Commun. Math. Phys. 127, 71–99 (1990)

Communications in
Mathematical
Physics

Z/NZ Conformal Field Theories

P. Degiovanni
LPTENS, 24 rue Lhomond, F-75005 Paris, France*

Abstract. We compute the modular properties of the possible genus-one characters of some Rational Conformal Field Theories starting from their fusion rules. We show that the possible choices of S matrices are indexed by some automorphisms of the fusion algebra. We also classify the modular invariant partition functions of these theories. This gives the complete list of modular invariant partition functions of Rational Conformal Field Theories with respect to the $A_N^{(1)}$ level one algebra.

Introduction

Since the important work of Belavin, Polyakov and Zamolodchikov [1], it has become clear that Conformal Field Theory (CFT) has exceptional properties in two dimensions. In particular, the symmetry of these theories is so huge that the hope of a possible classification has emerged. The main idea is to classify the states of a CFT using representations of the symmetry algebra of the theory.

Rational Conformal Field Theories, where only a finite number of representations appear, provide the simplest situation. Recently the application of these ideas through a detailed study of modular invariance on any surface (punctured or not punctured and in any genus) has produced remarkable results [2, 3, 4, 5]. One of the most amazing facts is the appearance of an unexpected relationship between the fusion rules of a RCFT and the modular properties of genus-one characters $\mathrm{tr}(q^{L_0})$. This relationship, due to Verlinde [6], leads to a new method of investigation of RCFTs: one can try to classify RCFTs starting from their fusion rules. This paper is an attempt at giving a few illustrations of this method.

In this approach, the first step is of course to find some fusion rules to work with. It appears that (finite) group theory provides us such material quite spontaneously. Verlinde's work enables us to recover the modular properties of

* Unité propre de Recherche du Centre National de la Recherche Scientifique, associée à l'Ècole Normale Supérieure et à l'Université de Paris-Sud

the characters on the torus. We recall a few basic facts in Sect. 1 and we show that the different choices of the matrix representing the modular transformation $\tau \to -1/\tau$ are related by certain automorphisms of the fusion rules. We explain how to carry this program for a finite abelian group. This program is completely achieved in the more pedagogical case of a cyclic group $\mathbf{Z}/N\mathbf{Z}$ in Sect. 2. We also mention some examples of RCFTs which have precisely these properties. In order to understand the structure of the theories considered in Sect. 2, we classify all their modular invariant partition functions in Sect. 3: namely, we find that there is exactly one modular invariant partition function associated with each divisor of N if N is odd (respectively $N/2$ if N is even). In Sect. 4, we collect a few interesting properties of these modular invariants.

This work has been motivated by our attempt to get familiar with Verlinde's work and by a recent work of C. Itzykson on $A_N^{(1)}$ level 1 theories [7]. He formulated a conjecture on the possible modular invariants which we prove in Sect. 3: the modular invariant partition functions are indexed by divisors of N when N is odd and divisors of $N/2$ when N is even. The reader interested in this proof can pass directly to Sect. 3.

1. Conformal Field Theory from Group Theory

Last year, an unexpected connection between the fusion rules and the modular properties of the characters has been discovered by E. Verlinde [6]. Our idea is to use Verlinde's theorem to reconstruct as much as possible a rational conformal theory from its fusion rules.

1.1 Verlinde's Theorem. Let us recall some basic facts about Verlinde's work. We will not give any proof but only give the main results. The main tool is the fusion algebra. Before going into details, let us state a few facts.

In a conformal field theory, the Hilbert space of states is a representation of the tensor product of two Virasoro algebras constructed from the analytic and the anti-analytic components of the energy momentum tensor $T(z)$ and $\bar{T}(\bar{z})$ respectively. Generally, this representation is reducible and each irreducible component corresponds to a primary field. In some cases, the Hilbert space is a finite sum of such representations. These theories have been classified by Cappelli, Itzykson and Zuber [8]. But it is well known that there exist many other conformal theories. The most natural case to consider is the case of Rational Conformal Field Theories (RCFTs). We say that a conformal theory is rational when there exist two operator algebras A_L and A_R consisting of analytic (respectively, anti-analytic) fields containing $T(z)$ (respectively, $\bar{T}(\bar{z})$), and $\mathbf{1}$ such that the Hilbert space of the theory is a finite sum of irreducible highest weight representations of $A_L \otimes A_R$. An example of this is provided by the WZW models (where the Sugawara construction holds). We will see other examples later. In the following, we will write φ_i for an irreducible highest weight representation of an extended algebra (such as A_L or A_R).

The building blocks of a conformal field theory are the chiral vertex operators. We refer the reader to the works of Moore and Seiberg [5], Tsuchiya and Kanie (in the context of affine algebras) [9] and also Frenkel, Lepowsky et al. [10] for a precise definition. Let us consider three irredicible highest weight representations of the chiral algebra A with associated vectors spaces V_i, V_j and V_k. The chiral vertex operators of type i, j, k are fields of linear operators which map $V_i \otimes V_j$ into V_k in a way which is coherent with the action of A on states defined as contour integral of holomorphic fields in A. The chiral vertex operators of type i, j, k form a vector space, noted $\begin{bmatrix} k \\ j, i \end{bmatrix}$, the dimension of which is used to define the fusion rules:

Definition 1. *The fusion rules are the* $N_{i,j}^k = \dim \begin{bmatrix} k \\ j, i \end{bmatrix}$.

Before recalling Verlinde's result, we must introduce other tools. Given a representation of an extended algebra we can define the associated character. Let V_i be such a representation, it is graded by the L_0 operator:

$$V_i = \bigoplus_{n \in \mathbb{N}} V_i^{(n)}, \quad L_0 = (h_i + n)\mathbf{1} \text{ on } V_i^{(n)},$$

where h_i is the eigenvalue of L_0 associated with the highest weight state of V_i. Then we define:

$$\chi_i(q) = \sum_{n \in \mathbb{N}} \dim V_i^{(n)} q^{n + h_i - c/24}.$$

We shall assume that these formal series are convergent in the unit disc with 0 deleted. Let q be equal to $\exp(2\pi i \tau)$, the modular properties of the characters are described by:

$$\chi_i(\tau + 1) = \exp\left(2\pi i\left(h_i - \frac{c}{24}\right)\right)\chi_i(\tau) = \sum_j T_i^j \chi_j(\tau), \tag{1}$$

$$\chi_i(-1/\tau) = \sum_j S_i^j \chi_j(\tau). \tag{2}$$

We also suppose that any representation φ_i of A has a conjugate representation $\varphi_{\hat{i}}$ with the same character but such that the operator product expansion of a representation and its conjugate contains the identity operator. This defines the matrix $C_i^j = \delta_{\hat{i}}^j$ which is an involution. Let us recall some properties of the fusion rules, one sees that:

$$N_{i,j,k} = N_{i,j}^{\hat{k}} \text{ is symmetric in } i, j, \text{ and } k,$$
$$N_{0,i}^j = \delta_i^j,$$

where 0 denotes the identity operator. We are now ready to recall Verlinde's result [6].

Theorem 1 (E. Verlinde). *The $N_{i,j}^k$'s are the structure constants of a commutative and associative algebra (called the fusion algebra) and S diagonalizes all the $\hat{N}_i$'s with $\hat{N}_i = (N_{i,j}^k)$:*

$$\hat{N}_i = S \hat{\Lambda}_i S^{-1},$$

where $(\hat{\Lambda}_i)_{j,k} = \delta_j^k \lambda_i^{(j)}$ and $\lambda_i^{(j)} = S_i^j / S_0^j$.

We finally obtain Verlinde's formula:

$$N_{i,j}^{k}=\sum_{n}\frac{S_i^n S_j^n S_n^{k*}}{S_0^n}. \tag{3}$$

Now, we would like to see to what extent the fusion rules determine the theory. For example, one can try to reconstruct the S matrix from these fusion rules. As soon as we have a set $\hat{N}_i$ of matrices the entries of which are the structure constants of a commutative and associative algebra with involution $i \rightarrow \hat{\imath}$, we can diagonalize them simultaneously with a unitary matrix S. We can also choose this matrix such that all S_0^i's are real positive numbers. As C is an automorphism of the fusion algebra, we have $\lambda_{\hat{\imath}}^{(j)}=\lambda_i^{(j)*}$ (complex conjugate) thus giving $CS=S^*$. The important point is that it is precisely the modular transformation matrix of the characters which does the job. This implies that $S^2=C$ and as was shown by Verlinde and Dijkgraaf, S is symmetric. We stress that this condition is absolutely necessary if we want this matrix to represent the modular properties of some characters!

Then, one can try to solve the equation $(ST)^3=\mathbf{1}$ in order to find the central charge and the dimensions that appear in this theory. We must stress that it is not clear whether there really exists a conformal field theory associated with these numbers. Moreover, the preceding equation, as we shall see later, does not determine uniquely the central charge and the dimensions. The asymptotic behaviour of the characters and factorization conditions restrict them further.

1.2 Possible S-Matrices and Automorphisms of the Fusion Rules. Given matrices $\hat{N}_i$ defining a fusion algebra and a possible S-matrix, one can try to find all other possible S-matrices.

Definition 2. *We define a possible S-matrix to be a symmetric unitary matrix which diagonalizes all $\hat{N}_i$'s and obeys $CS=SC=S^*$ and $S_0^i>S_0^0>0$ for all i's.*

This last assumption is justified in the case of a unitary theory. Below, we shall restrict ourselves to that case.

We have the following lemma:

Lemma. *Let $w'^{(j)}$ and $w''^{(j)}$ be two eigenbases for the $\hat{N}_i$'s then there exist a permutation σ and non-zero complex numbers η_i such that:*

$$w''^{(j)}=\eta_j w'^{(\sigma(j))}.$$

Proof. We know that the $\hat{N}_i$'s are simultaneously diagonalizable. Let us choose $E_i^{\alpha_i}$ an eigenspace of each matrix $\hat{N}_i$ and let us show that $\dim\left(\bigcap_i E_i^{\alpha_i}\right)<2$. This will show that if $w'^{(j)}$ is an eigenbasis for all $\hat{N}_i$'s, then each $w'^{(j)}$ has to belong to a one-dimensional vector space. This will prove the lemma.

Let E_i^{α} be the eigenspaces of $\hat{N}_i$ and define:

$$E_{[\alpha]}=\bigcap_i E_i^{\alpha_i}, \quad [\alpha]=(\alpha_i)_i.$$

Clearly $E_{[\alpha]}\cap E_{[\alpha']}=\{0\}$ when $[\alpha]\neq[\alpha']$. We also have:

$$\mathbf{C}^N = \sum_{[\alpha]} E_{[\alpha]} = \bigoplus_{[\alpha], E_{[\alpha]} \neq \{0\}} E_{[\alpha]}.$$

We denote by E_a the non-zero spaces, they are mutually orthogonal. We know that there exists an orthonormal eigenbasis $(w^{(j)})_j$ for the $\hat{N}_i$'s. If E_a contains a two-dimensional subspace, then there exists $l \neq j$ such that $(w^{(l)}, w^{(j)}) \in E_a^2$. Hence, $w^{(j)}$ and $w^{(l)}$ are associated with the same eigenvalues of $\hat{N}_i$ for any i. Therefore, the columns j, l of any matrix S diagonalizing all $\hat{N}_i$'s are proportional thanks to $\lambda_i^{(j)} = S_i^j / S_0^j$. This is clearly absurd. Finally all E_a's are one-dimensional and the lemma is proved.

If we consider now S and S' two possible S-matrices, we know by unitarity that $w^{(j)} = (S_i^j)_i$ and $w'^{(j)} = (S_i'^j)_i$ are two orthonormal eigenbases for the $\hat{N}_i$'s. By applying the lemma, there exist a permutation σ and complex numbers of unit modulus (by orthonormality) η_i such that:

$$S_i'^j = \eta_j S_i^{\sigma(j)}$$

for all i, j. The positivity of S_0^j and $S_0'^j$ implies that $\eta_j = 1$ for all j. The symmetry of S and S' implies that $S_i'^j = S_{\sigma(i)}^j$ for all i, j. We now use $CS = SC = S^*$ and $CS' = S'C = S'^*$ to show that $\sigma(\hat{j}) = \widehat{\sigma(j)}$. Finally, $w^{(\sigma(0))} = (S_i^{\sigma(0)})_i = (S_i'^0)_i$ has real positive coordinates, therefore the scalar product of $w^{(\sigma(0))}$ and $w^{(0)}$ is strictly positive and as $(w^{(j)})_j$ is an orthonormal basis, $\sigma(0) = 0$. Finally, we can use Verlinde's formula:

$$N_{\sigma(i),\sigma(j),\sigma(k)} = \sum_n \frac{S_{\sigma(i)}^n S_{\sigma(j)}^n S_{\sigma(k)}^n}{S_0^n} = \sum_n \frac{S_i^{\sigma(n)} S_j^{\sigma(n)} S_k^{\sigma(n)}}{S_0^{\sigma(n)}} = N_{i,j,k}.$$

We have shown that σ defines an automorphism of the fusion algebra.

Definition 3. *A permutation of the fields is called an automorphism of the fusion algebra if and only if it verifies*:

$$N_{\sigma(i),\sigma(j),\sigma(k)} = N_{i,j,k}, \quad \sigma(0) = 0, \quad \sigma(\hat{\imath}) = \widehat{\sigma(i)}.$$

Conversely, let σ be a permutation of the fields which defines an automorphism of the fusion algebra which verifies: $S_i^{\sigma(j)} = S_{\sigma(i)}^j$. We thus define $S_i'^j = S_i^{\sigma(j)}$. It is very easy to check that this matrix is a possible S-matrix. Finally, we have proved the following result:

Theorem 2. *Let S be a possible S-matrix for a given fusion algebra, then any other possible S-matrix is of the form*

$$S_i'^j = S_i^{\sigma(j)},$$

where σ defines an automorphism of the fusion algebra and verifies

$$S_{\sigma(i)}^j = S_i^{\sigma(j)}.$$

All such automorphisms define all possible S-matrices.

The condition $S_{\sigma(i)}^j = S_i^{\sigma(j)}$ ensures the symmetry of S'. We can also address in full generality what we call the equivalence problem. Let us suppose that we have a fusion algebra and a possible S-matrix associated with it, we would like to find, among other possible S-matrices, those which differ from S by a permutation of the representations. Then, one such matrix S' is defined by $S'^{j}_{i} = S^{\Sigma(j)}_{\Sigma(i)}$, where Σ is a permutation. In this case, it is clear that if T is a matrix defined in (1) and associated with S ($(ST)^3 = \mathbf{1}$), then $T'^{j}_{i} = T^{\Sigma(j)}_{\Sigma(i)}$ verifies $(ST)^3 = \mathbf{1}$ and can be considered as a T matrix associated with the fields $\varphi_{\Sigma(i)}$. We shall say that the two theories are equivalent (at the level of S and T). Notice that S' is symmetric. We then easily see that Σ must be an automorphism of the fusion algebra.

Conversely, we check that if Σ defines an automorphism of the fusion algebra, $S'^{j}_{i} = S^{\Sigma(j)}_{\Sigma(i)}$ is a possible S-matrix.

We shall now characterize the automorphisms σ such that the possible associated S-matrix $S'^{j}_{i} = S^{\sigma(j)}_{i}$ differs of S by a permutation of the fields. Let Σ be an arbitrary permutation which defines an automorphism of the fusion algebra, define $w^{(j)}_{\Sigma} = (S^{j}_{\Sigma(i)})$. Using the lemma, there exists a permutation $\tilde{\Sigma}$ such that $w^{(j)}_{\Sigma} = w^{\Sigma(j)}$. Finally, we have:

$$S^{j}_{\Sigma(j)} = S^{\tilde{\Sigma}(j)}_{i}, \quad S^{j}_{\tilde{\Sigma}(i)} = S^{\Sigma(j)}_{i},$$

which could have been used to define $\tilde{\Sigma}$. With this language, remark that $\tilde{\sigma} = \sigma$ in Theorem 2. Using these relations and $SC = CS = S^*$ we see that $\tilde{\Sigma}$ defines an automorphism of the fusion algebra. Moreover, the map $\Sigma \to \tilde{\Sigma}$ verifies $\Sigma_1 \Sigma_2 = \tilde{\Sigma}_2 \tilde{\Sigma}_1$ and $\Sigma^{-1} = \tilde{\Sigma}^{-1}$. We have $S^{\Sigma(j)}_{\Sigma(i)} = S^{\tilde{\Sigma}\Sigma(j)}_{i}$ and therefore:

Proposition 1. *If $S'^{j}_{i} = S^{\sigma(j)}_{i}$ is a possible S-matrix which is equivalent to S by a permutation Σ of the fields, then Σ defines an automorphism of the fusion algebra such that $\sigma = \tilde{\Sigma}\Sigma$.*

We shall see some illustrations of this result later. Remark the similarity between the correspondence $\Sigma \to \tilde{\Sigma}$ and matrix transposition. This will become clear in the analysis of RCFTs associated with abelian groups.

1.3 Conformal Field Theory and Group Theory. In order to carry out this program, one has to find some "nice" fusion rules. There exists a very natural way to generate some fusion rules: we can use finite group theory [11]. Let us consider G a finite group, it has a finite number of inequivalent irreducible representations which we denote by π_i. Any tensor product of them can be decomposed into irreducible representations:

$$\pi_i \otimes \pi_j = \bigoplus_k N^{k}_{i,j} \pi_k,$$

where $N^{k}_{i,j}$ is the multiplicity of the π_k representation. Thanks to the associativity and commutativity of the tensor product, the $\tilde{N}_i$'s define a representation of a commutative and associative algebra. Let $\pi_{\hat{\imath}}$ be the complex conjugate representation of π_i, then it is clear that $N^{\hat{k}}_{i,j}$ is symmetric in i, j and k because it is the multiplicity of the trivial representation of G in the tensor product $\pi_i \otimes \pi_j \otimes \pi_k$. Finally, if π_0 is the trivial representation, then $N^{j}_{0,i} = \delta^{j}_{i}$. Therefore these $N^{k}_{i,j}$ verify all hypotheses of Verlinde's theorem. In the corresponding field theory, with each irreducible representation of G, we associate a "primary field" such that the $N^{k}_{i,j}$ of finite group theory give us the fusion algebra of the underlying field theory. Naturally, the trivial representation of G is associated with the identity operator and two conjugate irreducible representations of G are associated with conjugate fields. We have not yet completed the analysis of this program,[1] and therefore we shall restrict ourselves to the case of finite abelian groups where things are simpler.

It is well known that every finite abelian group is a direct product of cyclic groups:

$$G \simeq \prod_{i=1}^{n} \frac{\mathbf{Z}}{N_i\mathbf{Z}}.$$

We shall use the following notation for group elements:

$$g \in G, \quad g = (g_1, \ldots, g_n),$$

where g_i is an integer mod N_i and we will use the additive notation. The irreducible representations of G are one-dimensional and are labelled by elements of G. To be more precise, define:

$$\forall (g, g') \in G^2, \quad \langle g, g' \rangle = \sum_{i=1}^{n} g_i g'_i / N_i \quad (\mathrm{mod}\ 1).$$

For a given $g \in G$ the representation associated with g is defined by

$$g' \to \exp(2\pi i \langle g, g' \rangle).$$

It is thus clear that:

$$N_{g,g'}^{g''} = \delta_{g+g'}^{g''}.$$

The eigenvalues of $\hat{N}_g$ are the $\exp(2\pi i \langle g, g' \rangle)$ for g' in G. Henceforth, for all $g \in G$, there exists a bijection σ_g of G such that $\lambda_g^{(g')} = \exp(2\pi i \langle g, \sigma_g(g') \rangle)$ and we must look for a symmetric matrix S which satisfies:

$$\frac{S_g^{g'}}{S_0^{g'}} = \lambda_g^{(g')}.$$

We easily find that:

$$S_g^{g'} = \frac{1}{\sqrt{|G|}} \exp(2\pi i \langle g, \sigma_g(g') \rangle)$$

with $|G|$ standing for the cardinal of G. In order to characterize more precisely σ_g, we introduce the following vector of $\mathbf{C}^{|G|}$:

$$\omega_g = (\exp(2\pi i \langle g, \sigma_g(g') \rangle))$$

and the hermitian product on $\mathbf{C}^{|G|}$:

$$\langle \alpha, \beta \rangle = \frac{1}{|G|} \sum_{g \in G} \alpha_g \overline{\beta_g}.$$

[1] Not every non-abelian finite group can be used for this purpose, we are still investigating this question. The main obstruction is the symmetry of the S matrix

Verlinde's relation (3) is in this case equivalent to:

$$\langle \omega_g \omega_{g'}, \omega_{g''} \rangle = \delta_{g+g'}^{g''}$$

for all g, g', g'' in G. But $(\omega_g)_{g\in G}$ is an orthonormal basis of $\mathbf{C}^{|G|}$ and thus $\omega_g\omega_{g'}$ is collinear to $\omega_{g+g'}$ and by comparing the first component of these vectors, $\omega_g\omega_{g'} = \omega_{g+g'}$. Using this property and the symmetry of S $((\omega_g)_{g'} = (\omega_{g'})_g)$, we find that:

$$S_g^{g'} = \frac{1}{\sqrt{|G|}} \prod_{(i,j)\in\langle 1,n\rangle^2} \exp(2\pi i K_{i,j} g_i g'_j),$$

where $K_{i,j}$ is of the form $B_{i,j}/(N_i \wedge N_j)$ with $B_{i,j}$ defined mod $N_i \wedge N_j$ and symmetric. Consequently, we have:

$$\sigma_g(g') = \left(\sum_{j=1}^{n} K_{i,j} g'_j \right)_i, \quad (\langle g, \sigma_g(g') \rangle \text{ is noted } K(g,g'))$$

which defines an automorphism σ_g (independent of g) of G as was shown before.

We shall now briefly indicate how to find the dimensions of primary fields and the central charge. For the sake of simplicity, we give here the method and carry out the detailed computation for $G = \mathbf{Z}/N\mathbf{Z}$ in the next section. We have to solve $(ST)^3 = \mathbf{1}$. This equation can be rewritten in the form:

$$e^{2\pi ic/8} \exp(-2\pi i(h_g + h_{g'} + K(g,g'))) = \frac{1}{\sqrt{|G|}} \sum_{k\in G} \exp(2\pi i(h_k + K(g+g',k))). \tag{4}$$

We also impose that $h_0 = 0$ and that $h_{-g} = h_g$. We obtain $2h_g - K(g,g) \equiv 0 \pmod 1$. We choose some representatives for the $B_{i,j}$ coefficients, and let us define ψ_g by $\exp(2\pi i h_g) = \psi_g \exp(i\pi K(g,g))$. Indeed any change of representatives for the $B_{i,j}$ can be compensated by a change of ψ_g. More precisely, suppose that we change $B_{i,j} \to B_{i,j} + W_{i,j}(N_i \wedge N_j)$, where $W_{i,j}$ are integers, then $\exp(2\pi i h_g)$ is multiplied by a factor $\exp(i\pi \sum W_{i,j} g_i g_j)$ which is 1 or -1. We shall therefore choose some representatives which are easy to handle. For example, we impose that $B_{i,j} = B_{j,i}$ not only in $\mathbf{Z}/(N_i \wedge N_j)\mathbf{Z}$ but also in $\mathbf{Z}$. With this choice, (4) is equivalent to:

$$\psi_g \psi_{g'} e^{2\pi ic/8} = \frac{1}{\sqrt{|G|}} \sum_{k\in G} \psi_k \exp(i\pi K(k+g+g', k+g+g')). \tag{5}$$

In order to solve this equation, one needs to perform some shifting of indices. Let $u = (\alpha_i N_i)$ a representative of the trivial element in G, then:

$$K(g+u, g+u) = K(g,g) + 2K(g,u) + K(u,u)$$

and

$$\tfrac{1}{2}K(u,u) = \sum_{i<j} B_{i,j}\alpha_i\alpha_j \frac{N_i N_j}{N_i \wedge N_j} + \frac{1}{2}\sum_i B_{i,i}\alpha_i^2 N_i.$$

So, everything can be done safely if and only if $B_{i,i}$ is even when N_i is odd: $K(g+u, g+u) \equiv K(g,g) \pmod 2$. We can always consider this case by shifting $B_{i,i}$

of N_i when necessary. With this choice, we find that $\psi_{-g}=\psi_g$ and $\psi_{g+u}=\psi_g$. Specializing $\psi_0=1$ in Eq. (5); we find that $\psi_{g+g'}=\psi_g\psi_{g'}$, and therefore $g\to\psi_g$ is a morphism of G into $\{-1,1\}$. It is thus determined by its value on the generators of G. In our example, the generators are the $g^{(j)}=(\delta_i^j)_i$ of order N_i. This constraints $\psi_{g^{(j)}}=1$ if N_i is odd, in the other cases $\psi_{g^{(j)}}=\pm 1$. At this point, we see that the central charge is determined mod 8 and the dimensions mod 1 (because we can multiply any solution T of $(ST)^3=\mathbf{1}$ by $\exp(2\pi i/3)$). Here, let us analyze the previously mentioned equivalence problem. S and S' are equivalent in this sense if and only if there exists Σ permutation of G such that $K(\Sigma(g),\Sigma(g'))=K'(g,g')$ modulo integers, and as we have seen before Σ is an automorphism of G. Therefore, as proved more generally in 1.2, Σ defines an automorphism of the fusion rules hence of the group G. The condition on S means that $K(g,g')=K(\Sigma(g),\Sigma(g'))$ modulo integers. We can find the equivalence classes of K matrices in some interesting cases:

Case $G=(\mathbf{Z}/p\mathbf{Z})^n$, p odd prime. In this case, $N_i=p$ for all i. Σ is defined by its action on the n generators and can be represented by a $n\times n$ matrix with entries in the finite field $\mathbf{Z}/p\mathbf{Z}$. B is also a $n\times n$ matrix with entries in the same set. Translating the previous conditions into this language, we find that $\Sigma^t B\Sigma=B$, where Σ^t is the transposed matrix of Σ. We are reduced to classifying non-degenerate (B defines an automorphism of G) quadratic forms on the n dimensional vector space over the field $\mathbf{Z}/p\mathbf{Z}$. This problem has been solved a long time ago. Let us recall the result [12]:

Theorem 3. *Any non degenerate quadratic form defined on $\mathbf{F}^n$ where $\mathbf{F}$ is a finite field with odd characteristic is equivalent to*:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & 0 \\ \vdots & \ddots & \vdots & \\ 0 & & 1 & 0 \\ 0 & \cdots & 0 & a \end{pmatrix}, \quad \textit{a not zero and defined modulo a square.}$$

We only have two cases. The matrix B is diagonal. We are thus led to the case G cyclic which is the subject of the next section. In this case, we shall be able to compute the Gaussian sums which give the central charge mod 8.

2. Dimensions and Central Charges in Z/NZ Theories

2.1 Determination of S and T. In this section, we shall focus on theories associated with a cyclic group. More precisely, all the representations of the symmetry algebra of the theory are indexed by an integer mod N and the fusion rules are:

$$N_{i,j}^k=\delta_{i+j,k}.$$

In this case, as we have seen in the previous section, we can compute the S matrix and we find that there exists an automorphism σ of the fusion rules, hence of the group $\mathbf{Z}/N\mathbf{Z}$ such that:

$$S_{n,m}=\frac{1}{\sqrt{N}}\exp\left(2\pi i\frac{n\sigma(m)}{N}\right).$$

In the $\mathbf{Z}/N\mathbf{Z}$ case, the automorphisms are rather trivial: they are given by an integer a invertible mod N and map x to ax. We thus have to solve $(ST)^3=\mathbf{1}$ with $S_{n,m}=N^{-1/2}\exp(2\pi ianm/N)$ and we also impose that $h_0=0$ and $h_{N-n}=h_n$. As we have seen in the previous section:

$$\exp(2\pi ih_n)=\psi_n\exp\left(2\pi i\frac{an^2}{2N}\right),\quad \psi_n=\pm 1$$

with $\psi_0=1$ and $\psi_{N-n}=(-1)^{Na}\psi_n$. As explained in the general case, we must distinguish two cases according to N's parity. When N is even, a is defined mod N and if N is odd a is defined mod $2N$ and is assumed to be even. This enables $n\rightarrow\psi_n$ to define a group homomorphism from $\mathbf{Z}/N\mathbf{Z}$ into $\{1,-1\}$. Therefore, we find:

N **even.** In this case, a is odd. In this case, $\psi_1=\pm 1$ and both possibilities can be realized,

$$\psi_k=1,\quad e^{2\pi ic/8}=\frac{1}{\sqrt{2}}S_{2N}(a),$$

$$\psi_k=(-1)^k,\quad e^{2\pi ic/8}=\frac{1}{\sqrt{2}}S_{2N}(a)\exp\left(-\frac{2\pi iNa^{-1}}{8}\right).$$

We explain how to compute the Gaussian sum $S_{2N}(a)$ in appendix 1 and the reader will check that we find real central charges for the theories considered here. Finally, we check that $(ST)^3=\mathbf{1}$ is satisfied by our solutions. This solves the problem of finding all dimensions and central charges in this case.

N **odd.** Here, a is defined mod $2N$ and is even. We also have $\psi_1=1$ and therefore, we only have one solution which is given by:

$$\psi_n=1,\quad \exp\left(2\pi i\frac{c}{8}\right)=S_N(b).$$

This completely solves our problem.

2.2 Dimensions and Central Charges, Discussion of some Examples. We have obtained the complete set of dimensions mod 1 and central charges mod 8. It is interesting to compare the different lists of dimensions mod 1 for different a's. We have already analyzed this equivalence problem in some more complicated cases. Here, a and a' give the same list if and only if a/a' is a square in $\mathbf{Z}/N\mathbf{Z}$. In Appendix B, we identify the group $U(\mathbf{Z}/N\mathbf{Z})/U(\mathbf{Z}/N\mathbf{Z})^{(2)}$, where $U(\mathbf{Z}/N\mathbf{Z})$ is the group of invertible elements in the ring $\mathbf{Z}/N\mathbf{Z}$ and $U(\mathbf{Z}/N\mathbf{Z})^{(2)}$ is the set of invertible elements which are squares. We refer the reader to Appendix B for detailed results. A surprise is that $U(\mathbf{Z}/N\mathbf{Z})/U(\mathbf{Z}/N\mathbf{Z})^{(2)}$ in general has more than two elements. In fact, we already know some examples of $\mathbf{Z}/N\mathbf{Z}$ theories.

The rational gaussian model is the simplest example. We consider a free boson X compactified on a circle of radius R and with action:

$$S=\frac{1}{4\pi}\int \partial X\bar{\partial}X\,d^2z.$$

The Hilbert space of this theory decomposes into irreducible representations of the "$U(1)_L\times U(1)_R$ current algebra" generated by $\partial X,\bar{\partial}X$.

The highest weight states relatively to the $U(1)$ current algebra are created by chiral vertex operators $\exp(ipX_L(z))$. The dimension of this field is given by $h_p=p^2/2$. The quantum number associated with $U(1)$ is p.

In the case of the gaussian model, the allowed values of $(p,\bar{p})$ belong to a two-dimensional even self dual Lorentzian lattice as a consequence of modular invariance. Therefore, this theory is not trivially rational. We need to enlarge the symmetry by imposing that there exists a $U(1)_L\times U(1)_R$ primary field which has $\bar{h}=0$. This condition constrains the radius, we find that:

$$\frac{R^2}{2}=p/q,\quad p\wedge q=1.$$

In this case, we obtain a spin pq conserved current. The extended algebra has already been written down by Moore and Seiberg [4]. They have also written the generalized characters. These are indexed by an integer mod $N=2pq$ and have the following transformation law under a modular transformation:

$$S_n^m=\frac{1}{\sqrt{2pq}}\exp\left(2\pi i\frac{nm}{2pq}\right),\quad T_n^m=\delta_n^m\exp\left(2\pi i\frac{n^2}{4pq}\right),$$

Therefore, using Verlinde's formula, we find that in this model:

$$N_{i,j}^k=\delta_{i+j,k}.$$

We note that the highest weight states of the irreducible representations of the extended algebra are created by vertex operators, the operator product expansion of which is known to be additive. These theories correspond to the case $a=1,N$ even and $\psi_n=1$.

Another example has been recently exhibited by C. Itzykson [7]. He showed that the $A_N^{(1)}$ level 1 theories have $\mathbf{Z}/N\mathbf{Z}$ fusion rules. In this case, N can be even or odd, a is equal to $N-1$ and $\psi_n=1$. We refer the reader to his paper for more details on the computation of the S and T matrices.

E. Verlinde pointed out to us that the $E_6^{(1)}$ level one theories have $\mathbf{Z}/3\mathbf{Z}$ fusion rules and the $E_7^{(1)}$ level one theories correspond to $\mathbf{Z}/2\mathbf{Z}$. The dimensions and the central charges can be computed using our formulas with $a=1$ and $\psi_n=(-1)^n$ for E_7 and $a=1$ for E_6.

These are clearly not the only possibilities! Let us take for example N prime different from 2 and 3, $\mathbf{Z}/N\mathbf{Z}$ is a simple group and therefore, we cannot decompose our theory into pieces. The only example we know is given by $SU(N)$ at level one, but here $U(\mathbf{Z}/N\mathbf{Z})/U(\mathbf{Z}/N\mathbf{Z})^{(2)}=\mathbf{Z}/2\mathbf{Z}$. There is one extra possibility. See Appendix B for a complete list. The important question is to know whether the other cases can be realized by conformal field theories. We don't have any answer to this reconstruction problem.

3 Classification of Modular Invariants for $\mathbf{Z}/N\mathbf{Z}$ Theories

3.1 Notation and Methods. In this section, we consider a set of N characters χ_λ which transform under the modular group as:

$$\chi_\lambda(-1/\tau) = \sum_{\lambda'\in\mathbf{Z}/N\mathbf{Z}} S_{\lambda,\lambda'}\chi_{\lambda'}(\tau)$$

$$\chi_\lambda(\tau+1) = \sum_{\lambda'\in\mathbf{Z}/N\mathbf{Z}} T_{\lambda,\lambda'}\chi_{\lambda'}(\tau),$$

where the S matrix via Verlinde's theorem gives $\mathbf{Z}/N\mathbf{Z}$ fusion rules. In this case, we know S and T have the following expressions:

$$S_{\lambda,\lambda'} = \frac{1}{\sqrt{N}}\exp\left(2\pi i a\frac{\lambda\lambda'}{N}\right), \quad T_{\lambda,\lambda'} = \delta_{\lambda,\lambda'}\exp\left(2\pi i\left(\frac{a\lambda^2}{2N} - \frac{c}{24}\right)\right), \tag{6}$$

where a is an integer mod $2N$, a and N are coprime and a is even when N is odd. We are looking for modular invariant partition functions of the form $Z = \Sigma\hat{N}_{\lambda,\bar{\lambda}}\chi_\lambda\overline{\chi_{\bar{\lambda}}}$ with multiplicities $\hat{N}_{\lambda,\bar{\lambda}}\in\mathbf{N}$.

In fact, characters of adjoint representations are equal and we impose not only modular invariance of the partition function but of the operator content of the theory. This remark leads to the following equations:

$$S^\dagger\hat{N}S = \hat{N}, \quad T^\dagger\hat{N}T = \hat{N}. \tag{7}$$

The phase $\exp(-2\pi i c/24)$ which appears in T doesn't play any role in equation (7), and we shall forget it in the following. We shall proceed in two steps: we first solve equation (7) with $\hat{N}\in M_N(\mathbf{C})$ and then we impose the integrality and positivity conditions on $\hat{N}$. Finally we shall find that solutions are labelled by divisors of N when N is odd and by divisors of $N/2$ when N is even. The set of matrices satisfying (7) will be called the commutant in the following and noted C_a.

3.2 Finding the Commutant. Cappelli, Itzykson and Zuber (denoted by CIZ below) have introduced a suitable basis of $M_N(\mathbf{C})$: $(P^kQ^l)_{k,l}$ with $(k,l)\in(\mathbf{Z}/N\mathbf{Z})^2$ and $P_{\lambda,\lambda'} = \delta_{\lambda,\lambda'+1}$ and $Q_{\lambda,\lambda'} = \delta_{\lambda,\lambda'}\exp(2\pi i\lambda/N)$. Then an easy computation shows that:

$$S^\dagger PS = Q^{-a}, \quad T^\dagger PT = \exp(-2\pi i a/2N)PQ^{-a},$$
$$S^\dagger Q^a S = P; \quad T^\dagger Q^a T = Q^a.$$

Therefore if we let $\bar{Q} = Q^a$, the following relations hold:

$$\begin{aligned} &P^N = \bar{Q}^N = 1; \quad P\bar{Q} = \bar{Q}P\exp\left(-2\pi i\frac{a}{N}\right) \\ &S^\dagger PS = \bar{Q}^{-1}, \quad T^\dagger PT = \exp(-2\pi i a/2N)P\bar{Q}^{-1}, \\ &S^\dagger\bar{Q}S = P; \qquad T^\dagger\bar{Q}T = \bar{Q}, \end{aligned} \tag{8}$$

$\bar{Q}, P, \exp(2\pi i a/N)$ define a representation of the Heisenberg group similar to the one used by CIZ [8] and Gepner and Qiu [13]. Moreover, $a \wedge N = 1$ shows that $(P^k\bar{Q}^l)$ with $k, l \pmod N$ is a basis of $M_N(\mathbf{C})$. Equations (8) enable us to prove that:

$$\forall \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \in SL_2(\mathbf{Z}),$$

$$\begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} \cdot P^k\bar{Q}^l = \exp\left(2\pi i \frac{a}{2N}(\bar{a}\bar{b}k^2 + \bar{c}\bar{d}k^2 + 2\bar{b}\bar{c}kl)\right) P^{\bar{a}k+\bar{c}l}\bar{Q}^{\bar{b}k+\bar{d}l}. \tag{9}$$

Only $\Gamma^{2N} \cong SL_2(\mathbf{Z}/2N\mathbf{Z})$ acts non-trivially. Consequently, a generating family of the commutant can be obtained by averaging the $P^k\bar{Q}^l$ under this finite group. A basis is found by restricting k, l to lie in a fundamental domain of $(\mathbf{Z}/N\mathbf{Z})^2$ under the action of Γ^N provided that we only consider k, l such that the average of $P^k\bar{Q}^l$ under the modular group is not zero.

There exists a very natural morphism of rings from $\mathbf{Z}/2N\mathbf{Z}$ onto $\mathbf{Z}/N\mathbf{Z}$ defined by the restriction $\operatorname{mod} N$. This morphism lifts to a group morphism on special linear groups defined on these rings and we call its kernel H. CIZ have shown that in the case where N is even this restricts k, l to be even if we want the average of $P^k\bar{Q}^l$ to be non-zero under H (and then under Γ^{2N}). It is easy to analyze the same problem in the case N odd. The group H then has 6 elements and is isomorphic to Σ_3. Moreover, we check that $P^k\bar{Q}^l$ is H-invariant, which shows that a basis of the commutant is given by:

$$\frac{1}{|\Gamma^{2N}|}\sum_{A\in\Gamma^{2N}} A\cdot\bar{Q}^{2\delta}, \quad \delta | n, \quad \text{for} \quad N \text{ even},$$

$$\frac{1}{|\Gamma^{N}|}\sum_{A\in\Gamma^{N}} A\cdot\bar{Q}^{\delta}, \quad \delta | n, \quad \text{for} \quad N \text{ odd},$$

where $n = N$ if N is odd, and $n = N/2$ for N even below.

For our purpose, it will be convenient to obtain a second basis of C_a consisting of matrices with integer entries. We consider the matrices $\Omega^{(\delta)}$, $\delta | n$ introduced by CIZ. Let δ be a divisor of n and define $\alpha = \delta \wedge n/\delta$. Then, there exist $(a', b') \in \mathbf{Z}^2$ such that $a'n/\delta\alpha - b'\delta/\alpha = 1$ and we define $\omega(\delta) = a'n/\delta\alpha + b'\delta/\alpha \pmod{N/\alpha^2}$. We thus define the following matrices:

$$\Omega^{(\delta)}_{\lambda,\bar{\lambda}} = \begin{cases} 0 \quad \text{if} \quad \lambda \text{ or } \bar{\lambda} \text{ is not zero} \bmod \alpha \\ \sum_{\xi\in\mathbf{Z}/\alpha\mathbf{Z}} \delta_{\bar{\lambda},\omega(\delta)\lambda+\xi N/\alpha} \end{cases}. \tag{10}$$

Indeed in the case N odd, the number $\omega(\delta)$ changes by a multiple of $2N/\alpha^2$ when one changes a' and b' preserving $a'n/\delta\alpha - b'\delta/\alpha = 1$ but in the definition of the matrix $\Omega^{(\delta)}$, we only need $\omega(\delta) \bmod N/\alpha^2$. Let us discuss the two cases successively:

N even. We extend here the results found by CIZ by taking account of the occurrences of $a \neq 1$ in the expressions of S and T. It is clear that $\Omega^{(\delta)}_{\lambda,\bar{\lambda}} = \Omega^{(\delta)}_{a\lambda,a\bar{\lambda}}$. Let $S^{(1)}_{\lambda,\bar{\lambda}} = \exp(2\pi i\lambda\bar{\lambda}/N)/\sqrt{N}$, then CIZ showed that $S^{(1)}\Omega^{(\delta)} = \Omega^{(\delta)}S^{(1)}$ and that the $\Omega^{(\delta)}$'s form a free family. We have:

$$S_{\lambda,\bar{\lambda}} = S^{(1)}_{a\lambda,\bar{\lambda}},$$

and then $S\Omega^{(\delta)}=\Omega^{(\delta)}S$. In the same way:

$$\Omega^{(\delta)}_{\lambda,\bar{\lambda}}\neq 0 \Rightarrow \lambda^2-\bar{\lambda}^2\equiv 0 \pmod{2N}$$

shows that $T\Omega^{(\delta)}=\Omega^{(\delta)}T$. Then $\Omega^{(\delta)}\in C_a$; but $\dim C_a = Nb$ *of divisors of* n and this shows that $(\Omega^{(\delta)})_{\delta|n}$ is a basis of C_a.

N odd. This case has not been considered by CIZ and thus we describe in more detail how to find the commutant. Let us introduce the following matrices for each divisor δ of N:

$$\Omega'^{(\delta)}=\frac{\delta}{N}\sum_{(x,y)\in(\mathbf{Z}/N/\delta\mathbf{Z})^2}\exp\left(2\pi i\frac{axy\delta^2}{2N}\right)P^{\delta x}\bar{Q}^{\delta y}.$$

Partitioning $(\mathbf{Z}/(N/\delta)\mathbf{Z})^2$ using $k=x\wedge y\wedge(N/\delta)$ shows that:

$$\Omega'^{(\delta)}=\frac{\delta}{N}\sum_{k|(N/\delta)}\frac{k\delta}{N}|\Gamma^{N/k\delta}|M_{k\delta},$$

where $M_{k\delta}$ denotes the average of $\bar{Q}^{k\delta}$. Therefore $\Omega'^{(\delta)}\in C_a$. An elementary computation shows that:

$$\forall(\lambda,\bar{\lambda})\in(\mathbf{Z}/N\mathbf{Z})^2,\quad \Omega^{(\delta)}_{\lambda,\bar{\lambda}}=\Omega'^{(\delta)}_{\lambda,\bar{\lambda}}.$$

Consequently the $\Omega^{(\delta)}_{\delta|n}$ form a basis of the commutant.

At this stage, we have found a basis of the commutant consisting of matrices with integers coefficients.

Theorem 4. *$(\Omega^{(\delta)})_{\delta|n}$ is a basic of C_a.*

Consequently, all C_a's are equal, we shall denote them by C in the following.

3.3 Imposing Integrality and Positivity: General Results. We shall now impose the integrality and positivity condition.

$$\hat{N}=\sum_{\delta|n}c_\delta\Omega^{(\delta)};\quad \hat{N}_{\lambda,\bar{\lambda}}\in\mathbf{N}.$$

We also impose unicity of the vacuum which is the $\lambda=\bar{\lambda}=0$ operator: $\hat{N}_{0,0}=\sum_{\delta|n}c_\delta=1$. The idea is to write a subset of conditions which implies that all the c_δ are non-negative integers. Our idea is to look for the indices for which only a small number of $\Omega^{(\delta)}$'s have non-zero entries. Hence, it is convenient to fix δ and to analyze what happens in the row $\lambda=\alpha(\delta)$ of the matrix $\hat{N}$: this row is the first apart from the row $\lambda=0$ where $\Omega^{(\delta)}$ has non-zero entries. More precisely, we shall show in Subsect. 3.4 that when N is odd or when N and $n/\alpha(\delta)^2$ are even (see Subsect. 3.5), the row $\lambda=\alpha(\delta)$ of $\hat{N}$ contains at least one coefficient equal to c_δ and thus $c_\delta\in\mathbf{N}$. In the cases where N is even and $n/\alpha(\delta)^2$ is odd, there exist two divisors δ_+ and δ_- such that $c_\delta+c_{\delta_+}, c_\delta+c_{\delta_-}$ appear as entries in the row $\lambda=\alpha(\delta)$ and all other coefficients in this row are either 0 or are greater than the two preceding ones. In Subsect. 3.6, we shall see how to solve the integrality and positivity condition with this result. Let us state the final result:

Theorem 5. *The modular invariant partition functions satisfying the integrality and* *positivity requirements and the unicity of the vacuum are given by*:

$$Z_\delta(\tau) = \sum_{(\lambda,\bar\lambda)\in(\mathbf{Z}/N\mathbf{Z})^2} \Omega^{(\delta)}_{\lambda,\bar\lambda}\chi_\lambda(\tau)\overline{\chi_{\bar\lambda}(\tau)}, \quad \delta|n.$$

We shall first prove a few general lemmas and then, by a detailed counting of coefficients of different types in the appropriate rows, prove the announced result and conclude. The aim of this subsection is to show that we only need to look at a limited number of divisors δ' to find isolated coefficients c_δ in row $\alpha(\delta)$ (Proposition 3).

In the following, we shall note for δ and δ' two divisors of n:

$$P_\delta = \{\alpha(\delta)\omega(\delta) + N\xi/\alpha(\delta)/\ \xi\in\mathbf{Z}/\alpha(\delta)\mathbf{Z}\},$$
$$P_{\delta',\alpha(\delta)} = \{\alpha(\delta)\omega(\delta') + N\xi/\alpha(\delta')/\ \xi\in\mathbf{Z}/\alpha(\delta')\mathbf{Z}\},$$

where $\alpha(\delta')|\alpha(\delta)$. We shall note α for $\alpha(\delta)$ when no ambiguity is present. P_δ is the set of column numbers λ for which $\Omega^{(\delta)}_{\alpha,\lambda} \neq 0$ and $P_{\delta',\alpha}$ is the set of column numbers such that $\Omega^{(\delta')}_{\alpha,\lambda} \neq 0$.

We will use intensively the following lemmas:

Lemma 1. *If* $\alpha(\delta) = \alpha(\delta')$, *then*

$$P_\delta \cap P_{\delta'} \neq \emptyset \Leftrightarrow P_\delta = P_{\delta'} \Leftrightarrow \Omega^{(\delta)} = \Omega^{(\delta')} \Leftrightarrow \delta = \delta' \Leftrightarrow \omega(\delta) \equiv \omega(\delta') \pmod{N/\alpha(\delta)^2}.$$

Lemma 2. *If* $\alpha(\delta')|\alpha(\delta)$, *then*

$$P_\delta \cap P_{\delta',\alpha(\delta)} \neq \emptyset \Leftrightarrow P_{\delta',\alpha(\delta)} \subset P_\delta \Leftrightarrow \omega(\delta') \equiv \omega(\delta) \pmod{N/\alpha(\delta)^2}.$$

Lemma 3. *If* $\alpha(\delta') = \alpha(\delta'') = \alpha'$ *is a divisor of* $\alpha(\delta)$, *then*

$$P_{\delta'',\alpha(\delta)} \cap P_{\delta',\alpha(\delta)} \neq \emptyset \Leftrightarrow P_{\delta'',\alpha(\delta)} = P_{\delta',\alpha(\delta)} \Leftrightarrow \omega(\delta') \equiv \omega(\delta'') \pmod{N/\alpha(\delta)\alpha'}.$$

Lemma 4. *If* $\alpha(\delta'')|\alpha(\delta')$ *and* $\alpha(\delta')|\alpha(\delta)$, *then*

$$P_{\delta'',\alpha(\delta')} \subset P_{\delta'} \quad \textit{and} \quad P_{\delta',\alpha(\delta)} \subset P_\delta \Rightarrow P_{\delta'',\alpha(\delta)} \subset P_\delta.$$

Proof. We shall only prove Lemma 2, the method being similar for the others. It is clear that $P_{\delta',\alpha(\delta)} \subset P_\delta$ leads to $\omega(\delta') \equiv \omega(\delta) \pmod{N/\alpha(\delta)^2}$ and that the converse is also true. Suppose now that $P_\delta \cap P_{\delta',\alpha(\delta)} \neq \emptyset$ then there exists $\xi\in\mathbf{Z}/\alpha\mathbf{Z}$ such that $\alpha\omega(\delta') + N\xi/\alpha(\delta') \equiv \alpha\omega(\delta) \pmod{N/\alpha(\delta)}$; but $\alpha(\delta')|\alpha(\delta)$ so $\alpha\omega(\delta') \equiv \alpha\omega(\delta)$ $\pmod{N/\alpha(\delta)}$. This proves Lemma 2.

We now prove that any $P_{\delta',\alpha}$ lies inside a P_δ:

Proposition 2. *Given* α *such that* $\alpha^2|n$ *and* $\delta'|n$ *with* $\alpha(\delta')|\alpha$, *there exists* $\delta|n$ *such that* $\alpha(\delta) = \alpha$ *and* $P_{\delta',\alpha} \subset P_\delta$.

We need a lemma:

We consider the vector subspace of the commutant defined by:

$$C^\alpha = \{M\in C/\lambda \neq 0 \pmod{\alpha} \text{ or } \lambda' \neq 0 \pmod{\alpha} \Rightarrow M_{\lambda,\lambda'} = 0\}.$$

Then the following lemma holds:

Lemma. $C^\alpha = \mathrm{Vect}\,(\Omega^{(\delta)})_{\alpha|\alpha(\delta)}$.

Proof. Clearly $\Omega^{(\delta)}$ for $\alpha|\alpha(\delta)$ belongs to C^α; we also know that $(\Omega^{(\delta)})_{\delta|n}$ is a basis of C and thus let us decompose an element M of C^α over this basis,

$$M = \sum_{\delta | n} c_\delta \Omega^{(\delta)}.$$

We take δ_0 such that $c_{\delta_0} \neq 0$ and such that $\alpha(\delta_0)$ is minimal. Due to Lemma 1, the coefficients c_δ for different δ's such that $\alpha(\delta) = \alpha(\delta_0)$ in row $\alpha(\delta_0)$ appear in different columns. No divisor having $\alpha(\delta) \neq \alpha(\delta_0)$ can contribute in this row because $\alpha(\delta_0)$ is minimal. Consequently $\alpha | \alpha(\delta_0)$ if $M \in C^\alpha$. By recurrence the lemma is now clear.

Proof. Define for $\alpha^2 | n$ G_α by:

$$G_\alpha = \{\omega \in \mathbf{Z}/(N/\alpha^2)\mathbf{Z} / \, \omega^2 = 1 \ (\operatorname{mod} N/\alpha^2)\}, \qquad N \text{ odd}$$
$$\text{resp } G_\alpha = \{\omega \in \mathbf{Z}/(N/\alpha^2)\mathbf{Z} / \, \omega^2 = 1 \ (\operatorname{mod} 2N/\alpha^2)\}, \qquad N \text{ even.}$$

Then consider α', α two divisors of n such that $\alpha' | \alpha$. We can define for $\omega' \in G_{\alpha'}$,

$$\Omega^{(\omega', \alpha)}_{\lambda, \lambda'} = \begin{cases} 0 \quad \text{if} \quad \alpha \text{ doesn't divide } \lambda \text{ or } \lambda' \\ \sum\limits_{\xi \in \mathbf{Z}/\alpha' \mathbf{Z}} \delta_{\lambda', \omega' \lambda + N\xi/\alpha'} \end{cases},$$

and clearly $\Omega^{(\omega', \alpha)} \in C^\alpha$. So if $\alpha(\delta') | \alpha$ then $\omega(\delta') \in G_{\alpha(\delta')}$. But $\Omega^{(\omega(\delta'), \alpha)} \in C^\alpha$ and we have from the expressions of the different matrices:

$$\Omega^{(\delta')}_{\alpha, \lambda} \neq 0 \Leftrightarrow \Omega^{(\omega(\delta'), \alpha)}_{\alpha, \lambda} \neq 0.$$

We then decompose the latter matrix on the basis found for C^α in the lemma and this shows that $P_{\delta', \alpha}$, i.e. the column indices of non-zero elements of $\Omega^{(\delta')}$ in the row α are in the union of the P_δ's for δ such that $\alpha(\delta) | \alpha$ and $\alpha | \alpha(\delta)$ hence $\alpha(\delta) = \alpha$. Proposition 1 then follows from Lemma 2.

Proposition 3. *Let α be such that $\alpha^2 | n$:*

$$\bigcup_{\substack{\delta'; \alpha(\delta') | \alpha \\ \alpha(\delta') \neq \alpha}} P_{\delta', \alpha} = \bigcup_{p \, prime, \, p | \alpha} \left(\bigcup_{\delta'; \alpha(\delta') = \alpha/p} P_{\delta', \alpha} \right). \tag{11}$$

Proof. Consder any δ' such that $\alpha(\delta') | \alpha$ and $\alpha(\delta') \neq \alpha$, then there exists a prime number p verifying $\alpha(\delta') | (\alpha/p)$. Then we use Proposition 3 to find δ'' such that $\alpha(\delta'') = \alpha/p$ and $P_{\delta', \alpha/p} \subset P_{\delta''}$; then Lemma 4 shows that $P_{\delta', \alpha} \subset P_{\delta'', \alpha}$ and this proves Proposition 3.

This proposition show that it is sufficient to look at a small number of divisors to study what happens in row α. We only need to compute the cardinal of the second set appearing in Proposition 3 and compare it to $\alpha = |P_\delta|$. Before getting to this point, we need a last result:

Proposition 4. *If $\omega \in G_\alpha (\alpha^2 | n)$ there exists a unique divisor δ of n such that $\alpha(\delta) = \alpha$ and $\omega(\delta) = \omega$.*

Proof. The unicity is quite obvious because two divisors having the same ω and α would define the same matrix $\Omega^{(\delta)}$'s and thus must be equal by linear independence of the $\Omega^{(\delta)}$. Consider now the existence problem and take $\omega \in G_\alpha$. There exists $(\rho, \bar{\rho})$, $\rho \bar{\rho} = N/\alpha^2$ (respectively $2N/\alpha^2$) if N is odd (respectively if N is even) and $(x, y) \in \mathbf{Z}^2$

such that:

$$\omega - 1 = x\rho, \quad \omega + 1 = y\bar{\rho}. \tag{12}$$

For N odd, ρ and $\bar{\rho}$ are odd and therefore by shifting ω of N/α^2 if necessary, one can choose x and y to be even. We then introduce $\delta = \alpha\rho$. By rewriting Eq. (12) one finds:

$$\omega = \frac{x}{2}\frac{\delta}{\alpha} + \frac{y}{2}\frac{N}{\delta\alpha}\left(\operatorname{mod}\frac{N}{\alpha^2}\right), \quad 1 = \frac{y}{2}\frac{N}{\delta\alpha} - \frac{x}{2}\frac{\delta}{\alpha}$$

which gives the result.

In the case N even, the same kind of method can be used but with more care because of parity problems. If ρ and $\bar{\rho}$ are even, then we define $\delta = \alpha\rho/2$ and we have $\bar{\rho}/2 = n/\delta\alpha$. If $\bar{\rho}$ is odd, we choose $\delta = \alpha\rho/4$ which is an integer. Finally, we have $\omega = \omega(\delta)$ and $\alpha = \alpha(\delta)$.

3.4 Combinatorics with N odd. According to Proposition 3, our problem is to compute the number $X_\delta = \left|\bigcup_{p|\alpha}\left(\bigcup_{\delta'/\alpha(\delta') = \alpha/p} P_{\delta',\alpha} \cap P_\delta\right)\right|$ for a given δ such that $\alpha(\delta) = \alpha$. In the following, we shall note ω for $\omega(\delta)$. If in the above expression, $P_{\delta',\alpha} \cap P_\delta \neq \emptyset$, then we know that $\omega(\delta') \equiv \omega \ (\operatorname{mod} N/\alpha^2)$ and $\omega(\delta')^2 \equiv 1 \ (\operatorname{mod} Np^2/\alpha^2)$. Proposition 4 tells us that given $\omega' \in G_{\alpha/p}$ there exists a unique δ' such that $\omega(\delta') \equiv \omega' \ (\operatorname{mod} Np^2/\alpha^2)$, $\alpha(\delta') = \alpha/p$. Therefore, we are led to solve the following equations:

$$\omega'^2 \equiv 1 \ (\operatorname{mod} Np^2/\alpha^2), \quad \omega' \equiv \omega \ (\operatorname{mod} N/\alpha^2). \tag{13}$$

Moreover, according to Lemma 3, we only care for solutions $\omega' \operatorname{mod} Np/\alpha^2$. Let us fix a representative of ω in **Z** and introduce $\omega^2 - 1 = Nr/\alpha^2$, then we obtain:

$$\frac{N}{\alpha^2}x^2 + 2\omega x + r \equiv 0 \ (\operatorname{mod} p^2), \tag{14}$$

where $\omega' = \omega + xN/\alpha^2$ and x is defined $\operatorname{mod} p^2$. We must analyze two cases separately.

p divides N/α^2. Then, the reduction of this equation $\operatorname{mod} p$ has a unique solution x_0 because it is a regular first degree equation. Any solution of (14) is of the form $x = x_0 + py$, where $y \in \mathbf{Z}/p\mathbf{Z}$; and we have:

$$2\omega y + \frac{1}{p}\left(\frac{N}{\alpha^2}x_0^2 + 2\omega x_0 + r\right) \equiv 0 \quad (\operatorname{mod} p).$$

Finally (14) has exactly one solution $\operatorname{mod} p^2$.

p does not divide N/α^2. The reduction $\operatorname{mod} p$ of Eq. (14) is a second degree equation and as **Z**/p**Z** is a finite field, we can solve it by usual techniques. Let us note $(N/\alpha^2)^{-1}$ the inverse of N/α^2 in $(\mathbf{Z}/p\mathbf{Z})^*$; then the solutions are:

$$x'_\pm = (N/\alpha^2)^{-1}(-\omega \pm 1).$$

Any solution of (14) is of the form $x = x'_{\pm} + y \pm p$ with y defined mod p. We obtain the following equation for y:

$$\pm 2y_{\pm} + \frac{1}{p}\left(\frac{N}{\alpha^2}x_{\pm}^2 + 2\omega x_{\pm} + r\right) \equiv 0 \pmod{p}.$$

Equation (14) thus exactly admits two solutions mod p^2 which are already different mod p.

All this shows that:

$$\text{If} \quad p \left| \frac{N}{\alpha^2}, \right. \quad \bigcup_{\alpha(\delta') = \alpha/p} (P_{\delta} \cap P_{\delta',\alpha}) = P_{\delta_0,\alpha}, \tag{15}$$

$$\text{If} \quad p \not\left| \frac{N}{\alpha^2}, \right. \quad \bigcup_{\alpha(\delta') = \alpha/p} (P_{\delta} \cap P_{\delta',\alpha}) = P_{\delta'_{+},\alpha} \cup P_{\delta'_{-},\alpha} \tag{16}$$

and: $P_{\delta'_{+},\alpha} \cap P_{\delta'_{-},\alpha} = \emptyset$ because $\omega'_{+} \neq \omega'_{-} \pmod{pN/\alpha^2}$.

Let $\alpha = \prod_{j=1,\ldots,k} p_j^{\alpha_j}$ be the decomposition of α into prime factors. We introduce $\varepsilon_j = 0$ if $p_j | (N/\alpha^2)$ and $\varepsilon_j = \pm$ if $p_j \not| (N/\alpha^2)$ and $P_{j,\varepsilon_j} = P_{\delta'_{j,\varepsilon_j},\alpha}$. Then we have:

$$\left| \bigcup_{j=1}^{k} \left(\bigcup_{\varepsilon_j} P_{j,\varepsilon_j} \right) \right| = \sum_{l=1}^{k} (-1)^{l+1} \sum_{1 \leqq j_1 < \cdots < j_l \leqq k} \left| \bigcap_{m=1}^{l} \left(\bigcup_{\varepsilon_{j_m}} P_{jm,\varepsilon_{j_m}} \right) \right|.$$

But:

$$\left| \bigcap_{m=1}^{l} \left(\bigcup_{\varepsilon_{j_m}} P_{jm,\varepsilon_{j_m}} \right) \right| = \left| \bigcup_{[\varepsilon_j]} \left(\bigcap_{m=1}^{l} P_{j_m,\varepsilon_{j_m}} \right) \right| = \sum_{[\varepsilon_j]} \left| \left(\bigcap_{m=1}^{l} P_{j_m,\varepsilon_{j_m}} \right) \right|$$

because $P_{j,\varepsilon}$'s for fixed j and different ε's are disjoint. We have to find $\left| \bigcap_{m=1}^{l} (P_{j_m,\varepsilon_{j_m}}) \right|$. The elements of the set considered here are trivially in one-to-one correspondence with solutions of the following linear system:

$$\forall (r,s) \in \langle 1, l \rangle^2; \quad \frac{N}{\alpha}(p_{j_r}\xi_{j_r} - p_{j_s}\xi_{j_s}) + \alpha(\omega(\delta'_{jr,\varepsilon_{jr}}) - \omega(\delta'_{j_s}, \varepsilon_{j_s})) \equiv 0 \pmod{N}$$

with $\xi_j \in \mathbf{Z}/(\alpha/p_j)\mathbf{Z}$. This system is equivalent to:

$$\forall m \in \langle 1, l-1 \rangle^2; \quad \frac{N}{\alpha}(p_{j_m}\xi_{j_m} - p_{j_{m+1}}\xi_{j_{m+1}}) + \alpha(\omega(\delta'_{j_m,\varepsilon_{j_m}}) - \omega(\delta'_{j_m+1,\varepsilon_{j_m}})) \equiv 0 \pmod{N} \tag{17}$$

Let us consider the following morphism of groups:

$$\psi: \prod_{m=1}^{l} \left(\frac{\mathbf{Z}}{(\alpha/p_{j_m})\mathbf{Z}} \right) \rightarrow \left(\frac{\mathbf{Z}}{\alpha\mathbf{Z}} \right)^{l-1},$$

$$(\xi_{j_m})_{m \in \langle 1,l \rangle} \mapsto (p_{j_m}\xi_{j_m} - p_{j_{m+1}}\xi_{j_{m+1}})_{m \in \langle 1,l-1 \rangle}.$$

Thanks to Bezout's theorem, this morphism is surjective and its kernel can easily be found:

$$\ker \psi \simeq \frac{\mathbf{Z}}{\frac{\alpha}{\prod_{m=1}^{l} p_{j_m}}\mathbf{Z}}.$$

This shows that the system (17) has exactly $\alpha \Big/ \prod_{m=1}^{l} p_{j_m}$ solutions. Then we have:

$$X_\delta = \sum_{l=1}^{k} (-1)^{l+1} \sum_{1 \leqq j_1 < \cdots < j_l \leqq k} \left(\sum_{[\varepsilon_{j_m}]} \frac{\alpha}{\prod_{m=1}^{l} p_{j_m}} \right).$$

But we are interested in $N_\delta = \alpha - X_\delta$. If we introduce θ_j the number of values taken by ε_j, we can rewrite N_δ under the amusing form:

$$N_\delta = \frac{\alpha}{\prod_{j=1}^{k} p_j} \prod_{j=1}^{k} (p_j - \theta_j).$$

We have seen that $\theta_j = 1$ or 2, thus N_δ is a strictly positive integer. Consequently, we know that there exists at least one element of P_δ which does not belong to any $P_{\delta'}$ for δ' such that $\alpha(\delta')$ is a strict divisor of $\alpha(\delta)$. Therefore in row $\alpha = \alpha(\delta)$ appears at least one isolated c_δ coefficient which by integrality and positivity is a non-negative integer. The unicity of the vacuum forces any physical modular invariant partition function to be of the following form (which is already a solution of our problem):

$$Z(\tau) = \sum_{(\lambda,\bar{\lambda}) \in (\mathbf{Z}/N\mathbf{Z})^2} \Omega^{(\delta)}_{\lambda,\bar{\lambda}} \chi_\lambda(\tau) \overline{\chi_{\bar{\lambda}}(\tau)}.$$

Therefore, Theorem 5 is proved in this case.

3.5 Combinatorics for N even. In this subsection, we shall consider the case where N is even using the same strategy than in Subsect. 3.4. However, as we shall see, the discussion is slightly different and the case n/α^2 odd will be discussed in 3.6. In this case; we know that the set G_α for $\alpha^2 | n$ is defined by

$$G_\alpha = \{\omega \in \mathbf{Z}/(N/\alpha^2)\mathbf{Z}/\omega^2 \equiv 1 \pmod{2N/\alpha^2}\}.$$

For this reason, in order to find all divisors δ' of n such that $P_{\delta',\alpha} \subset P_\delta$, $\alpha(\delta') = \alpha/p$, where δ is a fixed divisor of n and p is a prime divisor of α, we are led to the following equation:

$$\frac{N}{\alpha^2} x^2 + 2\omega x + 2s \equiv 0 \pmod{2p^2}, \quad x \in \frac{\mathbf{Z}}{p^2\mathbf{Z}}, \tag{18}$$

where $\omega^2 - 1 = 2Ns/\alpha^2$. We obtain this exactly as in Subsect. 3.4 by writing that $\omega' = \omega + xN/\alpha^2$ and writing down explicitly the condition $\omega' \in G_{\alpha/p}$. By the different results proved before, we thus define a unique divisor δ' of n such that $\alpha(\delta') = \alpha/p$;

$\omega(\delta')=\omega'$. Equation (18) can be rewritten in the form:

$$\frac{n}{\alpha^2}x^2+\omega x+s\equiv 0 \pmod{p^2}. \tag{19}$$

We first consider the case: $p\neq 2$. The preceding discussion can be adapted without any surprise and we find that:

$$\text{If}\quad p|N/\alpha^2;\quad \bigcup_{\alpha(\delta')=\alpha/p}(P_{\delta',\alpha}\cap P_\delta)=P_{\delta'_0,\alpha}, \tag{20}$$

$$\text{If}\quad p\not|N/\alpha^2;\quad \bigcup_{\alpha(\delta')=\alpha/p}(P_{\delta',\alpha}\cap P_\delta)=P_{\delta'_+,\alpha}\cup P_{\delta'_-,\alpha}, \tag{21}$$

because Eq. (19) has precisely one (respectively two) solutions mod p^2.

When $p=2$; things are slightly more subtle. Let us reduce Eq. (19) mod 2; we find:

$$\left(\frac{n}{\alpha^2}+1\right)x+s\equiv 0 \pmod 2,$$

where we have used $\omega\equiv 1 \pmod 2$, $x^2\equiv x \pmod 2$.

This equation has exactly one solution when n/α^2 is even and in this case, we can lift it back to a unique solution mod 4. This case is therefore not a problem.

On the other hand, the case n/α^2 odd is at the heart of the trouble. This can only occur when $n=2^{2t}m, t\in\mathbf{Z}, m$ even, and for δ such that δ/α, $n/\delta\alpha$ are odd. This implies that, given two integers a,b such that $an/\delta\alpha-b\delta/\alpha=1, a\equiv b+1 \pmod 2$. But $\omega^2=1-4abn/\alpha^2$ and therefore $s\equiv 0 \pmod 2$. Consequently, Eq. (19) has two solutions mod 2 and the reader will check that it has exactly two solutions mod 4. This shows the existence of two divisors δ'_+ and δ'_- of n that satisfy $P_{\delta',\alpha}\subset P_\delta$, $\alpha(\delta')=\alpha/2$, and again $P_{\delta'_+,\alpha}\cap P_{\delta'_-,\alpha}=\emptyset$.

If, as in Subsect. 3.4, we compute the number of elements in the set

$$P_\delta\setminus\bigcup_{\substack{\alpha(\delta')|\alpha\\ \alpha(\delta')\neq\alpha}}(P_{\delta',\alpha}\cap P_\delta)),$$

we find:

$$\frac{\alpha}{\prod_{p|\alpha}p}\prod_{p|\alpha}(p-\theta_p), \tag{22}$$

which is a positive integer but is strictly positive only when $n/\alpha(\delta)^2$ is even. We arrive at the following result:

Partial Theorem 5. *Let δ be any divisor of n such that n/α^2 is even then if $\sum c_\delta\Omega(\delta)$ has only positive integer entries then:*

$$c_\delta\in\mathbf{N}.$$

3.6 End of the Proof for N even, n/α^2 odd. Ler us have a closer look at the case n/α^2 odd. In this case, it is clear that:

$$P_\delta=P_{\delta'_+,\alpha}\cup P_{\delta'_-,\alpha},\quad P_{\delta'_+,\alpha}\cap P_{\delta'_-,\alpha}=\emptyset.$$

We would like to prove that in row α, there exist entries of the form $c_\delta + c_{\delta'_+}$ and $c_\delta + c_{\delta'_-}$. For this purpose, we shall compute:

$$\left| P_{\delta'_+,\alpha} \setminus \left(\bigcup_{\substack{\delta'',\alpha(\delta'')|\alpha \\ \alpha(\delta'')\neq\alpha,\alpha/2}} P_{\delta'',\alpha} \right) \right|.$$

Consider any δ'' such that $\alpha(\delta'')|\alpha$ and $\alpha(\delta'') \neq \alpha, \alpha/2$, then either there exists $p \neq 2$ a prime divisor of α and $\alpha(\delta'')|(\alpha/p)$, or $\alpha(\delta'') = \alpha/2^k$ with a suitable k.

We consider directly the most complicated case where $\alpha/2$ is even. In this case, we look for all divisors δ'' verifying:

$$\alpha(\delta'') = \alpha/4, \quad P_{\delta'',\alpha} \subset P_{\delta'_+,\alpha}$$

because we can check that $P_{\delta'',\alpha} \subset P_{\delta'_+}$ or $P_{\delta'',\alpha} \subset P_{\delta'_-}$. This is equivalent to search all ω'' mod $32n/\alpha^2$ which satisfy

$$\omega' \equiv \omega'_+ \pmod{8n/\alpha^2}, \quad \omega'^2 \equiv 1 \pmod{64n/\alpha^2},$$

and we are only interested in solutions ω'' mod $32n/\alpha^2$. It is easy to check that we obtain a regular first degree equation in x where $\omega'' = \omega'_+ + 8nx/\alpha^2$. Thus there exists a unique δ'' with $\alpha(\delta'') = \alpha/4$ and $P_{\delta'',\alpha} \subset P_{\delta'_+}$. We shall now compute

$$\left| P_{\delta'_+,\alpha} \setminus \left(\bigcup_{\substack{p|\alpha \\ p\neq 2}} \bigcup_{\varepsilon_p} (P_{\delta'_+,\alpha} \cap P_{\delta_{p,\varepsilon_p},\alpha}) \right) \right|.$$

The usual technique gives us:

$$\frac{\alpha}{\prod_{p|\alpha} p} \prod_{\substack{p|\alpha \\ p\neq 2}} (p - \theta_p). \tag{23}$$

In the same way, we compute

$$\left| P_{\delta'',\alpha} \setminus \bigcup_{\substack{p|\alpha \\ p\neq 2}} \bigcup_{\varepsilon_p} (P_{\delta_{p,\varepsilon_p},\alpha} \cap P_{\delta'',\alpha}) \right|.$$

We have found:

$$\frac{\alpha}{2\prod_{p|\alpha} p} \prod_{\substack{p|\alpha \\ p\neq 2}} (p - \theta_p) \tag{24}$$

and, with:

$$\left| P_{\delta'_+,\alpha} \setminus \left(P_{\delta'',\alpha} \cup \left(\bigcup_{\substack{p|\alpha \\ p\neq 2}} \bigcup_{\varepsilon_p} (P_{\delta'_+,\alpha} \cap P_{\delta_{p,\varepsilon_p},\alpha}) \right) \right) \right| = \left| P_{\delta'_+,\alpha} \setminus \left(\bigcup_{\substack{p|\alpha \\ p\neq 2}} \bigcup_{\varepsilon_p} (P_{\delta'_+,\alpha} \cap P_{\delta_{p,\varepsilon_p},\alpha}) \right) \right|$$
$$- \left| P_{\delta'',\alpha} \setminus \bigcup_{\substack{p|\alpha \\ p\neq 2}} \bigcup_{\varepsilon_p} (P_{\delta_{p,\varepsilon_p},\alpha} \cap P_{\delta'',\alpha}) \right|,$$

we find using expressions (23) and (24):

$$\left|P_{\delta'_+,\alpha}\setminus\left(P_{\delta'',\alpha}\cup\left(\bigcup_{p|\alpha,p\neq 2}\ \bigcup_{\varepsilon_p}(P_{\delta'_+,\alpha}\cap P_{\delta_{p,\varepsilon_p},\alpha})\right)\right)\right|=\frac{\alpha}{2\prod\limits_{p|\alpha}p}\prod_{p|\alpha,p\neq 2}(p-\theta_p). \tag{25}$$

This is a strictly positive integer.

The proof can be adapted in the case $\alpha/2$ is odd. It is even simpler because for any divisor satisfying $\alpha(\delta')|\alpha$ and $\alpha(\delta')\neq\alpha,\alpha/2$, there exists some odd prime divisor of α divising $\alpha(\delta')$. Consequently, we only have to compute:

$$\left|P_{\delta'_+,\alpha}\setminus\left(\bigcup_{\substack{p|\alpha\\ p\neq 2}}\ \bigcup_{\varepsilon_p}(P_{\delta'_+,\alpha}\cap P_{\delta_{p,\varepsilon_p},\alpha})\right)\right|=\frac{\alpha}{\prod\limits_{p|\alpha}p}\prod_{\substack{p|\alpha\\ p\neq 2}}(p-\theta_p), \tag{26}$$

and this is again a strictly positive integer. We have therefore proved the following lemma:

Lemma 5. *If δ verifies $n/\alpha(\delta)^2$ odd; then there exist two divisors $\delta'_\pm$ with*

$$\alpha(\delta'_\pm)=\alpha(\delta)/2,\quad c_\delta+c_{\delta'_\pm} \textit{ are matrix elements of } \sum c_\delta\Omega^{(\delta)}.$$

Let us now conclude our study of the case N even.

Lemma 5 states that we can associate with any δ such that $n/\alpha(\delta)^2$ is odd, two divisors $\delta'_\pm$ where $c_\delta+c_{\delta'_\pm}$ are positive integers and by partial theorem 5, $c_\pm$ are non-negative integers. Moreover, two different δ's will give different $\delta'_\pm$.

We thus introduce:

$$A=\left\{\delta\Big/\frac{n}{\alpha(\delta)^2}\equiv 1\ (\mathrm{mod}\,2)\right\},\quad B=\{\delta/\delta|n\}\setminus\bigcup_{\delta\in A}\{\delta,\delta'_+,\delta'_-\}.$$

We remark that we can rewrite

$$\begin{aligned}\sum_{\delta|n}c_\delta&=\sum_{\delta\in B}c_\delta+\sum_{\delta\in A}(c_\delta+c_{\delta'_+})+c_{\delta'_-}\\ &=\sum_{\delta\in B}c_\delta+\sum_{\delta\in A}(c_\delta+c_{\delta'_-})+c_{\delta'_+},\end{aligned} \tag{27}$$

where all terms are positive integers.

Case 1. $\exists\delta''\in B,\ c_{\delta''}\neq 0$. In this case, we have by Lemma 5:

$$\forall\delta\in A,\quad c_{\delta'_\pm}=c_\delta+c_{\delta'_\pm}=0,$$

and by partial theorem 5:

$$\forall\delta\in B\setminus\{\delta''\},\quad c_\delta=0.$$

Therefore, the $\hat{N}$ matrix is one of the $\Omega^{(\delta)}$ and clearly satisfies positivity, integrality and vacuum unicity requirements. This gives the desired result.

Case 2. $\forall\delta\in B,\ c_\delta=0$. Then, there exists a unique δ_0 in A such that $c_{\delta_0}+c_{\delta'_{0,+}}+c_{\delta'_{0,-}}=1$ and

$$\forall\delta\neq\delta_0,\quad c_\delta=c_{\delta'_+}=c_{\delta'_-}=0.$$

We therefore have three possibilities:

$$\begin{aligned} c_{\delta_0} &= 1, & c_{\delta'_{0,+}} &= 0, & c_{\delta'_{0,-}} &= 0,\\ c_{\delta_0} &= -1, & c_{\delta'_{0,+}} &= 1, & c_{\delta'_{0,-}} &= 0,\\ c_{\delta_0} &= -1, & c_{\delta'_{0,+}} &= 0, & c_{\delta'_{0,-}} &= 1, \end{aligned}$$

but the last two cases are eliminated because $\hat{N}_{0,N/\alpha} = -1$. Just like before, we find that the $\hat{N}$ matrix is one of the $\Omega^{(\delta)}$.

We have thus proved Theorem 5.

4. Some Amusing Properties of Z/NZ Partition Functions

4.1 Modular Invariants and Automorphisms of the Fusion Rules. Recently, Dijkgraaf and Verlinde have shown that for any modular invariant partition function of the form [14]:

$$Z = \sum_{i\in I} \chi_i \overline{\chi_{\Sigma(i)}},$$

where $(\chi_i)_{i\in I}$ is a set of characters of an extended algebra and Σ is a bijection of I, Σ is an automorphism of the fusion rules (id est Σ verifies: $N^k_{i,j} = N^{\Sigma(k)}_{\Sigma(i),\Sigma(j)}$, $\Sigma(\mathbf{1}) = \mathbf{1}$, $\widehat{\Sigma(i)} = \Sigma(\hat{\imath})$), and $h_i - h_{\Sigma(i)} \in \mathbf{Z}$ and $\tilde{\Sigma}\Sigma = \mathbf{1}$ to ensure modular invariance under T (respectively S). In our case the automorphisms of the fusion rules are precisely automorphisms of the additive group $\mathbf{Z}/N\mathbf{Z}$. These are indexed by u invertible mod N and map x to ux. The condition $h_i - h_{\Sigma(i)} \in \mathbf{Z}$ is equivalent to $u^2 = 1 \pmod{2N}$ if N is even and $u^2 = 1 \pmod N$ if N is odd. The partition function associated with such an automorphism must be:

$$Z = \sum_{\lambda=0}^{N-1} \chi_\lambda \overline{\chi_{u\lambda}}.$$

Given u fulfilling the conditions above, we can find a unique δ divisor of n such that $\alpha(\delta) = 1$, $\omega(\delta) = u$ and therefore:

$$Z_\delta = \sum_{(\lambda,\bar{\lambda})\in(\mathbf{Z}/n\mathbf{Z})^2} \delta_{\lambda,u\bar{\lambda}} \chi_\lambda \overline{\chi_{\bar{\lambda}}} = \sum_{(\lambda,\bar{\lambda})\in(\mathbf{Z}/n\mathbf{Z})^2} \Omega^{(\delta)}_{\lambda,\bar{\lambda}} \chi_\lambda \overline{\chi_{\bar{\lambda}}}.$$

This partition function is modular invariant. This shows the converse of Dijkgraaf–Verlinde's theorem in this particular context, namely $\omega(\delta)$ defines the automorphism of the fusion algebra.

4.2 Extended Diagonal Z/NZ Theories. Some other interesting objects are the extended diagonal modular invariants. These invariants can be written as a sum of squared moduli of sums of characters. A very natural idea is to consider these sums of characters as characters of an extended algebra. Then, it is interesting to find the fusion rules of this algebra. In our example, the most general invariant can be written as:

$$Z = \sum_{k\in\mathbf{Z}/(N/\alpha(\delta))\mathbf{Z}} \sum_{\xi\in\mathbf{Z}/\alpha(\delta)\mathbf{Z}} \chi_{k\alpha(\delta)} \bar{\chi}_{k\alpha(\delta)\omega(\delta)+\xi N/\alpha},$$

and if this is a sum of moduli squared, for any $k \bmod N/\alpha$, there will exist $\xi \bmod \alpha$ such that:

$$k(1-\omega(\delta)) \equiv \frac{N}{\alpha^2}\xi \quad (\operatorname{mod} N/\alpha).$$

Therefore, using the definition of $\omega(\delta)$, it is easy to show that $n/\delta\alpha = 1$ and hence that $\omega(\delta) = 1$. Let us find the divisors δ of n such that $n/\delta\alpha = 1$, we see that $\alpha = n/\delta$ is equivalent to $(n/\delta)|\delta$, i.e. $n|\delta^2$ ($\delta = n$ for example, corresponds to the diagonal invariant). Conversely, if this condition is fulfilled, then $\omega(\delta) = 1$. Then, we have:

$$\left| \sum_{\xi\in\mathbf{Z}/\alpha(\delta)\mathbf{Z}} \chi_{\alpha(\delta)k+N\xi/\alpha(\delta)} \right|^2 = \sum_{\xi\in\mathbf{Z}/\alpha(\delta)\mathbf{Z}} \sum_{\xi'\in\mathbf{Z}/\alpha(\delta)\mathbf{Z}} \chi_{\alpha(k+N\xi/\alpha(\delta)^2)} \bar{\chi}_{\alpha(\delta)(k+N\xi/\alpha(\delta)^2)+N\xi'/\alpha(\delta)}.$$

Finally, we obtain with n/δ standing for α:

$$\sum_{k\in\mathbf{Z}/(\delta^2N/n^2)\mathbf{Z}} \left| \sum_{\xi\in\mathbf{Z}/(n/\delta)\mathbf{Z}} \chi_{nk/\delta+N\delta\xi/n} \right|^2 = \sum_{(\lambda,\bar{\lambda})\in(\mathbf{Z}/N\mathbf{Z})^2} \Omega^{(\delta)}_{\lambda,\bar{\lambda}} \chi_\lambda \overline{\chi_{\bar{\lambda}}}.$$

The extended diagonal theories are associated with divisor such that $n|\alpha^2$. The extended characters are given by:

$$\tilde{\chi}_k = \sum_{\xi\in\mathbf{Z}/(n/\delta)\mathbf{Z}} \chi_{nk/\delta+N\delta\xi/n},$$

where k is defined $\operatorname{mod} \delta^2N/n^2$. An easy computation gives us the S matrix for these characters and we find:

$$S_{k,l} = \frac{1}{\sqrt{N'}} \exp\left(2\pi i \frac{akl}{N'}\right); \quad N' = N\delta^2/n^2. \tag{28}$$

This is exactly a finite Fourier transform of the type considered in 3.1. Notice that a and $N\delta/n^2$ are coprime. This phenomenon expands to any Z_δ. Let us write:

$$\begin{aligned} Z_\delta &= \sum_{\substack{k\in\mathbf{Z}/(N/\alpha)\mathbf{Z} \\ \xi\in\mathbf{Z}/\alpha\mathbf{Z}}} \chi_{k\alpha} \bar{\chi}_{k\alpha\omega+(N/\alpha)\xi} \\ &= \sum_{k\in\mathbf{Z}/(N/\alpha^2)\mathbf{Z}} \sum_{(\xi_1,\xi_2)\in(\mathbf{Z}/\alpha\mathbf{Z})^2} \chi_{k\alpha+\xi_1(N/\alpha)} \bar{\chi}_{k\omega\alpha+\xi_2N/\alpha}. \end{aligned}$$

If we introduce for $k\in\mathbf{Z}/(N/\alpha^2)\mathbf{Z}$,

$$\tilde{\chi}_k = \sum_{\xi\in\mathbf{Z}/(N/\alpha)\mathbf{Z}} \chi_{k\alpha+\xi N/\alpha},$$

then

$$Z_\delta = \sum_{k\in\mathbf{Z}/(N/\alpha^2)\mathbf{Z}} \tilde{\chi}_k \overline{\tilde{\chi}_{k\omega}}$$

with $\omega^2 \equiv 1$ (mod $2N/\alpha^2$) when N is even and $\omega^2 \equiv 1$ (mod N/α^2) when N is odd. Then, there exists δ' divisor of N/α^2 such that $\alpha(\delta') = 1$ and $\omega(\delta') = \omega$, thus showing that Z_δ is of the type considered in Subsect. 4.1. The $\tilde{\chi}_k$'s are the characters with respect to the maximally extended chiral algebra of the model. The reader will easily check that the S matrix of those $\tilde{\chi}_k$'s is given by (30) with $N' = N/\alpha^2$. In fact, there is a kind of stability of the fusion rules in this case which was not present for example in the $A_1^{(1)}$ case.

Finally, we can rewrite the partition function of the rational Gaussian model considered in Subsect. 2.2 in the form of a Z_δ. Let us consider the case of a free boson compactified on a circle of radius R with $R^2/2 = p/q$, we define:

$$Q_k(z) = \exp(ikb\sqrt{2pq}X(z)).$$

These operators define a subalgebra of the maximally extended chiral algebra of the theory. We can organize the Hilbert space of the model with respect to the representation theory of this algebra. In our case, the theory is still rational. The characters of the irreducible representations are indexed by an integer n mod $2pqb^2$ and are given by:

$$\tilde{\chi}_n = \frac{1}{\eta(\tau)} \sum_{l \in \mathbf{Z}} q^{(n+2b^2pql)^2/4b^2pq}.$$

The partition function of the rational Gaussian model is given by:

$$Z_{p,q} = \frac{1}{|\eta(\tau)|^2} \sum_{(n,m) \in \mathbf{Z}^2} q^{(pn+qm)^2/4pq} \bar{q}^{(pn+qm)^2/4pq},$$

which can easily be rewritten as:

$$Z_{p,q} = \sum_{\substack{k \in \mathbf{Z}/2pqb^2\mathbf{Z} \\ l \in \mathbf{Z}/b\mathbf{Z}}} \tilde{\chi}_{kb} \overline{\tilde{\chi}_{\omega kb + 2pqlb}},$$

where ω is defined as in (12) with $N = 2pq$ and $\delta = p$. Therefore, there exists a unique δ divisor of $2pqb^2$ such that $\alpha(\delta) = b$ and $\omega(\delta) = \omega$. This shows that $Z_{p,q}$ can be rewritten as a Z_δ. When one takes $b = 1$, i.e. when one considers the maximally extended chiral algebra of the theory, the partition function is of the type considered in Subsect. 4.1 as was shown in [4] in full generality and just above in our cases.

4.3 An Amusing Identity. In a recent work [7], C. Itzykson has shown that the $\mathbf{Z}/N\mathbf{Z}$ fusion rules are realized in terms of $A_N^{(1)}$ level 1 theories. In this case, the parameter a was $N - 1$. The rational gaussian model provides a realisation of these fusion rules for N even and $a = 1$. Thus, our study of modular invariants classifies all modular invariant partition functions of rational gaussian models and of $A_N^{(1)}$ level 1 models. Notice that as soon as N is a square there exists a unique partition function which is a modulus squared. C. Itzykson showed how to recover the cubic root of the modular form $j(\tau)$ from the $N = 9$, $\delta = 3$ invariant [7], the reader can also easily check using $SU(25)$ level 1 invariants that:

$$\sum_{k=0}^{5} \chi_{5k}(\tau) = j(\tau) - 120. \tag{29}$$

5. Conclusion

Finally, we have completely determined the modular properties of the characters and the modular invariants in the case where G is a cyclic group. This case gives an illustration of the general facts we mentioned in Sect. 1, namely that given a particular fusion algebra, the different possibilities for the S matrix are labelled by permutations σ of the fields which define automorphisms satisfying $S^j_{\sigma(i)} = S_i^{\sigma(j)}$ of the fusion algebra. Concerning the modular properties, we have obtained some partial information in the case of an arbitrary abelian group. There remains to solve explicitly the equivalence problem mentioned in Sect. 1 and find all modular invariants in the general case. Another interesting problem is the study of the case where G is not abelian. In this case the symmetry of S implies some constraint on the group G.

However, it seems much more important to address the reconstruction problem. In our approach, we determine different properties of the RCFT from its fusion rules but it is not clear when there is really a conformal theory with these properties. For example, we can construct some finite dimensional representations of $SL_2(\mathbf{Z})$ using this method but it is not clear that these representations can be realized using characters, i.e. functions with only positive integers in their q-development. Furthermore one has to find the chiral algebra the representation theory of which would give us these functions as characters.

A. Gaussian Sums

Here, we recall how to compute some special sums known as Gaussian sums [15]. Let us define:

$$S_N(a) = \frac{1}{\sqrt{N}} \sum_{k \in \mathbf{Z}/N\mathbf{Z}} \exp\left(2\pi i \frac{ak^2}{N}\right).$$

We restrict ourselves to a invertible mod N; the other cases can trivially be reduced to this case. We refer the reader to the literature for details and proofs. We can first of all restrict the computation to the case where N is a power of a prime.

Proposition A.1. *Let a, b, c three integers with no common divisor. Then $S_{ab}(c) = S_a(bc)S_b(ac)$.*

We are reduced to computing $S_{p^\alpha}(a)$, where a and p are coprime. This can be achieved quite easily when p is odd, only $p = 2$ is more tricky. We only give the final results:

Proposition A.2. *Let p be an odd prime number and a an invertible* mod p, *then*:

$$S_{p^\alpha}(a) = \left(\frac{a}{p}\right) S_{p^\alpha}(1).$$

Proposition A.3. *Let a be an odd integer*; *then*:

$$S_{2^\alpha}(a) = \varepsilon(a)\left(\frac{-2^\alpha}{a}\right) S_{2^\alpha}(1),$$

where $\varepsilon(a) = 1$ (respectively i) when $a = 1$ (mod 4) *(respectively $a = -1$* (mod 4)) *and*

$$\left(\frac{x}{y}\right) = \prod_{\substack{p\,\text{prime}\\ p|y}} \left(\frac{x}{p}\right)$$

is the Jacobi symbol.

Finally,

Proposition A.4. *We have*:

$$S_N(1) = \frac{1+i}{2}(1 + (-i)^N).$$

With these results, one can compute all Gaussian sums quite easily. For example, we have:

$$S_{4n}(\pm 1) = 1 \pm i.$$

B. Quadratic Equations in $\mathbf{Z}/N\mathbf{Z}$

In this appendix, we shall discuss in more detail the structure of the quotient group:

$$\frac{U(\mathbf{Z}/N\mathbf{Z})}{U(\mathbf{Z}/N\mathbf{Z})^{(2)}}.$$

We first use the Chinese lemma. Let $N = \prod_{j=1}^{k} p_j^{\alpha_j}$ be the decomposition of N in prime factors; there exists an isomorphism of rings:

$$\varphi : \frac{\mathbf{Z}}{N\mathbf{Z}} \to \prod_{j=1}^{k} \frac{\mathbf{Z}}{p_j^{(\alpha_j)}\mathbf{Z}}$$

which associates with any integer mod N its reductions mod $p_j^{\alpha_j}$. If all reductions of an integer are squares, then it is clear that the integer itself is a square because φ is a ring morphism. Reciprocally, if an integer is a square, then its reductions are also squares using φ^{-1}. Consequently:

$$\frac{U(\mathbf{Z}/N\mathbf{Z})}{U(\mathbf{Z}/N\mathbf{Z})^{(2)}} \simeq \prod_{j=1}^{k} \frac{U(\mathbf{Z}/p_j^{\alpha_j}\mathbf{Z})}{U(\mathbf{Z}/p_j^{\alpha_j}\mathbf{Z})^{(2)}}. \tag{30}$$

Henceforth we are led to analyze the case where N is a power of a prime p. We shall distinguish two cases: $p = 2$, $p \neq 2$.

Case $N = p^\alpha$, $p \neq 2$:

We want to determine if equation $x^2 = a$ (where a is a parameter) has solutions in $\mathbf{Z}/p^\alpha\mathbf{Z}$. This trick is to reduce this equation mod p and then to lift back the solutions in $\mathbf{Z}/p^\alpha\mathbf{Z}$. Let us remark that if $y^2 \equiv a \pmod{p^\beta}$, then $(y + zp^\beta)^2 \equiv y^2 + 2zp^\beta \pmod{p^{\beta+1}}$. Henceforth, we can choose z such that $(y + zp^\alpha)^2 \equiv a \pmod{p^{\beta+1}}$. This shows that x is a square in $\mathbf{Z}/p^\alpha\mathbf{Z}$ if and only if it is a square in $\mathbf{Z}/p\mathbf{Z}$. The characterisation of the squares in the finite field $\mathbf{Z}/p\mathbf{Z}$ has been solved a long time ago. Let us recall a few facts about this: we define the Legendre symbol [12] by:

$$\left(\frac{m}{p}\right) = m^{(p-1)/2} \pmod{p}.$$

Then, we have the following short exact sequence:

$$1 \to (\mathbf{Z}/p\mathbf{Z}^*)^{(2)} \to \mathbf{Z}/p\mathbf{Z}^* \xrightarrow{(\frac{\cdot}{p})} \mathbf{Z}/2\mathbf{Z} \to 1,$$

where the second arrow is the canonical injection. In the case $N = p^\alpha$, we have:

$$U(\mathbf{Z}/p^\alpha\mathbf{Z})^{(2)} = \ker\varphi, \quad \varphi(x) = x^{(p-1)/2} \pmod{p},$$

and φ is a morphism from $U(\mathbf{Z}/p^\alpha\mathbf{Z})$ into $\mathbf{Z}/p\mathbf{Z}^*$. The image of this morphism is $\{-1, 1\}$. Therefore:

$$\frac{U(\mathbf{Z}/p^\alpha\mathbf{Z})}{U(\mathbf{Z}/p^\alpha\mathbf{Z})^{(2)}} \simeq \frac{\mathbf{Z}}{2\mathbf{Z}}. \tag{31}$$

Case $N = 2^\alpha$:

This case is slightly more subtle. For example, it is well known that

$$U(\mathbf{Z}/2\mathbf{Z}) = U(\mathbf{Z}/2\mathbf{Z})^{(2)} = \{1\}.$$

By inspection, one finds that:

$$\frac{U(\mathbf{Z}/4\mathbf{Z})}{U(\mathbf{Z}/4\mathbf{Z})^{(2)}} = \mathbf{Z}/2\mathbf{Z}, \tag{32}$$

and with a little more work:

$$\frac{U(\mathbf{Z}/8\mathbf{Z})}{U(\mathbf{Z}/8\mathbf{Z})^{(2)}} = (\mathbf{Z}/2\mathbf{Z})^2. \tag{33}$$

Let us now analyze the case $n = 2^\alpha$, $\alpha \geqq 4$. We have:

$$(x + 2^{\beta-1}z)^2 = x^2 + 2^{2(\beta-1)}z^2 + 2^\beta zx,$$

and consequently, if $x^2 \equiv a \pmod{2^\beta}$ with $\beta \geqq 3$; then there exists $z \in \mathbf{Z}$ such that $(x + 2^{\beta-1}z)^2 \equiv a \pmod{2^{\beta+1}}$. Finally, a is a square in $\mathbf{Z}/2^\alpha\mathbf{Z}$ if and only if it is a square in $\mathbf{Z}/8\mathbf{Z}$. This shows that:

$$\forall\alpha \geqq 4, \quad \alpha \in \mathbf{Z}; \quad \frac{U(\mathbf{Z}/2^\alpha\mathbf{Z})}{U(\mathbf{Z}/2^\alpha\mathbf{Z})^{(2)}} = (\mathbf{Z}/2\mathbf{Z})^2. \tag{34}$$

This concludes our study.

Acknowledgements. During this work, I benefited from many useful conversations with B. Julia. I also thank C. Itzykson for remarks on his work. The case of non-abelian groups has catalyzed exciting conversations between M. Bauer, Ph. Roche and myself. A. Dewisme, F. Digne, M. Finkelmann, P. Lescot, J. F. Mestre, J. Michel, and L. Puig gave me much useful information about Gaussian sums and finite group theory. Finally, some steps of the proof in Sect. 3 were checked numerically. I thank Th. Papadopoulo for his generous and useful help with these verifications.

References

1. Belavin, A. A., Polyakov, A. B., Zamolodchikov, A. B.: Infinite conformal symmetry in 2D field theory. Nucl. Phys. B. **241**, 333–380 (1984)

2. Vafa, C.: Towards classification of conformal field theories. Phys. Lett. B. **206**, 421–426 (1988)
3. Moore, G., Seiberg, N.: Polynomial equations for rational conformal field theories. Phys. Lett. **212**, 451–460 (1988)
4. Moore, G., Seiberg, N.: Naturality in conformal field theory. Preprint IASSNS-HEP 88/31
5. Moore, G., Seiberg, N.: Classical and quantum conformal field theory. Preprint IASSNS-HEP 88/35
6. Verlinde, E.: Fusion rules and modular transformations in 2D CFT's. Nucl. Phys. B (FS 22) **300**, 360–376 (1988)
7. Itzykson, C.: Level one Kac-Moody characters and modular invariance. Conformal Field Theories and related topics. Binetruy, P., Sorba, P., Stora, R., (eds), Nucl. Phys. B. (Proc. Suppl.) **5**, pp. 150–165 Amsterdam: North-Holland 1988
8. Cappelli, A., Itzykson, C., Zuber, J. B.: The ADE classification of $A_1^{(1)}$ and minimal conformal field theories. Commun. Math. Phys. **113**, 1–26 (1987)
9. Tsuchiya, A., Kanie, Y.: Vertex operators in CFT on PC_1 and monodromy representations of the braid group. Lett. Math. Phys. **13**, 303 (1987)
10. Frenkel, I., Lepowsky, J., Meurman, A.: Vertex operators and the Monster. New York: Academic Press (to appear)
11. Serre, J. P.: Représentation linéaire des groupes finis. Paris: Hermann 1968
12. Serre, J. P.: Cours d'arithmétique. Paris: PUF 1970
13. Gepner, D., Qiu, Z.: Modular invariant partition functions for parafermionic theories. Nucl. Phys. B. (FS 19) **285**, 423–453 (1987)
14. Dijkgraaf, R., Verlinde, E.: Modular invariance and the fusion algebra. Conformal Field Theories and related topics. Binetruy, P., Sorba, P., Stora, R., (eds). Nucl. Phys. B. (Proc. Suppl.) **5**, pp. 87–97 Amsterdam: North-Holland 1988
15. Lang, S.: Algebraic number theory. Reading, MA: Addison-Wesley 1970

Communicated by K. Gawedzki

Received February 28, 1989; in revised form June 20, 1989