation of $Z[M]$ to the computation of $Z[S_3, L_J]$, which is the topological invariant ([8]) associated with the sphere S_3 decorated by a framed link L.

Then, let L be colored by $J \in (\mathbb{Z}/N\mathbb{Z})^{\sharp(L)}$, we have

$$Z_{a,+}[S_3, L_J] = S_{00} \times \exp\left(2\pi i \frac{a}{2N} {}^t J . A_L . J\right) \tag{109}$$

This result is obvious for $\sharp(L) = 0$ and for the unknotted circle with framing n. It can be proved by induction on $\sharp(L)$. Let us assume that it has been proved for any L such that $\sharp(L) \leq n$ where $n \in \mathbb{N}$. Now, let L be a link with $n+1$ components. In order to compute $Z[S_3, L]$ we shall choose a regular projection plane. We assume the framing of the link to be normal to this projection plane ([9]). The basic idea is to use a kind of "skein relation" and a formula due to Kauffman for computing in a combinatorial way the linking number of two oriented knots.

Let us consider two oriented knots L and L' in S_3 and a regular projection with respect to the link (L, L'). Let us denote by $\alpha(L)$ and $\alpha(L')$ the projections of L and L' on the projection plane. In the neighbourhood of each intersection point $p \in \alpha(L) \cap \alpha(L')$, the situation looks like ([10]):

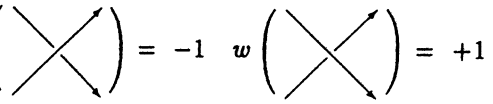


([8]) In the framework of Chern-Simons theory, this is nothing but the expectation value of regularized Wilson loops.

([9]) This can always be achieved.

([10]) Up to a rotation.

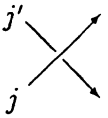
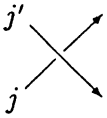
where the arrows indicate the orientations of each curve. We now associate with each intersection a weight:

(110) $w\left(\right) = -1 \quad w\left(\right) = +1$ 

Passing from a type + intersection to a type − one will be called a *shift*. Then, the intersection number $\langle L, L' \rangle$ is given by [30], p. 14:

$$\langle L,\ L\rangle = \frac{1}{2} \sum_{p \in \alpha(L) \cap \alpha(L')} w(p) \tag{111}$$

Following Witten, we have obtained in [15] :

(112) $Z[S_3,$  $] = Z[S_3,$  $] \times \left(\frac{S_{jj'}}{S_{00}}\right)$

This is a kind of skein relation without any right hand side! Let us now consider L_{n+1} the $n+1$-th component of L. By a finite sequence of elementary shifts and isotopy deformations, we can pass from L to L', the $n+1$-th component of which can be isolated from all others components by cutting along a two-sphere S_2. In particular, this component is not linked to the other ones. We call $\Delta_+(k)$ and $\Delta_-(k)$ the variations in the number of type + (respectively type −) crossings between components $n+1$ and k in this operation. Formula (112) shows that

$$Z[S_3, L] = Z[S_3, L'] \times \prod_{k=1}^{n} \left(\frac{S_{j_{n+1} j_k}}{S_{00}}\right)^{(\Delta_+(k) - \Delta_-(k))/2} \tag{113}$$

Cutting along S_2 gives

$$Z[S_3, L'] = \frac{Z[S_3, L' \setminus L'_{n+1}] \times Z[S_3, L'_{n+1}]}{S_{00}} \tag{114}$$

Using (111), we have

$$\left(\frac{S_{j_{n+1}\, j_k}}{S_{00}}\right)^{(\Delta_+(k) - \Delta_-(k))/2} = \exp\left(2\pi i \frac{2a j_k j_{n+1}}{N} \langle L_{n+1}, L_k \rangle\right)$$

and in the end, applying the recurrence hypothesis to $L' \setminus L'_{n+1}$, we obtain formula (109).

The partition function for a boundaryless oriented three-manifold without any decoration is therefore:

$$Z_{a,+}[M] = \exp\left(-2\pi i \frac{c(a)}{8}\sigma_L\right)(S_{00})^{\sharp(L)+1} \times \sum_{J\in(\mathbb{Z}/N\mathbb{Z})^{\sharp(L)}} \exp\left(2\pi i \frac{a}{2N}{}^t J.A_L.J\right) \tag{115}$$

It is an interesting exercise to prove invariance under Kirby's moves directly. Let us recall Kirby's theorem ([31], [32]):

THEOREM 1. – *Let L and L' be two oriented framed links in S_3, the three-manifolds M_L and $M_{L'}$ obtained by surgery along L and L' are isomorphic if and only if, one can pass from L to L' by a finite number of the following moves:*

- *Isotopy in S_3.*
- *Retiring an unknotted and unlinked component of framing ± 1 to L. This is called an $\mathcal{O}_1$ move.*
- *For some $i \neq j$, replace L_i by L'_i which is a band-connected sum of L_i and a parallel curve to L_j. The framing of L'_i is $\langle L_1 + L_j, L_i + L_j\rangle$. This is called an $\mathcal{O}_2$ move.*

Let us now check the invariance of expression (115) under these moves. As we shall see, invariance under $\mathcal{O}_2$ moves is obvious whereas in the general framework of [15] it was not ([11]).

- Since the intersection matrix A_L is an isotopy invariant, the r.h.s. of equation (115) is an isotopy invariant of L.
- Let us check the invariance under the $\mathcal{O}_1$ moves. Let L be an n-component oriented framed link and C_ε be an unknotted oriented framed knot of framing $\varepsilon = \pm 1$ which can be isolated from L by a two sphere in S_3. We have

$$A_{L,C} = \begin{pmatrix} & & & 0 \\ & A_L & & \vdots \\ & & & 0 \\ 0 & \cdots & 0 & \varepsilon \end{pmatrix}$$

([11]) One had to use the Fenn and Rourke moves.

and therefore $\sigma_{L,C} = \sigma_L + \varepsilon$, and $\sharp(L,C) = \sharp(L) + 1$. Henceforth,

$$\sum_{J \in (\mathbb{Z}/N\mathbb{Z})^{\sharp(L,C)}} \exp\left(2\pi i \frac{a}{2N} {}^t J . A_{L,C} . J\right)$$

factorizes as

$$\left(\sum_{J \in (\mathbb{Z}/N\mathbb{Z})^{\sharp(L)}} \exp\left(2\pi i \frac{a}{2N} {}^t J . A_L . J\right)\right) \times \left(\sum_{x \in \mathbb{Z}/N\mathbb{Z}} \exp\left(2\pi i \frac{a}{2N} x^2 \varepsilon\right)\right)$$

The main point is that the change of σ_L compensates the second term in this product. Henceforth, the r.h.s of equation (115) is $\mathcal{O}_1$-invariant.

• Invariance under the $\mathcal{O}_2$ moves is obvious. Let us asume that in such a move, component L_i is transformed into $L_1 \sharp L_j$ and has framing $\langle L_i + L_j, L_i + L_j \rangle$. Let Q_L be a quadratic formin $\mathbb{R}^{\sharp L}$ represented by A_L in the canonical basis $(e_k)_{1 \leq k \leq \sharp(L)}$ of $\mathbb{R}^{\sharp L}$. Let also be $Q_{L'}$ be represented by $A_{L'}$ and $u \in GL_{\sharp(L)}(\mathbb{R})$ be defined by

$$\begin{cases} \forall k \neq i, \quad u(e_k) = e_k \\ u(e_i) = e_i + e_j \end{cases} \tag{116}$$

then one trivially has:

$$Q_{L'} = Q_L \circ u \tag{117}$$

The key point is that u is invertible as a ring homomorphism of $\mathbb{Z}$-modules. Henceforth

$$\sum_{J \in (\mathbb{Z}/N\mathbb{Z})^{\sharp(L)}} \exp\left(2\pi i \frac{a}{2N} Q_L(J)\right) = \sum_{J \in (\mathbb{Z}/N\mathbb{Z})^{\sharp(L)}} \exp\left(2\pi i \frac{a}{2N} Q_{L'}(J)\right)$$

Since $\sigma_{L'} = \sigma_L$ and $\sharp(L') = \sharp(L)$, the $\mathcal{O}_2$ invariance of the r.h.s of equation (115) follows.

Let us identify these invariants with Kohno's ones:

N **odd**. In this case, $a = 2b$ where $b \in (\mathbb{Z}/N\mathbb{Z})^*$. Using equation (89), one immediately recovers Kohno's invariant (*see* Theorem 3.6 of [34]).

N **even**. In this case, a is odd and considered modulo $2N$. We remark that shifting a into $a + N$ changes the exponential in (115):

$$\begin{aligned} &\exp\left(2\pi i \frac{a+N}{2N} {}^t J . A_L . J\right) \\ &\quad = \exp\left(2\pi i \frac{a}{2N} {}^t J . A_L . J\right) \times (-1)^{\sum_j n_j J_j^2} \end{aligned} \tag{118}$$

This shift $a \mapsto a + N$ explains why Kohno has written down two invariants when N is even (*see* p. 348 of [34]). Equation (115) captures them both.

Of course, instead of using the data of reference [19], we could have relaxed the $S_{00} > 0$ condition, and get "new" invariants. Turning $S(a)$ into $-S(a)$ and $\exp(2\pi i c(a)/8)$ into $-\exp(2\pi i c(a)/8)$ produces an invariant denoted by $Z_{a,-}$. Then, equation (105) simply follows from equation (115) since

$$Z_{-,a}[M] = Z_{+,a}[M] \times (-1)^{\sharp(L)-\sigma(L)+1}$$

and (*see* [36], Remark 1.8):

$$\begin{aligned} \sharp(L) - \sigma(L) &\equiv \dim(\ker(A_L)) \pmod 2 \\ \dim(\ker(A_L)) &= \dim(H^1(M, \mathbb{Z})) \end{aligned}$$

equation (105) is proved.

4.1. Explicit evaluation for prime numbers

The case $N = 2$ has in fact been considered in details by Kirby and Melvin [33]. The invariant computed by these authors is

$$\tau_3[M] = 2^{-n/2} \left(\frac{1-i}{\sqrt{2}}\right)^{\sigma_L} \sum_{S \subset L} i^{S.S} \tag{119}$$

where the sum is over all sublinks S of L and $S.S$ denotes $\sum_{(i,j)\in\pi_0(S)^2} \langle S_i, S_j \rangle$. It is clear that

$$Z_{-1,+}[M] = \frac{\tau_3[M]}{\sqrt{2}} \tag{120}$$

This identity is not a surprise since the $SU(2)_{k=1}$ WZW model, which should give $\tau_3(M)$, has $\mathbb{Z}/2\mathbb{Z}$ fusion rules!

Let us now assume that N is an odd prime number p. In this case, for a framed oriented link L in S_3, let $A_L^{(p)}$ denote the reduction modulo p of L's intersection form. Here, L will be a surgery presentation for M. Using the classification theorem for quadratic forms over finite fields [37], we can compute explicitely $Z_{a,+}[M]$ in terms of data relative to $A_L^{(p)}$. A non degenerate quadratic form Q on $\mathbb{F}_p$ is equivalent to

$$Q(x_1, \ldots, x_n) = x_1^2 + \ldots + x_{n-1}^2 + \alpha\, x_n^2$$

where α is not zero and taken modulo squares in $\mathbb{F}_p$. Henceforth, up to an equivalence, the quadratic form represented by $A_L^{(p)}$ is classified by $\dim(\ker A_L^{(p)})$ and an element $\alpha \in \mathbb{F}_p^*/(\mathbb{F}_p^2)$. In this case, let us denote by $r_p(L)$ and σ_L the rank modulo p of A_L and the signature of A_L. We can easily show that

$$Z_{a,+}[M] = \left(\frac{\alpha}{p}\right) p^{(\sharp(L)-r_p(L)-1)/2} \left(S_p(1)\left(\frac{b}{p}\right)\right)^{r_p(L)-\sigma_L} \tag{121}$$

A. About Gauss sums

In this paper, we need to evaluate the following Gauss sum

$$S_N(a) = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \exp\left(2\pi i \frac{ak^2}{N}\right) \tag{122}$$

where $a \wedge N = 1$. We shall only recall the basic results but not their proofs. The interested reader may consult [35]. First of all, we need to recall some basic facts about Legendre and Jacobi symbols:

DEFINITION 1. – *Let p be an odd prime number, $x \in \mathbb{Z}/p\mathbb{Z}$, we define the Legendre symbol as:*

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a square modulo } p \\ -1 & \text{if not} \end{cases} \tag{123}$$

The Jacobi symbol is defined by:

DEFINITION 2. – *Let $N = \prod_p p^{\nu_p(N)}$ be an odd number, $x \in \mathbb{Z}/N\mathbb{Z}$, we define the Jacobi symbol as:*

$$\left(\frac{x}{N}\right) = \prod_p \left(\frac{x}{p}\right)^{\nu_p(N)} \tag{124}$$

It is straightforward to show the following properties of these symbols:

$$\left(\frac{x}{NM}\right) = \left(\frac{x}{N}\right)\left(\frac{x}{M}\right) \quad \text{and} \quad \left(\frac{xy}{N}\right) = \left(\frac{x}{M}\right)\left(\frac{y}{M}\right) \tag{125}$$

The strategy for computing $S_N(a)$ consists in evaluating $S_N(a)/S_N(1)$, and then computing $S_N(1)$. If N is an odd number coprime with a, we have

$$S_N(a) = \left(\frac{a}{N}\right) S_N(1). \tag{126}$$

When N is even, the result is slightly more complicated: first of all, let us write $N = 2^{\nu_2(N)}N'$ where N' is *odd*. Then, we have:

$$S_N(a) = \left(\frac{a}{N'}\right)\left(\frac{-1}{a}\right)\left(\frac{2^{\nu_2(N)}}{a}\right)\frac{\mathcal{E}(aN')}{\mathcal{E}(N')}\,S_N(1) \tag{127}$$

where

$$\begin{cases} \mathcal{E}(x) = 1 & \text{when } x \equiv 1 \pmod 4 \\ \mathcal{E}(x) = i & \text{when } x \equiv -1 \pmod 4 \end{cases} \tag{128}$$

This quantity satisfies:

$$\mathcal{E}(xy) = (-1)^{(x-1)(y-1)/4}\,\mathcal{E}(x)\mathcal{E}(y) \tag{129}$$

and:

$$\sigma(\mathcal{E}(x)) = (-1)^{(x-1)(\chi_4(\sigma)-1)/4}\,\mathcal{E}(x). \tag{130}$$

We also recall that for N an odd integer, we have:

$$\left(\frac{-1}{N}\right) = (-1)^{(N-1)/2} \qquad \text{and} \qquad \left(\frac{2}{N}\right) = (-1)^{(N^2-1)/2} \tag{131}$$

The evaluation of $S_N(1)$ has been performed by Gauss:

$$S_N(1) = \sum_{k\in\mathbb{Z}/N\mathbb{Z}} \frac{\xi_N^{k^2}}{\sqrt{N}} = \frac{1+i}{2}(1+(-i)^N) \tag{132}$$

B. Useful results on cyclotomic fields

In this appendix, we discuss to which number field $\sqrt{n}$ belongs for $n \in \mathbb{N}$. We shall set $\xi_n = \exp(2i\pi/n)$, and denote by $\mathbb{Q}_n$ the extension $\mathbb{Q}(\xi_n)$. It is a finite normal extension of $\mathbb{Q}$. First of all, let us recall a basic lemma:

LEMMA. – *Let k and l be two non zero integers, then*

$$\mathbb{Q}(\xi_k, \xi_l) = \mathbb{Q}_{k\smile l} \tag{133}$$

where $k \smile l$ denotes the smallest common multiple of k and l.

This Lemma trivially follows from Bezout's theorem. It shows that if n is an odd integer, $\mathbb{Q}_{2n} = \mathbb{Q}_n$ since $\mathbb{Q}_2 = \mathbb{Q}$.

(134)

n	field
$n \equiv 0 \pmod 4$	$\mathbb{Q}_n$
$n \equiv 1 \pmod 4$	$\mathbb{Q}_n$
$n \equiv 2 \pmod 4$	$\mathbb{Q}_{4n}$
$n \equiv 3 \pmod 4$	$\mathbb{Q}_{4n}$

Let us recall that theaction of any element $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is determined by the cyclotomic character $\chi_n : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$. These characters satisfy the obvious compatibility relations that enable defining the profinite character $\chi : \sigma \mapsto (\chi_n)_{n\in\mathbb{N}^*} \in \widehat{\mathbb{Z}}^*$.

In order to determine to which number field $\sqrt{n}$ belongs, we shall use the expression (132) for the Gauss sum which already shows that $\sqrt{n}$ belongs to some cyclotomic extension of $\mathbb{Q}$. The discussion is performed according to the different values of $n(\mathrm{mod}\ 4)$. The results are the following:

In some cases, we can find the minimal $\alpha \in \mathbb{N}$ such that $\sqrt{n} \in \mathbb{Q}_{2^\alpha m}$ where m is odd. More precisely, let us show that the power of 2 given in the above table is minimal for $n \equiv 2,\ 3 \pmod 4$.

• *Case* $n \equiv 2 \pmod 4$: $\sqrt{n} \in \mathbb{Q}_{4n}$. – Let us assume that $\sqrt{n}$ belongs to $\mathbb{Q}_{2n}$, we write $n = 2n'$ where n' is odd–henceforth $n' \wedge 8 = 1$–and since $i \in \mathbb{Q}_{2n}$ and $S_{2n}(1) = 1 + i$, we would get $\sqrt{2n} \in \mathbb{Q}_{2n}$ and therefore $\sqrt{2} \in \mathbb{Q}_{2n}$. Thus

$$\xi_8 = \sqrt{2}\frac{(i+1)}{2} \in \mathbb{Q}_{2n}.$$

Using Lemma B and $8 \wedge n' = 1$ we would get $\xi_{4n} \in \mathbb{Q}_{2n}$. This contradiction shows that $\sqrt{n}$ cannot belong to $\mathbb{Q}_{2n}$.

• *Case* $n \equiv 3 \pmod 4$. – Let us assume that $\sqrt{n} \in \mathbb{Q}_{2n}$, then since $S_n(1) = i$, this would imply that $i \in \mathbb{Q}_{2n}$, which is impossible since 4 does not divide $2n$. Therefore, $\sqrt{n} \in \mathbb{Q}_{4n}$ only.

When $n \equiv 0,\ 1 \pmod 4$, the power of two is clearly not minimal since n can be the square of an integer! For the same reason, the power of anyother prime divisor is not minimal.

ACKNOWLEDGEMENTS

We thank M. Bauer, D. Carpentier, P. Di Francesco, M. Duneau, T. Gannon, C. Itzykson, P. Roche, Ph. Ruelle, L. Schneps, E. Thiran,

M. Walton, J. B. Zuber for valuable communications as well as the computer and GAGE team of formal calculus in École Polytechnique, whose CPT provided A.C. and E.B. with excellent working conditions.

REFERENCES

[1] J. CARDY, Operator content of 2d conformal field theories, *Nucl. Phys.*, Vol. **B. 270**, 1986, pp. 186-204.

[2] A. CAPPELLI, C. ITZYKSON and J. B. ZUBER, The ADE classification of $A_1^{(1)}$ and minimal conformal field theories, *Comm. Math. Phys.*, Vol. **113**, 1987, pp. 1-26. J. M. DROUFFE and C. ITZYKSON, Théorie Statistique des Champs, CNRS, Paris, 1989. M. BAUER, Thèse, unpublished.

[3] A. COSTE and T. GANNON, Remarks on Galois symmetry in RCFT, *Phys. Lett.*, Vol. **B 323**, 1994, pp. 316-321.

[4] J. DE BOER and J. GOEREE, Markov traces and type II_1 factors in conformal field theory, *Comm. Math. Phys.*, Vol. **139**, 1991, p. 267.

[5] P. DEGIOVANNI, Moore and Seiberg equations, topological field theories and Galois theory, in *The Grothendieck theory of dessins d'enfants*, L. SCHNEPS Ed., London Mathematical Society, Lecture Note Series, Vol. **200**, 1993, pp. 359-368.

[6] G. MOORE and N. SEIBERG, Polynomial equations for rational conformal field theories, *Phys. Lett. B.*, Vol. **212**, 1988, pp. 451-460.

[7] G. MOORE and N. SEIBERG, Classical and quantum conformal field theory, *Comm. Math. Phys.*, Vol. **123**, 1989, pp. 177-255.

[8] R. DIJKGRAAF, E. VERLINDE and H. VERLINDE, Modular invariance and the fusion algebra, *Conformal Field Theories and Related Topics*, P. BINÉTRUY, P. SORBA and R. STORA Eds., *Nucl. Phys.* **B.** (Proc. Suppl.), Vol. **5**, North Holland, 1988, pp. 87-97.

[9] A. KATO, Classification of modular invariant partition functions in two dimensions, *Mod. Phys. Lett.*, Vol. **A2**, 1987, pp. 585-600.

[10] T. GANNON, *Nucl. Phys.* Vol. **B 396**, 1993, pp. 708; and The classification of affine $su(3)$ modular invariant partition functions, *Comm. Math. Phys.* Vol. **161**, 1994, pp. 233-264. T. GANNON, The classification of Affine SU(3) Modular Invariant Partition Functions Revisited, texfile hep-th-9404185. T. GANNON and Q. HO-KIM, The low level modular invariant partition functions of rank two algebras, *Int. J. Mod. Phys.*, Vol. **A 9**, 1994, pp. 2667-2686. T. GANNON and Q. HO-KIM, The rank four heterotic modular invariant partition functions, *Nucl. Phys.*, Vol. **B 425**, 1994, pp. 319-342

[11] Ph. RUELLE, E. THIRAN and J. WEYERS, Implications of an arithmetical symmetry of the commutant for modular invariants, *Nucl. Phys.*, Vol. **B 402**, 1993, pp. 693-708. Ph. RUELLE, Thesis, unpublished.

[12] E. WITTEN, Quantum field theory and the Jones polynomial, *Comm. Math. Phys.*, Vol. **121**, 1989, pp. 351-399.

[13] N.Y. RESHETIKHIN and V.G. TURAEV, Invariants of 3-manifolds via link polynomials and quantum groups, *Invent. Math.*, Vol. **103**, 1991, pp. 547-597.

[14] D. ALTSCHULER and A. COSTE, Quasi-quantum groups, three manifolds and topological field theory, *Comm. Math. Phys.* Vol. **150**, 1992, pp. 83-107.

[15] P. DEGIOVANNI, Moore and Seiberg's equations and 3D topological field theories, *Comm. Math. Phys.*, Vol. **145**, 1992, pp. 459-505.

[16] T. KOHNO, Topological invariants for 3-manifolds using representations of mapping class groups (1), *Topology*, Vol. **31**, 1992, pp. 203-230.

[17] P. DEGIOVANNI, *Equations de Moore et Seiberg, théories topologiques et théorie de Galois*, Preprint ENSLAPP-L-458-94, March 1994.

[18] A. GROTHENDIECK, *Esquisse d'un programme*, Rapport Scientifique, 1984, unpublished.

[19] P. DEGIOVANNI, $\mathbb{Z}/N\mathbb{Z}$ Conformal Field Theories, *Comm. Math. Phys.*, Vol. **127**, 1990, pp. 71-99.
[20] *Abrégé d' histoire des mathématiques*, sous la direction de J. DIEUDONNÉ, Hermann, Paris, 1986. M. MALLIAVIN, *Algèbre commutative*, Masson, 1985.
[21] Ph. DI FRANCESCO and J.-B. ZUBER, Fusion potentials (1), *J. Phys.*, Vol. **A 26**, 1993, pp. 1441-1454.
[22] T. KAWAI, On the structure of fusion algebras, *Phys. Lett.*, Vol. **B 217**, 1989, pp. 247-251.
[23] D. GEPNER and E. WITTEN, String theory on group manifolds, *Nucl. Phys.*, Vol. **B 278**, 1986, pp. 493-549.
[24] J. FUCHS, B. GATO-RIVERA, B. SCHELLEKENS, and C. SCHWEIGERT, Modular invariants and fusion rule automorphisms from Galois theory, *Phys. Lett.*, Vol. **B 334**, 1994, pp. 113-120.
[25] D. GEPNER, Fusion rings and geometry, *Comm. Math. Phys.*, Vol. **141**, 1991, pp. 381-411. M. CRESCIMANO, Fusion Potentials for G_k and handle squashing, *Nucl. Phys.*, Vol. **B 393**, 1993, p. 361.
[26] J. HUMPHREYS, Introduction to Lie algebras and their representations, Springer GTM.
[27] D. COX, J. LITTLE and D. O'SHEA, Ideals, Varieties and Algorithms, Springer U.T.M., 1991. H. COHEN, *A Course in Computational Algebraic Number Theory*, Springer G.T.M. 138, 1993.
[28] HUA LOO KENG, Introduction to Number Theory, Springer (82). E. HECKE, *Vorlesungen über die Theorie der algebraischen Zahlen*, Chapter 3, reprinted in german by Chelsea.
[29] M. BAUER and C. ITZYKSON, *Springer proc. in Phys.*, J. M. LUCK, P. MOUSSA and M. WALDSCHMIDT Eds., Vol. **47**, 1990, pp. 20-32,
[30] L. KAUFFMAN, *proc. J. Hopkins workshop*, Florence, 1989, LUSANNA *et al.* Eds., World Scientific, On Knots, Princeton Univ. Press.
[31] R. KIRBY, A calculus for framed links in S_3, *Invent. Math.*, Vol. **45**, 1978, pp. 35-56.
[32] R. KIRBY, The topology of 4-manifolds, *Lecture Notes in Mathematics*, Vol. **1374**, Springer Verlag, 1989.
[33] R. KIRBY and P. MELVIN, On the 3-manifold invariants of Witten and Reshetikhin-Turaev for $sl(2,\mathbb{C})$, 1991.
[34] T. KOHNO, Invariants of 3-manifolds based on Conformal Field Theory and Heegard splittings, Quantum groups, (P. P. KULISH ed., *Lecture notes in Mathematics*, Vol. **1510**, Springer-Verlag, 1990, pp. 341-349.
[35] S. LANG, *Algebraic number theory*, Addison-Wesley (Reading), 1970.
[36] W. B. R. LICKORISH, *Invariants of three-manifolds from the combinatorics of the Jones polynomial*, Cambridge University, Preprint, 1991.
[37] J. P. SERRE, *Cours d'arithméthique,* P.U.F., 1970.

(Manuscript received July 5, 1994.)