Commun. Math. Phys. 145, 85–121 (1992)

Communications in Mathematical Physics

Complete Classification of Simple Current Modular Invariants for RCFT's with a Center $(\mathbf{Z}_p)^k$

B. Gato-Rivera★ and A. N. Schellekens

CERN, 1211 Geneva 23, Switzerland

Received May 29, 1991; in revised form September 15, 1991

Abstract. Simple currents have been used previously to construct various examples of modular invariant partition functions for given rational conformal field theories. In this paper we present for a large class of such theories (namely those with a center that decomposes into factors $\mathbf{Z}_p$, p prime) the *complete* set of modular invariants that can be obtained with simple currents. In addition to the fusion rule automorphisms classified previously for *any* center, this includes all possible left–right combinations of all possible extensions of the chiral algebra that can be obtained with simple currents, for all possible current–current monodromies. Formulas for the number of invariants of each kind are derived. Although the number of invariants in each of these subsets depends on the current–current monodromies, the total number of invariants depends rather surprisingly only on p and the number of $\mathbf{Z}_p$ factors.

1. Introduction

As part of the program to classify all rational conformal field theories (RCFT's) – which is difficult and still far from being completed – one would like to classify all modular invariant partition functions of a given conformal field theory. This too has turned out to be a very hard problem, which so far has been solved completely only for a few special cases. In addition to some "free" theories those include the $SU(2)$ Kac–Moody algebras at arbitrary level [1] and some coset theories based on them. Furthermore one can always solve the problem by explicit computation if the number of primary fields is not too large. So far such computations have not provided much insight into the general solution to the problem.

There is however a subclass of modular invariants that should be more manageable, namely the class of invariants that can be obtained with simple currents [2]

★ On leave of absence from "Instituto de Física Fundamental", Madrid (to be defined below). For example, in the special case of $SU(2)$ Kac–Moody algebras these invariants reproduce the so-called A- and D-series. For other Kac–Moody algebras, these invariants can also be written down rather easily, reproducing the results described in [3–7]. Although in the absence of a complete classification of all invariants we cannot be certain how many of them are covered by simple currents, experience suggests that simple currents can be used to produce most of them (though unfortunately in general not all). This is even more likely to be the case for tensor products of RCFT's, where the number of simple current invariants grows very rapidly with the number of factors. It is certainly true that nearly the entire literature on the construction of modular invariants yielding various kinds of string theories can be understood in terms of simple currents. For this reason we believe that it is important to try to achieve a complete classification of modular invariant partition functions that can be obtained with simple currents.

This classification becomes especially non-trivial if the center of the RCFT (the abelian group generated by the fusion of the simple currents) consists of several $\mathbf{Z}_N$ factors. Examples of such theories can easily be obtained by tensoring Kac–Moody algebras or coset theories, but there is no need to be specific. The advantage of simple currents is precisely that one can solve the problem for generic classes of RCFT's, without having to specify in detail their modular transformation matrices S and T.

A first step towards classification was made in [8], where all fusion rule automorphisms that can be obtained with simple currents in any RCFT were derived. The possibility of extending the chiral algebra was not considered in [8], and this is the main goal of the present paper. Combining the results of [8] with all possible extensions of the algebra we obtain a classification of *all* simple current invariants for generic RCFT's. So far we have only succeeded in completing this last step for those RCFT's that have a center $(\mathbf{Z}_p)^k$, p prime. Our results also apply when the center is a product of factors $\mathbf{Z}_{N_1} \times \cdots \times \mathbf{Z}_{N_k}$, as long as each N_i is a product of single primes. In that case one simply decomposes the center into factors $(\mathbf{Z}_p)^{N_p}$, and applies our construction to each factor separately. In the following we will therefore only consider centers $(\mathbf{Z}_p)^k$.

Let us begin by reviewing a few basic facts about simple currents. Simple currents are primary fields whose fusion rules with any other field yield only one term. For unitary theories these have the property that $S_{0J}/S_{00} = 1$ [9], whereas non-unitary theories may, in principle, have fields for which this quantity is -1, which also have simple current fusion rules. Although we will allow non-unitary RCFT's, we will not take into account such fields. Furthermore we discard currents that do not satisfy the condition $ph(J) \in \mathbf{Z}$, where $h(J)$ is the conformal weight of the current. (This condition can be violated only if $p = 2$, in which case $2h(J)$ can be half-integer. For example, $SU(2)_k$ has a simple current violating it if k is odd. Such currents cannot yield any new modular invariants [8].) The remaining simple currents generate under fusion a discrete group $\mathbf{Z}_{N_1} \times \cdots \times \mathbf{Z}_{N_k}$, which is called the effective center of the RCFT. The word "effective" (which we will omit in the following) refers to the omission of currents with $ph(J) \notin \mathbf{Z}$.

In addition to the group structure $(\mathbf{Z}_p)^k$ due to the fusion rules, the set of simple currents is characterized by the current–current monodromies. The monodromy of any field a with respect to a simple current J is called the charge of that field, and is given by $Q_J(a) = h(a) + h(J) - h(Ja)$. It is defined modulo integers. If one chooses a basis of k currents $J_1, \ldots, J_k$, the charges of any field with respect to this basis form a vector $\vec{Q}(a)$, with $Q_i(a) \equiv Q_{J_i}(a)$. The current–current monodromies are then completely given by a symmetric $k \times k$ matrix $R_{ij} = Q_i(J_j) = Q_j(J_i)$. Since all charges are multiples of $\frac{1}{p}$ it is convenient to define also a matrix $\tilde{r}_{ij} = pR_{ij}$, defined modulo p.

The conformal weights of the currents can be expressed in terms of a matrix r, whose diagonal elements are defined mod $2p$ and whose off-diagonal elements are defined mod p:

$$h([\vec{\alpha}]) = -\frac{1}{2p}\sum_{ij} \alpha_i r_{ij} \alpha_j. \tag{1.1}$$

Here the notation is as in [8]: $[\vec{\alpha}]$ denotes a current $J_1^{\alpha_1} \cdots J_k^{\alpha_k}$. The diagonal elements of r are even. This is a matter of choice if p is odd, and a consequence of the condition $2h(J) \in \mathbf{Z}$ if $p = 2$. The matrix r is closely related to $\tilde{r}$, namely $\tilde{r}_{ij} = r_{ij} \bmod p$. Thus r is equivalent to $\tilde{r}$ as far as monodromies are concerned, but only the matrix r yields the correct conformal weights. Hence we may drop $\tilde{r}$ from now on.

Although there appear to be $p^{(1/2)k(k+1)}$ possible choices for the symmetric matrix r, the actual number of distinct possibilities is much smaller, since we have the freedom to choose different current bases. For $p \neq 2$ the matrix can be diagonalized, and furthermore the entries on the diagonal can be simplified. For $p = 2$ there are also many simplifications. We will discuss this in Appendix B.

A RCFT has a finite number of genus-one characters $\mathcal{X}_a(\tau)$. They transform into each other under the basic one-loop modular transformations

$$S: \tau \to -\frac{1}{\tau},$$

$$T: \tau \to \tau + 1.$$

On the characters, these transformations are represented by matrices S_{ab} and T_{ab} satisfying the defining conditions for the modular group: $(ST)^3 = S^2 = C$, where C is the charge conjugation matrix.

In terms of characters $\mathcal{X}_a$ and $\mathcal{X}_b^*$ of the left-moving sector and the right-moving sector respectively, modular invariant partition functions have the form $\sum_{a,b} \mathcal{X}_a(\tau) M_{ab} \mathcal{X}_b^*(\bar{\tau})$. The * indicates that the left-moving and right-moving characters, regarded as functions of τ, may be different, as long as their modular transformation matrices S and T are the same (so that there is a diagonal invariant $M_{ab} = \delta_{ab}$).

In general, the matrix M must satisfy the following conditions:

1. **Integrality**: $M_{ab} \in \mathbf{Z}$.
2. **Positivity**: $M_{ab} \geq 0$.
3. **Non-degeneracy of the vacuum**: $M_{00} = 1$.
4. **Modular invariance**: $[M, S] = [M, T] = 0$.
5. **Closure**: If $M_{ab} \neq 0$ and $M_{cd} \neq 0$ there must be at least one $M_{ef} \neq 0$ so that the field e appears in the fusion of a and f in the fusion of b and d.

All of these requirements are clearly necessary for M to have a chance of representing a well-defined conformal field theory. The last condition ensures that in the operator product of two fields $\phi_{ab}(z,\bar{z})$ and $\phi_{cd}(z,\bar{z})$ there is at least one operator allowed to appear on the right-hand side.

Ultimately one would like to have a list of all matrices M satisfying these conditions for any conformal field theory. At present, the best we can do is to give a complete classification of modular invariants satisfying one more condition:

6. **Simple current invariant**: $M_{ab}=0$ if there is no simple current J with $a=Jb$.

Finally one has to check that S satisfies a certain regularity condition, needed to rule out certain pathological theories. Most of these pathologies are directly or indirectly related to the presence of fixed-point fields (fields f which satisfy $Jf=f$ for some simple current J). It is difficult to formulate conditions for the validity of our results that are not only sufficient, but also necessary. A rather simple sufficient condition, adopted in this paper is:

7. **Regularity**: For every allowed charge $\vec{Q}$ there should be a field a with charge $\vec{Q}$ that is not a fixed point of any simple current, and whose matrix elements S_{ac} are all non-zero, except for zeroes due to fixed points.

The latter qualification is necessary because $S_{ab}=0$ if there exists a simple current J with $Q_J(a)\neq 0$ and $Jb=b$ or vice-versa. Note that unlike all the foregoing ones, this condition is a restriction of the RCFT's we consider, and not a condition on the matrix M.

The regularity condition is used for several purposes. First of all it is needed to constrain the fusion rule automorphisms. The classification of fusion rule automorphisms of [8] is only valid if the action of such an automorphism on a field is completely determined by the charge of that field. Roughly speaking, there should not exist any sets of fields that "decouple," i.e. that are not sufficiently strongly linked by S to a complete set of charges in the rest of the theory. If the regularity condition holds the action of an automorphism on any field a is fully determined by its action on any set Φ, consisting of fields that are not fixed points and whose charges are linearly independent and span the complete set of allowed charges. Since the fields in Φ are not fixed points every distinct solution to the equations of [8] yields a distinct fusion rule automorphism on Φ, which in turn implies a unique and distinct fusion rule automorphism on the entire theory.

The regularity condition is also used to make sure that in theories with extended chiral algebras the fixed points are well-behaved. This means that a row (or column) of M_{ab} for a fixed-point field a can be obtained in the obvious way from that of a non-fixed point with the same charges: one simply "folds up" the latter row, adding the matrix elements of M in the identified columns. This is proved in Appendix D, to which we defer as much as possible all problems associated with fixed points.

For a given center and monodromy matrix r there are many different conformal field theories, most of which satisfy the regularity condition. We will sometimes refer to such theories as "generic" RCFT's. If the regularity condition is not satisfied this may have several consequences. Sometimes a theory satisfies a weaker form of regularity that is still sufficient. In other cases there are fewer invariants than our construction produces, since some generically distinct invariants become identical if their difference cannot manifest itself because certain charges appear only for fixed-point fields. There are also cases where our classification is incomplete, even though the extra modular invariants are rather unusual, and are unlikely to correspond to sensible conformal field theories. However, even if the regularity condition is *not* satisfied all matrices M in our classification yield valid one-loop modular invariant partition functions. Some classes of theories where the regularity condition is satisfied, as well as some exceptions, are discussed at the end of Appendix D.

In the next section we will discuss the possible extensions of the chiral algebra, and the possible left–right combinations in which these extensions can appear. In Sect. 3 we will apply the general results to theories with a center $(\mathbf{Z}_p)^2$. For any monodromy matrix r we compute all modular invariants M. Remarkably, the *total* number of invariants is always the same (equal to $2(p+1)$), independent of r, even though the individual solutions for M depend strongly on r (as well as on the value of p modulo 4). In Sect. 4 we show that this phenomenon generalizes to $(\mathbf{Z}_p)^k$ for any k. The total number of invariants is equal to $\prod_{i=0}^{k-1}(1+p^i)$, for any p and r. We prove this by explicit computation of the number of invariants of any type.

Appendix A summarizes some results on number theory that are used in Sects. 3 and 4. In Appendix B we show how to simplify the matrix r, and we classify all inequivalent possibilities. In Appendix C formulas for the number of currents of a given spin are derived for any r. Finally, in Appendix D we discuss some technical issues related to fixed points.

2. Integer Spin Invariants

In this section we will show how to construct modular invariant matrices with $M_{b0} \neq 0$ for at least one $b \neq 0$. Such matrices give rise to extensions of the left algebra (and, as we will see, also to extensions of the right algebra; in the following, left indices of M refer to the left-moving sector). We begin with a derivation of the possible extensions of the algebra and their representations. Then we discuss the possible left–right pairings of the representations if the left and right algebras are the same. In Subsect. 2.3 we discuss the possible left–right pairings of different extensions. The results in this section are valid for a center $(\mathbf{Z}_p)^k$, but some have a more general validity.

2.1. Algebras and Representations. Consider a matrix M satisfying all conditions described in the introduction. From the commutation relation $SM = MS$ we derive

$$\sum_{[\vec{\alpha}]} M_{a,[\vec{\alpha}]a} e^{2\pi i \vec{\alpha}\cdot\vec{Q}(c)} = \sum_{[\vec{\gamma}]} e^{2\pi i \vec{\gamma}\cdot\vec{Q}(a)} M_{[\vec{\gamma}]c,c}. \tag{2.1}$$

Here we use the notation $[\vec{\alpha}]a$ for the action of the current $[\vec{\alpha}]$ on the field labelled a. To derive (2.1) we used [2, 10]

$$S_{[\vec{\alpha}]a,c} = e^{2\pi i \vec{\alpha}\cdot\vec{Q}(c)} S_{ac}, \tag{2.2}$$

and assumed that $S_{ac} \neq 0$. This is certainly true if $c = 0$. In that case we thus find that

$$\sum_{[\vec{\gamma}]} e^{2\pi i \vec{\gamma}\cdot\vec{Q}(a)} M_{[\vec{\gamma}],0} \in \mathbf{Z}^+, \tag{2.3}$$

where $\mathbf{Z}^+$ denotes the non-negative integers. This must be true for all possible charges $\vec{Q}(a)$. It is easy to show [11] that in any RCFT with simple currents, fields exist with any allowed value of the charge.

The closure condition implies that if $M_{J_1,0} \neq 0$ and $M_{J_2,0} \neq 0$, then $M_{J_1 J_2,0} \neq 0$. In other words, the set of currents J with $M_{J,0} \neq 0$ closes under fusion, and forms a subgroup of the center.

Furthermore, if $\vec{\gamma}$ denotes an integer spin combination of currents with $M_{[\vec{\gamma}],0} \neq 0$, and if $M_{ab} \neq 0$, then the closure condition implies that $M_{[\vec{\gamma}]a,b} \neq 0$. The conformal weight of the field $[\vec{\gamma}]a$ is

$$h([\vec{\gamma}]a) = h(a) + h([\vec{\gamma}]) - \vec{\gamma}\cdot\vec{Q}(a).$$

Because of T-invariance we must require that $h(b) = h(a) = h([\vec{\gamma}]a) \bmod 1$. It follows that M_{ab} can only be non-zero if $\vec{\gamma}\cdot\vec{Q}(a) = 0$ for all currents $[\vec{\gamma}]$ in the algebra. In other words, all fields with non-zero charge with respect to the left algebra are projected out.

From (2.1) we learn furthermore that all fields a whose charges with respect to all the currents in the left algebra are zero, must satisfy

$$\sum_{[\vec{\alpha}]} M_{a,[\vec{\alpha}]a} = \sum_{[\vec{\gamma}]} M_{[\vec{\gamma}],0} = E_L, \tag{2.4}$$

where E_L is the number of fields in the left algebra.[1] Hence all such fields must appear in the theory. In the following we will denote the condition of vanishing charge with respect to the left algebra as $\mathscr{A}_L\cdot\vec{Q}(a) = 0$.

Now we would like to determine the values of the non-vanishing matrix elements $M_{[\vec{\gamma}],0}$. Consider the relation $M_{00} = S_{0a}M_{ab}S_{b0}$. When written in terms of orbits this takes the form

$$M_{00} = \sum_{[\vec{\alpha}]} \sum_{a \text{ with } \mathscr{A}_L\cdot\vec{Q}(a)=0} (S_{0a})^2 M_{a,[\vec{\alpha}]a},$$

where we have used (2.2). Using (2.4) we get now

$$M_{00} = E_L \sum_{a \text{ with } \mathscr{A}_L\cdot\vec{Q}(a)=0} (S_{0a})^2.$$

On the other hand, for every integer spin subgroup of the center we can always construct a modular invariant $\tilde{M}$ so that $\tilde{M}_{b0} = 1$ exactly when b is a current in that subgroup. This can be achieved by multiplying matrices $M(J_1)\cdots M(J_l)$, each obtained by means of the orbifold inspired procedure of [2]. Each such matrix $M(J)$ yields an invariant with an identical left and right chiral algebra consisting of the current J and its powers. All fields that are non-local with respect to J are projected out, and all other fields are grouped into multiplets by the action of J, and paired diagonally. The currents J_i are mutually local, and are therefore not projected out by each other. In this way we can always construct a matrix $\tilde{M}_{b0} = 1$ if and only if $M_{b0} \neq 0$. Although M need not be identical to $\tilde{M}$, both matrices

[1] Note that $M_{[\vec{\gamma}],0}$ may in principle be larger than one, in which case there would be more than one field in the chiral algebra corresponding to the current $[\vec{\gamma}]$. We will prove that this cannot happen for simple current invariants. There are, however, exceptional invariants with $M_{b0} = 2$ [2]

satisfy $M_{ab} = \tilde{M}_{ab} = 0$ if a has a non-zero charge with respect to one of the currents in the algebra. Hence for $\tilde{M}$ we get

$$\tilde{M}_{00} = N_L \sum_{a \text{ with } \mathscr{A}_L \cdot \vec{Q}(a) = 0} (S_{0a})^2,$$

where N_L is the order of the subgroup of the center defined by the left algebra. Because $M_{00} = \tilde{M}_{00} = 1$, we conclude that $E_L = N_L$, and therefore $M_{[\vec{\gamma}],0} = 1$ for every current $[\vec{\gamma}]$ in the left algebra. Thus for every simple current invariant we find

$$M_{ab} = 0 \quad \text{if} \quad \mathscr{A}_L \cdot \vec{Q}(a) \neq 0,$$
$$\sum_b M_{ab} = N_L \quad \text{otherwise.}$$

In particular the number of currents in the right algebra, $N_R \equiv \sum_b M_{0b}$, is equal to N_L. From now on we will denote this number simply by N. Now all the previous arguments can be repeated for the right algebra $\mathscr{A}_R$. Note that the left and right algebras need not be identical.

The closure condition tells us furthermore something about the values of M on other orbits. If J is a field in the right algebra ($M_{0J} \neq 0$), then $M_{ab} \neq 0$ implies that also $M_{a,Jb} \neq 0$. If b is not a fixed point of any current in $\mathscr{A}_R$ this defines for each a precisely N non-vanishing matrix elements. Since we know that $\sum_b M_{ab} = N$ it follows that each of these matrix elements must be equal to 1. Thus given one matrix element on each row, one also knows all the others. The same is true for the columns of M.

This argument does not hold if b is a fixed point of one of the currents of the right algebra. In that case $\sum_b M_{ab}$ should still be equal to N, but the closure condition does not force us to distribute this sum over N different matrix elements. In Appendix D we show that the sum should be distributed equally over all fixed points. Thus if the action of the left or right algebra on a fixed point f produces only N_f different fields, where N_f is (necessarily) a divisor of N, then all the matrix elements of M in the row or column of f are equal to N/N_f.

The fields in the left- and right-moving sector with zero charges with respect to the left and right algebras are thus organized into representations of those algebras. Each representation consists of a number of representations of the original conformal field theory, combined by the action of $\mathscr{A}_L$ or $\mathscr{A}_R$. The modular invariant partition function is now specified completely by a one-to-one map taking the representations of the right algebra to those of the left algebra. This mapping must be one-to-one since this is the only way to respect the rule that $\sum_b M_{ab}$ is equal to N for all fields a that are local with respect to $\mathscr{A}_R$. The matrix M consists thus of blocks, whose internal structure is determined completely by the action of $\mathscr{A}_L$ and $\mathscr{A}_R$. Since our interest is only in simple current invariants, the mapping between the representations of the left and right algebras must be achieved by simple currents.

2.2. Identical Left and Right Extensions. Consider now first the invariants with $\mathscr{A}_L = \mathscr{A}_R \equiv \mathscr{A}$. In this case there is always at least a block-diagonal invariant, for which the mapping from the right to the left sector is the identity. Any other mapping corresponds to a fusion rule automorphism of the new theory that is obtained by extending the algebra. It is natural to suspect that for simple current invariants these automorphisms are generated by the simple currents of the new theory. There are two potential problems with this conjecture. First of all one may worry that simple currents that are projected out could still play a non-trivial rôle, and generate extra automorphisms not taken into account in [8]. This is not true for the following reason. Suppose J is a current in $\mathscr{A}$, and K any other current. Suppose $M_{a,Ka} \neq 0$. Then also $M_{a,JKa} \neq 0$. Hence $h(Ka) = h(JKa) = h(Ka) + h(J) - Q_J(K) - Q_J(a) \bmod 1$. Because $h(J) = Q_J(a) = 0 \bmod 1$ it follows that $Q_J(K) = 0$. Hence only currents K that are themselves in representations of $\mathscr{A}$ have to be considered.

The second potential problem has to do with fixed points. To make this precise, we go to a new basis in which only the representations of $\mathscr{A}$ occur. To define this basis we choose one orbit representative a in each $\mathscr{A}$-orbit of fields with zero charge, and we define new "characters"

$$\hat{\mathscr{X}}_a = \sqrt{\frac{N}{N_a}} \sum_{[\vec{\alpha}] \in \mathscr{A}}^{N_a} \mathscr{X}_{[\vec{\alpha}]a}, \tag{2.5}$$

where $\mathscr{X}$ denote the original characters. Here the sum is over all *distinct* fields on the orbit. Note that the new characters $\hat{\mathscr{X}}$ may have non-integral coefficients if the number of distinct fields in the orbit, N_a, is not equal to the number of currents in $\mathscr{A}, N$ (this happens when there are fixed points). The normalization in (2.5) is such that this basis transformation can be extended to an orthogonal transformation U on the set of characters, up to an overall factor $\sqrt{N}$ (the matrix U is defined more carefully in Appendix D).

It is easy to compute the matrix $\hat{S}$ that performs the transformation $\tau \to -\frac{1}{\tau}$ on the new characters $\hat{\mathscr{X}}$. This matrix is equal to $USU^\dagger$ restricted to the invariant subspace spanned by the characters $\hat{\mathscr{X}}_a$. The result is

$$\hat{S}_{ab} = \sqrt{N_a N_b} S_{ab},$$

where $\tau \to \tau + 1$ is represented by $\hat{T}_{ab} = T_{ab}$. For the fusion coefficients one finds

$$\hat{N}_{abc} = \sqrt{\frac{N_b N_c}{N_a N}} \sum_{[\vec{\alpha}] \in \mathscr{A}}^{N_a} N_{[\vec{\alpha}]a,b,c}, \tag{2.6}$$

where the sum is over all N_a different fields generated from a by the algebra. In general these fusion coefficients are not integers. The origin of this problem is the same as that of the non-integer coefficients in the characters, and the solution is known (see e.g. [12, 9, 13, 14]) in principle: the fixed-point fields have to be resolved into several distinct fields.

Although in many cases it is known how to do this explicitly [14], there is no general and mathematically rigorous formula for the correct matrix S. Furtunately, we can avoid it. Although in the presence of fixed points $\hat{S}$ is not the modular transformation matrix of the new theory, it is good enough for our purposes since it satisfies the requirements needed for the validity of the classification of automorphisms of Ref. [8] (see also the conditions specified in [15]). Namely, $\hat{S}$ is unitary and symmetric, it satisfies $(\hat{S}\hat{T})^3 = \hat{S}^2$, and although not all of its fusion coefficients are integers, the ones that matter are: it is easy to show that all simple currents have correct fusion rules.

In the new basis any modular invariant partition function with chiral algebra $\mathscr{A}$ takes the form

$$\sum_{a,b} \mathscr{X}_a M_{ab} \mathscr{X}_b^* = \sum_{a,b\,\text{orbits}} \hat{\mathscr{X}}_a \hat{M}_{ab} \hat{\mathscr{X}}_b^* .$$

Here the first sum is over all zero-charge fields, and the second only over the distinct orbits. The matrix $\hat{M}$ is equal to $UMU^\dagger$, restricted to the subspace spanned by the characters $\hat{\mathscr{X}}_a$. This subspace is an invariant subspace of $\hat{M}$ provided that the fixed-point entries of M are well-behaved. In fact, $\hat{M}$ has then non-zero entries only on this invariant subspace.

This transformation has the effect of collapsing the blocks of M into single entries, whose values are either zero or N, for non-fixed points as well as for fixed points. Clearly $[\hat{M}, \hat{S}] = [\hat{M}, \hat{T}] = 0$, since the unhatted matrices had that property. Furthermore, there is precisely one non-zero entry per row or column of $\hat{M}$. Therefore this matrix is N times a fusion rule automorphism of the fusion rules defined by $\hat{S}$.

This completes the classification of all modular invariants with the same left and right algebra. The algebras themselves are simply all possible subgroups of the center formed entirely by integer spin currents. The diagonal theory with this particular extension of the algebra can be obtained by multiplying matrices $M(J_i)$, so that the currents J_i span $\mathscr{A}$. All other theories with $\mathscr{A}_L = \mathscr{A}_R = \mathscr{A}$ can be obtained by applying the construction of all simple current fusion rule automorphisms presented in [8], using the matrix $\hat{S}$ defined above. This conclusion is valid for any set of simple currents, and not restricted to centers $(\mathbf{Z}_p)^k$.

The results obtained in the foregoing two sub-sections are in agreement with, and partly contained in those obtained in [12] using the "polynomial equations." However, our starting point is somewhat different. Unlike the authors of [12] we are only imposing conditions on the matrix M, and not on properties of the conformal blocks. Nevertheless we obtain a more tightly constrained general form of M than that of [12] because of the additional restriction to simple current invariants.

2.3. Different Left and Right Extensions. Now we have to deal with modular invariant partition functions with different left and right algebras. Our starting point is the following

Theorem. *Consider a* RCFT *with center* $(\mathbf{Z}_p)^k$. *Consider an integer spin current* K. *Then a modular invariant partition function satisfying all previous conditions, with left and right algebras* $\mathscr{A}_L$ *and* $\mathscr{A}_R$ *such that* $K \in \mathscr{A}_L$ *but* $K \notin \mathscr{A}_R$, *can exist only if there exists a simple current which is non-local with respect to* K. *Furthermore, a modular invariant partition function in which the integer spin currents* K *and* K', *generating different* $\mathbf{Z}_p$ *subgroups of the center, appear as left and right extensions, does indeed exist if both* K *and* K' *are each non-local with respect to at least one simple current in the theory.*

Proof. Suppose first that K is local with respect to any simple current in the theory, and that $K \in \mathscr{A}_L$. Consider any field a that has zero charge with respect to $\mathscr{A}_L$, and in particular with respect to K. Then if $M_{ab} \neq 0$, $b = Ja$ for some simple current J. For any field b that may appear, we find thus $Q_K(b) = Q_K(J) + Q_K(a)$. Hence K is local with respect to all representations of $\mathscr{A}_R$. It is then easy to show that K must be in $\mathscr{A}_R$ [16]. This proves the first part of the theorem.

Suppose now that K is non-local with respect to some other simple current, and analogously for K'. If the two currents K and K' are non-local with respect to *each other*, the modular invariant promised in the theorem can be constructed by simply multiplying the matrices $M(K)M(K')$. It is easy to show that in this product K is in the left algebra but not in the right one, and vice versa. Let us thus assume that K and K' are local with respect to each other. If J is non-local w.r.t. K and J' w.r.t. K', then either J or J' is non-local with respect to both K and K', or their product is. So we may assume that there is a single current J that is non-local with respect to both K and K'. Furthermore, by replacing K and K' by powers of themselves (which generate the same orbit as K and K'), we can arrange that $Q_K(J) = Q_{K'}(J) = \frac{1}{p}$. The 3×3 monodromy matrix $r_{ij}(\equiv pQ_i(J_j))$ of these three currents K, K' and J is thus

$$r = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 2m \end{pmatrix},$$

for some integer m.

Now we use the results of [8] to construct an automorphism in this system of three currents. As explained in that paper, any automorphism is characterized by a matrix μ satisfying the equations

$$\begin{aligned} (\mu + \mu^T + \mu r \mu^T)_{ij} &= 0 \bmod p, \quad i \neq j, \\ (\mu + \tfrac{1}{2}\mu r \mu^T)_{ii} &= 0 \bmod p. \end{aligned} \tag{2.7}$$

It is easy to check that the following matrix μ is a solution

$$\mu = \begin{pmatrix} m & m & -1 \\ m & m & -1 \\ -1 & -1 & 0 \end{pmatrix}. \tag{2.8}$$

It is also easy to check that the corresponding fusion rule automorphism $M(\mu)$ has the property that $M(\mu)M(K')$ is a modular invariant partition function with $K' \in \mathscr{A}_R$ (as is already manifest) and $K \in \mathscr{A}_L$.

The extension of this result to larger left and right algebras is straightforward. It is clear from the foregoing discussion that we have to distinguish two types of simple currents:

Type A: Currents that are local with respect to all simple currents in the theory (including themselves).

Type B: Currents that are non-local with respect to at least one simple current in the theory.

Note that type A currents can have either integer or half-integer spin, since currents with any other spin are non-local with respect to themselves, and thus necessarily of type B. Type B currents can have any spin.

It follows from the foregoing theorem that if any type A current appears in the left algebra, it *must* appear also in the right algebra, and vice versa. On the other hand, extensions by type B currents can be done independently in the left- and right-moving sectors. For a single $\mathbf{Z}_p$ factor this conclusion is already contained in the theorem. To understand why it is true for any number of extensions, we should first discuss how the center changes upon extension of the algebra.

If one extends the algebra by means of a type A current the center is reduced from $(\mathbf{Z}_p)^k$ to $(\mathbf{Z}_p)^{k-1}$. No currents are projected out, but the current J disappears into the identity character of the new theory, and is not a separate primary field anymore. If one extends the algebra with a type B current J, the center reduces from $(\mathbf{Z}_p)^k$ to $(\mathbf{Z}_p)^{k-2}$. The current J disappears for the same reason as before, and in addition one current J' and its powers disappears because it is not local with respect to J (any other current J'' can always be made local w.r.t. J by multiplying it with a suitable power of J').

Suppose we wish to construct an invariant with a left and a right algebra, both isomorphic to $(\mathbf{Z}_p)^q$, so that neither the left nor the right algebra contains any type A current (apart from the identity). It follows that there must be at least q independent currents that are non-local w.r.t. $\mathscr{A}_L$. If there were fewer, then some linear combination of the currents in $\mathscr{A}_L$ is local w.r.t. all currents, and hence is of type A, in contradiction to the assumption. The same is true for $\mathscr{A}_R$. We can now build the desired invariant in steps, each time adding a factor $\mathbf{Z}_p$ to the algebra on the left and the right. We are completely free in the choice of the $\mathbf{Z}_p$ factor we add on either side. After each step, the center in the left as well as the right sector is reduced by $\mathbf{Z}^2$: one factor has disappeared into the chiral algebra we are building, and one factor disappears from the set of q independent currents that was non-local w.r.t. the algebra. Therefore after k steps there is still an $q-k$ dimensional space of such currents available, enough to continue the process until $k=q$.

Note that we have shown previously that the left and right extensions must be equal in size. If the center is $(\mathbf{Z}_p)^k$, this completely fixes the group structure of the currents in the algebra up to isomorphism, since all equal size subgroups of $(\mathbf{Z}_p)^k$ are isomorphic. Within this restriction all left–right combinations are allowed except those involving different type A orbits, explicitly forbidden by the theorem. The foregoing construction gives us at least one example of a modular invariant partition function for any possible combination of left and right chiral algebras.

How do we find *all* such examples? Suppose the modular invariant M_0 has different left and right chiral algebras, $\mathscr{A}_L \neq \mathscr{A}_R$. Suppose that M_1 is a different matrix, but also with left algebra $\mathscr{A}_L$ and right algebra $\mathscr{A}_R$. Consider now the matrices $\frac{1}{N}M_0M_0^T$ and $\frac{1}{N}M_0M_1^T$, where N is the number of currents in $\mathscr{A}_L$ and $\mathscr{A}_R$. It is easy to check that both matrices have integer coefficients, multiplicity 1 for the identity, and commute with S and T. Furthermore both have left and right chiral algebras that are equal to each other and to $\mathscr{A}_L$. Finally, it is also obvious that the two products are different. The matrix $\frac{1}{N}M_0M_0^T$ is in fact the diagonal invariant of the theory with extended algebra $\mathscr{A}_L$, and $\frac{1}{N}M_0M_1^T$ must therefore be an automorphism of that theory. Clearly any further modular invariant M_i

with algebras $\mathscr{A}_L$ and $\mathscr{A}_R$ can be used to build a new and different fusion rule automorphism of the left theory.

Conversely, any fusion rule automorphism of the left theory can be used to change M_0 to a different matrix M_0' with left and right algebras $\mathscr{A}_L$ and $\mathscr{A}_R$. Hence the set of solutions with this combination of algebras is in one-to-one correspondence with the set of fusion rule automorphisms of the theory with algebra $\mathscr{A}_L$, which we know explicitly using the results of [8].

This completes the classification of all modular invariants with different left and right algebras. An obvious extension of the previous arguments should still be pointed out. Clearly the entire argumentation used above applies equally well to $\mathscr{A}_R$ (by using $M_0^T M_0$ instead of $M_0 M_0^T$). Hence the set of invariants is also in one-to-one correspondence with the fusion rule automorphism of the right theory. This implies that the fusion rule automorphisms of the left and the right theory are isomorphic to each other.

More interestingly, it follows that all extensions involving the same type A currents and the same *number* of type B currents are isomorphic to each other, since for any two such extensions there exists a matrix M_{ab} that maps the representations into each other in such a way that the fusion rules are preserved. An obvious consequence is that all new RCFT's obtained by extending the algebra of a given RCFT with the same type A currents and the same number of type B currents have isomorphic centers, and the same monodromy matrices r up to basis transformations.

This concludes the classification of all modular invariants. The only centers for which our classification is still incomplete are those that contain factors $\mathbf{Z}_{p^n}$, $n \geqq 2$. In this case we do not yet know in general which left algebra can be combined with which right algebra.

3. $\mathbf{Z}_p \times \mathbf{Z}_p$

In this section we will illustrate the results of the previous section and those of [8] for generic RCFT's with a center $\mathbf{Z}_p \times \mathbf{Z}_p$, p prime, generated by two simple currents J_1 and J_2. Our aim is to analyze the different modular invariant partition functions corresponding to any monodromy matrix r. For $p = 2$ this problem has already been solved in [11]. Here we will therefore focus on p odd. We recommend reading first Appendix A which contains several number-theoretic results that will be used frequently throughout this paper.

As explained in Appendix B, the monodromy matrix r can have the following inequivalent values: for p odd

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2n \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2n \end{pmatrix}, \tag{3.1}$$

where n is a non-square modulo p (i.e. a fixed representative of $\{n\}$), and for $p = 2$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}. \tag{3.2}$$

Consider first the solutions of the matrices M_{ab} that are permutations and define automorphisms of the fusion rules [8],

$$M_{0,[\vec{\alpha}]} = \delta^p_{0,[\vec{\alpha}]}, \quad \sum_{[\vec{\alpha}]} M_{a,[\vec{\alpha}]a} = 1. \tag{3.3}$$

This kind of solutions, analyzed in Ref. [8] for a general center $\mathbf{Z}_{N_1} \times \cdots \times \mathbf{Z}_{N_l}$, can be characterized by an integer valued matrix μ_{ij} $(i, j = 0, 1, \ldots, l)$ (defined mod p) that satisfy Eqs. (2.7). This matrix "measures," for any field a, the distance of the only non-vanishing element $M_{a,[\vec{\mu}(a)]a} = 1$ from the diagonal (the current $[\vec{\mu}(a)]$ is constructed out of the matrix μ_{ij} and the charge $\vec{Q}(a)$, see Ref. [8]).

For a center $\mathbf{Z}_p$, μ_{ij} reduces to a single parameter μ that satisfies $\mu + \frac{1}{2}\mu^2 r = 0 \bmod p$. If $r = 0$ the only solution is $\mu = 0$ corresponding to the diagonal invariant. If $r \neq 0$ there is an additional solution[2] $\mu = -\dfrac{2}{r} \bmod p$, a non-trivial automorphism. For a center $\mathbf{Z}_p \times \mathbf{Z}_p$ the number of solutions of (2.7) depends on r and p in a rather intricate way. For odd p the different possibilities are as follows.

(a) For $r = \mathrm{diag}(0,0)$ Eqs. (2.7) reduce to $\mu_{12} = -\mu_{21}$, $\mu_{11} = \mu_{22} = 0$. Therefore there are p solutions.

(b) For $r = \mathrm{diag}(0,2)$ the solutions of Eqs. (2.7) are determined by all p possible values of μ_{12} and two possible values of μ_{22} ($\mu_{22} = 0$ and $\mu_{22} = -1 \bmod p$), a total of $2p$ solutions. The same number of solutions is obtained for $r = \mathrm{diag}(0, 2n)$, as can be easily understood because Eqs. (3.4) are invariant under the simultaneous transformation (defined mod p) $r \to nr$, $\mu \to \mu/n$.

(c) For $r = \mathrm{diag}(2,2)$ the equation $\mu_{12}^2 = -\mu_{11}(1 + \mu_{11})$ has one solution for every value of the integer ratio $q = (\mu_{12}/\mu_{11}) \bmod p$, with $\mu_{11} \neq 0$, except for the values that satisfy $q^2 = -1 \bmod p$. There are two such values of q if $p = 4m + 1$ and none if $p = 4m - 1$. Since q takes all values including 0, this equation has $p - 2$ solutions with $\mu_{11} \neq 0$ if $p = 4m + 1$ and p if $p = 4m - 1$. In addition there is the trivial solution $\mu_{11} = \mu_{12} = 0$. Therefore the pair (μ_{11}, μ_{12}) has $p + 1$ solutions for $p = 4m - 1$ and $p - 1$ solutions for $p = 4m + 1$. The same results apply obviously to the pair (μ_{22}, μ_{21}) satisfying the equation $\mu_{21}^2 = -\mu_{22}(1 + \mu_{22})$. Finally there are two possibilities for coupling both pairs: $(\mu_{22} = \mu_{11}, \mu_{21} = -\mu_{12})$ and $(\mu_{22} = -1 - \mu_{11}, \mu_{21} = \mu_{12})$, so that the total number of automorphisms is $2(p + 1)$ for $p = 4m - 1$ and $2(p - 1)$ for $p = 4m + 1$.

(d) For $r = \mathrm{diag}(2, 2n)$ one finds, in a similar way as in the previous case, that the pairs (μ_{11}, μ_{12}) and (μ_{22}, μ_{21}) have $p + 1$ solutions if no integer l exists such that $-l^2 = n \bmod p$. If such an integer exists the number of solutions reduces to $p - 1$. Since n is by definition a non-square, one deduces that such integer l only exists for $p = 4m - 1$. As before, there are two ways to couple the pairs of solutions, so that the final number of automorphisms is $2(p - 1)$ for $p = 4m - 1$ and $2(p + 1)$ for $p = 4m + 1$.

---

[2] By $\dfrac{1}{r} \bmod p$ we mean here and in the following the integer $s \bmod p$ such that $sr = 1 \bmod p$. This number is well-defined and unique, modulo p, if $r \neq 0$

Now let us analyze the solutions for the matrices M_{ab} that provide extensions of the chiral algebra

$$M_{[\vec{\gamma}_L],0} = M_{0,[\vec{\gamma}_R]} = 1, \tag{3.4}$$

where the integer spin simple currents $[\vec{\gamma}_L]$ and $[\vec{\gamma}_R]$ are organized in subgroups of the center and extend the left and right chiral algebras respectively.

For a center $\mathbf{Z}_p$ the only possible extension of the chiral algebra is given by the center $\mathbf{Z}_p$ itself, provided $r=0$ since $h(J^\alpha) = -\frac{1}{2}\alpha^2 r/p \bmod 1$. In this case, all fields with non-vanishing charge are projected out. For a center $\mathbf{Z}_p \times \mathbf{Z}_p$ there are a variety of different possibilities for extending the chiral algebra depending on r and p, in an analogous and in some sense complementary way as for the automorphisms. Let us analyze the different possibilities for p odd.

(a) For $r = \operatorname{diag}(0,0)$ the left and right algebras must be the same, $\mathscr{A}_L = \mathscr{A}_R$, since all the simple currents are local to each other. All of them have integer spin, so that there are $p+2$ possible extensions of the chiral algebra corresponding to $p+1$ $\mathbf{Z}_p$ subgroups (generated by J_1 and $J_1^\alpha J_2$, $\alpha = 0, 1, \ldots p-1$) and to $\mathbf{Z}_p \times \mathbf{Z}_p$ itself. The modular invariants constructed out of these extensions are just the block-diagonal ones. The reason is that for every $\mathbf{Z}_p$ extension the center reduces to the other $\mathbf{Z}_p$ left, and this last one cannot produce new modular invariants since its currents have integer spin.

(b) For $r = \operatorname{diag}(0,2)$ there is only one subgroup of integer spin currents: the $\mathbf{Z}_p$ subgroup generated by J_1, that is local with respect to any other simple current. Therefore there is only one possible extension of the chiral algebra, with $\mathscr{A}_l = \mathscr{A}_R$. Since the left-over center $\mathbf{Z}_p$ is formed by currents with fractional spin ($h(J_2) = -1/p$), it will generate a non-trivial automorphism ($\mu = -1 \bmod p$) in addition to the trivial one. As a result there are two different modular invariants associated to the unique extension of the chiral algebra: the block-diagonal one and one permutation of the corresponding blocks. Similar results apply for the case $r = \operatorname{diag}(0, 2n)$.

(c) For $r = \operatorname{diag}(2,2)$ the condition on $J_1^\alpha J_2^\beta$ for having integer spin is $\alpha^2 = -\beta^2 \bmod p$. Therefore, this condition will be satisfied only for $p = 4m+1$, the solution being $\beta^2 = \left(\alpha\left[\left(\frac{p-1}{2}\right)!\right]\right)^2 \bmod p$. Since p is prime, the integer spin subgroups must contain currents with all possible values of α and β, from 0 to $p-1$. In particular $\alpha = 1$ must appear once in every subgroup. This implies that there are two integer spin $\mathbf{Z}_p$ subgroups corresponding to the two solutions $\left(\alpha = 1, \beta = \pm\left(\frac{p-1}{2}\right)! \bmod p\right)$ for $p = 4m+1$, and no integer spin currents for $p = 4m-1$. In the former case, the currents generating the two subgroups are non-local with respect to each other. Therefore one can extend the left or right chiral algebras independently by any of them. Thus for $p = 4m+1$ there are four possible extensions giving rise to four different modular invariants (the center remaining after these extensions is trivial, as explained in Sect. 2).

(d) For $r = \operatorname{diag}(2, 2n)$ the condition for $J_1^\alpha J_2^\beta$ to have integer spin is $\beta^2 n = -\alpha^2 \bmod p$. Thus, a non-square has to be equal to a negative square modulo p, a condition that gives two solutions for $\alpha = 1$ if $p = 4m-1$ and no solution if

Table 1.

r	p (prime)	# of automorphisms	# of extensions	total #
diag (0, 0)	odd	p	$p+2$	$2p+2$
diag (0, 2)	odd	$2p$	2	$2p+2$
diag (0, 2n)	odd	$2p$	2	$2p+2$
diag (2, 2)	$\begin{cases} 4m+1 \\ 4m-1 \end{cases}$	$2p-2$ $2p+2$	4 0	$2p+2$ $2p+2$
diag (2, 2n)	$\begin{cases} 4m+1 \\ 4m-1 \end{cases}$	$2p+2$ $2p-2$	0 4	$2p+2$ $2p+2$
diag (0, 0)	2	2	4	$2p+2$
diag (0, 2)	2	3	3	$2p+2$
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	2	2	4	$2p+2$
$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$	2	6	0	$2p+2$

$p = 4m + 1$. As before, the currents generating the two integer spin $\mathbf{Z}_p$ subgroups are non-local with respect to each other. As a result there will be four different modular invariants corresponding to the four possible extensions of the chiral algebra, for $p = 4m - 1$, and no extensions for $p = 4m + 1$.

All these results are summarized in Table 1. Observe that the total number of modular invariants, pure automorphisms plus extensions of the chiral algebra, is a constant equal to $2(p + 1)$ independently of the matrix r (for $\mathbf{Z}_p$ this number is 2). It seems that there is some sort of conservation rule or complementarity that interchanges pure automorphisms and extensions of the chiral algebra, although the pattern of this mechanism is very r-dependent. However, for the cases $r = \mathrm{diag}(2, 2)$ and $r = \mathrm{diag}(2, 2n)$ it turns out to be the same. As a matter of fact, between these two values of r there is a total symmetry of results under the interchange $p = 4m + 1 \leftrightarrow p = 4m - 1$.

For $p = 2$ a total of six modular invariants was found in [11], following the same rule as for p odd.

Now it is natural to conjecture that in general, for $(\mathbf{Z}_p)^k$, the total number of modular invariants will depend only on p and k, but not on the monodromy matrix r. We will see in the next section that this is indeed the case.

4. $(\mathbf{Z}_p)^k$

In this section we will analyze a generic RCFT with simple currents generating a center $(\mathbf{Z}_p)^k$, p prime. We will determine, for a given matrix r, the number of modular invariants of pure automorphism type and the number corresponding to extensions of the chiral algebra. Finally, we will prove our conjecture that the total number of modular invariants is independent of r and depends only on p and k in a universal way, i.e. is given by the same formula for $p = 2$ and $p = 4m \pm 1$.

As explained in Appendix B, the monodromy matrices r can be characterized in the following way. If p is odd r can be diagonalized, and the different equivalent matrices are given by three numbers (n_0, n_1, n_n): the number of diagonal elements

r_{ii} such that $\frac{r_{ii}}{2}$ is equal to 0, 1 and n respectively, where n is a non-square (a fixed representative of $\{n\}$). Furthermore n_n can only be zero or one. If $p=2$ the monodromy matrices cannot always be diagonalized and are described by the numbers n_A, n_B of 2×2 blocks $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ respectively, and the numbers n_0, n_1 of diagonal elements equal to 0 and 2, as before. The possible choices for the four numbers (n_0, n_1, n_A, n_B) are $(n_0, 0, n_A, 0)$, $(n_0, 0, n_A, 1)$ and $(n_0, 1, n_A, 0)$.

4.1. *p odd*

The Total Number of Automorphisms. Let us start with the computation of $A(n_0, n_1, n_n)$, the number of (pure) automorphisms corresponding to a monodromy matrix given by (n_0, n_1, n_n), for p odd. The direct analysis of (2.7) is too complicated for the general $(\mathbf{Z}_p)^k$ center (unmanageable already for $k=3$). Instead we will use the recipe formulated in [8] to compute $A(n_0, n_1, n_n)$ recursively. We refer the reader to Appendices A and C that contain some definitions and results used in the discussion which follows.

Suppose we are given a theory with center $(\mathbf{Z}_p)^k$, p odd prime, and monodromy matrix r described by (n_0, n_1, n_n). If an extra current is added with diagonal r-element $r_{(k+1)(k+1)}$, denoted as $2r$ ($r=0, 1$ or n), the equation satisfied by the corresponding diagonal μ-element $\mu_{(k+1)(k+1)}$, denoted as μ, is from (2.7)

$$\mu + r\mu^2 + \frac{1}{2}\sum_{j=1}^{k} \mu_{(k+1)_j} r_{jj} \mu_{(k+1)_j} = 0 \bmod p. \tag{4.1}$$

Now one has to find the solutions to this equation for all possible values of $\mu_{(k+1)_j}$, from 0 to $p-1$. But this is equivalent to finding the solutions to the equation

$$\mu + r\mu^2 + g(J) = 0 \bmod p \tag{4.2}$$

for the whole set of simple currents J of the original theory, since $g(J) = -ph(J) = \frac{1}{2}\sum_{j=1}^{k} \alpha_j r_{jj} \alpha_j$ and α_j runs from 0 to $p-1$.

One encounters the following cases. For $r=0$ one has $\mu = -g(J) \bmod p$, so that there is one solution for every J. Since the total number of simple currents is $p^{n_0+n_1+n_n}$, the recursion relation for the number of automorphisms is in this case

$$A(n_0+1, n_1, n_n) = p^{n_0+n_1+n_n} A(n_0, n_1, n_n). \tag{4.3}$$

For $r \neq 0$ the formal solution is given by[3]

$$\mu = \frac{1}{2r}[-1 \pm \sqrt{1-4rg(J)}] \bmod p. \tag{4.4}$$

[3] Here $\sqrt{a} \bmod p$ is defined to be the integer b so that $b^2 = a \bmod p$. There are precisely two solutions for b if a is a square $(\bmod p)$ (and p is a prime!), one solution if it is zero, and no solutions if it is a non-square $(\bmod p)$. The meaning of $\frac{1}{2r} \bmod p$ is explained in Sect. 3.

The number of solutions depends on whether $(1 - 4rg(J))$ is a square, a non-square or zero. For any current with $g(J) = 0$, Eq. (4.4) has two solutions. Since there are $I_0(n_0, n_1, n_n)$ simple currents with $g(J) = 0$, the contribution to the recursion factor of the number of automorphisms is $2I_0(n_0, n_1, n_n)$.

For $g(J) \neq 0$ several cases have to be distinguished by combining the following possibilities: $r = 1$ or $r = n$, $p = 4m + 1$ or $p = 4m - 1$ and $g(J) \in \{1\}$ or $g(J) \in \{n\}$.

Let us compute in some detail the total contribution to the recursion factor for the case $r = 1$, $p = 4m + 1$. If $g(J) \in \{1\}$ then $4rg(J) \in \{1\}$ and $-4rg(J) \in \{1\}$ as well. In the complete set of simple currents, $g(J)$ takes all $\frac{p-1}{2}$ different values of $\{1\}$ a number of times equal to $I_1(n_0, n_1, n_n)$. The addition of 1 to every complete set $\{1\}$ gives: 1 element equal to 0, $\frac{p-5}{4}$ elements of $\{1\}$ and $\frac{p-1}{4}$ elements of $\{n\}$. Thus there are $1 + 2\frac{p-5}{4}$ solutions for every complete set $g(J) \in \{1\}$. The contribution to the recursion factor is therefore $\frac{p-3}{2} I_1(n_0, n_1, n_n)$. If $g(J) \in \{n\}$ then $4rg(J) \in \{n\}$ and $-4rg(J) \in \{n\}$. Adding 1 to every complete set $\{n\}$ gives $\frac{p-1}{4}$ elements of $\{1\}$ and $\frac{p-1}{4}$ elements of $\{n\}$. Since $g(J)$ takes all $\frac{p-1}{2}$ different values in $\{n\}$ a number of times $I_n(n_0, n_1, n_n)$, the contribution to the recursion factor is $\frac{p-1}{2} I_n(n_0, n_1, n_n)$. Summing up the contributions corresponding to $g(J) = 0$, $g(J) \in \{1\}$ and $g(J) \in \{n\}$, and taking into account that the total number of currents satisfies

$$p^{n_0 + n_1 + n_n} = I_0(n_0, n_1, n_n) + \frac{p-1}{2} I_1(n_0, n_1, n_n) + \frac{p-1}{2} I_n(n_0, n_1, n_n) \tag{4.5}$$

one finally obtains

$$A(n_0, n_1 + 1, n_n) = [I_0(n_0, n_1, n_n) - I_1(n_0, n_1, n_n) + p^{n_0 + n_1 + n_n}] A(n_0, n_1, n_n) \tag{4.6}$$

with $p = 4m + 1$. The recursion relations for the other cases can be easily computed by repeating similar arguments. For the case $r = 1$, $p = 4m - 1$ one finds

$$A(n_0, n_1 + 1, n_n) = [I_0(n_0, n_1, n_n) - I_n(n_0, n_1, n_n) + p^{n_0 + n_1 + n_n}] A(n_0, n_1, n_n). \tag{4.7}$$

For $r = n$ the recursion factors turn out to be symmetric to those of $r = 1$ under the interchange $p = 4m + 1 \leftrightarrow p = 4m - 1$.

To obtain the final expression for $A(n_0, n_1, n_n)$ it is convenient to proceed in two steps. First one computes the solution for $A(0, n_1, n_n)$ applying the recursion relations above, and then one uses Eq. (4.3) to get the complete answer. For the first step, using the results of Appendix C for the quantities $I_a(0, n_1, n_n)$, $a = 0, 1, n$, one gets

$$A(0, n_1 + 1, n_n) = [p^N + (-1)^{n_1} p^{[N/2]}] A(0, n_1, n_n), \tag{4.8}$$

$$A(0, n_1, n_n + 1) = [p^N + (-1)^{n_n} p^{[N/2]}] A(0, n_1, n_n), \tag{4.9}$$

for $p = 4m + 1$, and

$$A(0, n_1 + 1, n_n) = [p^N + (-1)^{n_n} (-p)^{[N/2]}] A(0, n_1, n_n), \tag{4.10}$$

$$A(0, n_1, n_n + 1) = [p^N + (-1)^{n_1} (-p)^{[N/2]}] A(0, n_1, n_n), \tag{4.11}$$

for $p = 4m - 1$, where $N = n_1 + n_n$ and $\left[\frac{N}{2}\right]$ is the integer part of $\frac{N}{2}$. Since these results depend on N being odd or even, a double recursion is convenient. For N odd one finds the recursion factor $p^N(p^{N+1} - 1)$, for $p = 4m + 1$ as well as for $p = 4m - 1$, by increasing n_1 or n_n by two units and also by increasing n_1 and n_n one unit each. Thus for N odd

$$A(0, n_1, n_n) = 2 \prod_{l=1}^{(N-1)/2} p^{2l-1}(p^{2l} - 1), \tag{4.12}$$

where use has been made of $A(0,1,0) = A(0,0,1) = 2$. For N even the double recursion is more complicated that for N odd, but $A(0, n_1, n_n)$ can be computed easily by increasing n_1 or n_n by one unit in Eq. (4.12), using the recursion relations (4.8)–(4.11). One obtains, for $p = 4m + j$ $(j = \pm 1)$,

$$A(0, n_1, n_n) = 2[p^{N-1} - j^{N/2}(-1)^{n_1} p^{(N-2)/2}] \prod_{l=1}^{(N/2)-1} p^{2l-1}(p^{2l} - 1). \tag{4.13}$$

Now by using Eq. (4.3) one gets the recursion for the first argument

$$A(n_0, n_1, n_n) = \prod_{l=0}^{n_0 - 1} p^{N+l} A(0, n_1, n_n). \tag{4.14}$$

Thus one obtains finally, for N odd

$$A(n_0, n_1, n_n) = 2p^{(1/2)k(k-1) + (1/4)(1-N^2)} \prod_{l=1}^{(N-1)/2} (p^{2l} - 1), \tag{4.15}$$

for N even, $N \neq 0$,

$$A(n_0, n_1, n_n) = 2p^{(1/2)k(k-1) - (1/4)N^2} [p^{N/2} - j^{N/2}(-1)^{n_1}] \prod_{l=1}^{(N/2)-1} (p^{2l} - 1), \tag{4.16}$$

where $k = n_0 + N$, and for $N = 0$,

$$A(n_0, 0, 0) = p^{(1/2)n_0(n_0 - 1)}. \tag{4.17}$$

The Total Number of Modular Invariants. Now we will compute the number of modular invariants that provide extensions of the chiral algebra, for a given monodromy matrix r. By summing over all possible extensions (including the trivial one) and including for each extension all possible automorphisms, we obtain the total number of invariants $T(r, p, k)$. Our conjecture is that $T(r, k, p)$ is independent of r and depends on p and k in the following universal way:

$$T(r, k, p) = T(k, p) = \prod_{l=0}^{k-1} (1 + p^l). \tag{4.18}$$

We will calculate the number of invariants for any number of extensions of the algebra recursively. If one extends the algebra by l simple current orbits, one obtains a new theory with a new center and new monodromies. We have to know this information for two reasons: first of all to compute the number of fusion rule automorphisms of the new theory using the results of the previous subsection, and secondly to compute the number of single extensions, in order to go from l to $l + 1$.

The new center has already been determined in Sect. 2. If we extend the chiral algebra with a set of type B currents generating a $(\mathbf{Z}_p)^l$ subgroup of the center $(\mathbf{Z}_p)^k$, the latter reduces to $(\mathbf{Z}_p)^{k-2l}$. If we extend the algebra with type A currents (which exist if and only if $n_0 \neq 0$) generating a $(\mathbf{Z}_p)^l$ subgroup, the center $(\mathbf{Z}_p)^k$ reduces to $(\mathbf{Z}_p)^{k-l}$.

Now we determine the new matrix r. If we extend the algebra with a type A current, only that current itself will disappear, and n_0 is reduced by 1. The result of extensions by type B currents can be derived by making use of the isomorphism between such extensions which was discussed at the end of Sect. 2.3. In particular it was shown that the resulting r-matrices are all equal up to a choice of basis, and hence we can use any extension to compute the new r-matrix.

If r has just one non-vanishing entry on the diagonal there are no type B currents. If there are two non-vanishing entries there may or may not be a type B current, depending on p, as was discussed in detail in Sect. 3. If there is one, both non-vanishing entries disappear when the algebra is extended. Suppose therefore that there are at least three non-vanishing diagonal entries of r, labelled 1, 2 and 3. These entries may be assumed to be either equal to $2 \in 2\{1\}$ or $2n \in 2\{n\}$. Furthermore we may choose a basis so that $r_{11} = r_{22} = 2$ (in fact, we can choose a basis so that n_n is either 1 or 0).

We wish to extend the algebra with a linear combination of J_1 and J_2. If $p = 4m + 1$ there is an integer spin current of this type precisely if $r_{11} = r_{22} = 2$ (see Sect. 3). In the new theory both J_1 and J_2 disappear: one linear combination is part of the algebra, and the other one is projected out. Hence the new r-matrix has two entries "2" fewer, i.e. n_1 is reduced by 2.

Consider now $p = 4m - 1$. In this case there is an integer spin linear combination of J_1 and J_2 only if $r_{11} = 2$ and $r_{22} = 2n$ (or vice versa). We can bring r always to this form by means of the basis transformations discussed in Appendix B. If $r_{33} = 2n$ we simply interchange the labels 2 and 3, and if $r_{33} = 2$ we can change r_{33} and r_{22} simultaneously to the value $2n$. The extension of the algebra removes then one diagonal entry 2 and one diagonal entry $2n$ from r. Thus n_1 and n_n are both reduced by 1 (if $n_n = 0$ one may equivalently reduce n_1 by 3 and increase n_n by 1).

Let us analyze first the case $n_0 = 0$. It is convenient to introduce the notation $A(N, \varepsilon, j) = A(0, n_1, n_n)$ and $I_0(N, \varepsilon, j) = I_0(0, n_1, n_n)$, where $N = n_1 + n_n$, $\varepsilon = (-1)^{n_n}$ and $j = \pm 1$ corresponding to $p = 4m + j$ (as we have seen, the dependence of these quantities on ε and j only exists for N even). Note that ε is invariant under changes of basis, which allow us to decrease n_1 by an *even* number, while increasing n_n simultaneously by the same amount. According to the foregoing discussion, ε does not change upon extension of the algebra if $p = 4m + 1$, but it changes sign for each single extension by a type B current if $p = 4m - 1$. Thus after l extensions, the invariant parameters that determine r are modified from (N, ε) to $(N - 2l, \varepsilon j^l)$.

Define $B_l(N, \varepsilon, j)$ as the number of modular invariants with $(\mathbf{Z}_p)^l$ extensions of the chiral algebra, not including automorphisms, and $T_l(N, \varepsilon, j)$ as the number of such invariants including automorphisms, i.e.

$$T_l(N, \varepsilon, j) = B_l(N, \varepsilon, j) A(N - 2l, \varepsilon j^l, j). \tag{4.19}$$

Given $B_l(N, \varepsilon, j)$ one can obtain $B_{l+1}(N, \varepsilon, j)$ by combining all algebras with one extra integer spin orbit from the reduced center $(\mathbf{Z}_p)^{N-2l}$. The number of such orbits is

$$\frac{I_0(N-2l,\varepsilon j^l,j)-1}{p-1}. \tag{4.20}$$

Each orbit can be added independently on the left and on the right, as discussed in Sect. 2. However, on both the left and the right one gets any given extension many times, namely as many times as the number of $\mathbf{Z}_p$ subgroups of $(\mathbf{Z}_p)^{l+1}$, this number being equal to $\sum_{a=0}^{l} p^a$. The recursion relation is thus

$$B_{l+1}(N,\varepsilon,j)=\left[\frac{I_0(N-2l,\varepsilon j^l,j)-1}{p^{l+1}-1}\right]^2 B_l(N,\varepsilon,j), \tag{4.21}$$

where, for N odd

$$I_0(N-2l,\varepsilon j^l,j)=I_0(N-2l)=p^{N-2l-1}, \tag{4.22}$$

for N even

$$I_0(N-2l,\varepsilon j^l,j)=p^{N-2l-1}+(p-1)j^{N/2}\varepsilon p^{((N-2l)/2-1)}, \tag{4.23}$$

and we have used $(p-1)\sum_{a=0}^{l} p^a = p^{l+1}-1$. Taking into account that $B_0(N,\varepsilon,j)=1$, one obtains obviously

$$B_l(N,\varepsilon,j)=\prod_{m=0}^{l-1}\left[\frac{I_0(N-2m,\varepsilon j^m,j)-1}{p^{m+1}-1}\right]^2. \tag{4.24}$$

The number of modular invariants with $(\mathbf{Z}_p)^l$ extensions of the chiral algebra $T_l(N,\varepsilon,j)$, Eq. (4.19), can now be computed straightforwardly using the results (4.12), (4.13) and (4.22)–(4.24).

The *total* number of modular invariants $T(r,k,p)$ corresponding to a center $(\mathbf{Z}_p)^k$ and a monodromy matrix r given by $(0,n_1,n_n)$ is then

$$\begin{aligned} T(r,k,p)=T(N,\varepsilon,j) &= \sum_{l=0}^{[N/2]} T_l(N,\varepsilon,j) \\ &= \sum_{l=0}^{[N/2]} B_l(N,\varepsilon,j)\ A(N-2l,\varepsilon j^l,j). \end{aligned} \tag{4.25}$$

In the case at hand our conjecture (4.18) takes the form

$$T(N,\varepsilon,j)=T(N,p)=\prod_{l=0}^{N-1}(1+p^l). \tag{4.26}$$

To prove this we compute the quantity

$$T(N+2,\varepsilon,j)-(1+p^{N+1})(1+p^N)T(N,\varepsilon,j) \tag{4.27}$$

for N odd as well as for N even. This expression has to vanish if our conjecture turns out to be correct.

The direct computation of (4.27) using Eqs. (4.25), (4.12), (4.13) and (4.22)–(4.24) is rather difficult. Instead one can proceed as follows. One introduces some quantities

R_l such that (we omit ε and j in the arguments for clarity)

$$R_0\ A(N) = A(N+2), \tag{4.28}$$

$$R_{l+1}B_{l+1}(N)A(N-2(l+1)) = [R_l B_l(N) + B_{l+1}(N+2) - YB_l(N)]A(N-2l), \tag{4.29}$$

with $Y = (1+p^{N+1})(1+p^N)$. In this way the quantity (4.27), containing the sums given by (4.25), reduces to

$$2[(R_{(N-1)/2} - Y)B_{(N-1)/2}(N) + B_{(N+1)/2}(N+2)] \tag{4.30}$$

for N odd, where we have used $A(1) = 2$, and to

$$A(2)[(R_{(N-2)/2} - Y)B_{(N-2)/2}(N) + B_{N/2}(N+2)] + B_{(N+2)/2}(N+2) - YB_{N/2}(N) \tag{4.31}$$

for N even, with $A(2) = 2(p - \varepsilon j^{N/2})$ and $A(0) = 1$. Remarkably, the recursion relation (4.29) has a very simple solution, for N odd

$$R_l = p^N(p^{N+1} + 1 - 2p^{-l}) \tag{4.32}$$

and for N even

$$R_l = p^N(p^{N+1} + 1 - 2p^{-l} + \varepsilon j^{N/2} p^{(N/2)-l}(p-1)). \tag{4.33}$$

Using these expressions and Eqs. (4.22)–(4.24) it is easy to verify that the quantities (4.30) and (4.31) vanish.

Therefore we have proved that our conjecture (4.18) is true for theories with no zero eigenvalues in the monodromy matrix, in the case p odd.

When the monodromy matrix r contains n_0 diagonal elements equal to zero in addition to N non-vanishing ones, one can distinguish three kinds of integer simple currents: $(p^{n_0} - 1)$ currents corresponding to the "zero" part of r, $(I_0(N) - 1)$ currents corresponding to the "non-zero" part of r, and $(p^{n_0} - 1)(I_0(N) - 1)$ combined "zero-non-zero" currents (observe that the identity has been subtracted). Here $I_0(N) = I_0(N, \varepsilon, j)$. As before we will omit ε and j in what follows.

The extension of the chiral algebra by one $\mathbf{Z}_p$ leads to a reduced center $(\mathbf{Z}_p)^{k-1}$ in the first case, and to $(\mathbf{Z}_p)^{k-2}$ in the other two cases. The number of modular invariants with one $\mathbf{Z}_p$ extension, including automorphisms, is thus

$$\left(\frac{p^{n_0} - 1}{p-1}\right)A(n_0 - 1, N) + \left[\frac{p^{n_0}(I_0(N) - 1)}{p-1}\right]^2 A(n_0, N-2). \tag{4.34}$$

Observe that the number of possible orbits on the left term is not squared. The reason is that for these extensions the left and right chiral algebras must be the same, since the corresponding currents are of type A.

Taking into account overcounting factors for further extensions, one arrives easily at the following expression for the *total* number of modular invariants corresponding to a general monodromy matrix $r = \mathrm{diag}(0^{n_0}, 2^{n_1}, (2n)^{n_n})$, with $N = n_1 + n_n$:

$$T(n_0, N) = \sum_{a=0}^{n_0} Q_a(n_0) \sum_{b=0}^{(N-1)/2} \prod_{m=0}^{b-1} \left(\frac{p^{n_0 - a}[I_0(N-2m) - 1]}{p^{m+1} - 1}\right)^2 A(n_0 - a, N - 2b), \tag{4.35}$$

where $Q_a(n_0)$ is the number of subgroups $(\mathbf{Z}_p)^a$ contained in $(\mathbf{Z}_p)^{n_0}$. This number can be expressed in two equivalent ways:

$$Q_a(n_0) = \prod_{m=0}^{a-1} \left(\frac{p^{n_0-m}-1}{p^{m+1}-1} \right) = \sum_{\substack{\{k_1,k_2,\ldots,k_a\} \\ 0 \leqq k_a \leqq k_{a-1} \leqq \cdots k_1 \leqq (n_0-a)}} p^{\left\{ \sum_{i=1}^{a} k_i \right\}}. \tag{4.36}$$

By applying Eq. (4.14) one can factorize $T(n_0, N)$ in the form

$$T(n_0, N) = F(n_0, N) T(N), \tag{4.37}$$

where $T(N)$ is given by (4.25) and (4.26), and

$$F(n_0, N) = \sum_{a=0}^{n_0} Q_a(n_0) p^{((n_0-a)/2)(2N+n_0-a-1)}. \tag{4.38}$$

Then using

$$Q_a(n_0+1) = p^a Q_a(n_0) + Q_{a-1}(n_0) \tag{4.39}$$

one finds the recursion relation

$$F(n_0+1, N) = (1 + p^{n_0+N}) F(n_0, N) \tag{4.40}$$

with $F(0, N) = 1$, so that

$$F(n_0, N) = \prod_{l=N}^{n_0+N-1} (1 + p^l). \tag{4.41}$$

The *total* number of modular invariants is thus

$$T(n_0, N) = \prod_{l=0}^{n_0+N-1} (1 + p^l). \tag{4.42}$$

Since $n_0 + N = k$, we conclude that our conjecture (4.18) is true for a general monodromy matrix, in the case p odd.

4.2. *p even*

The Total Number of Automorphisms. The computations for p even are similar to those for p odd apart from one extra complication, which is due to the fact that r cannot be fully diagonalized. In deriving recursion relations we are forced to add 2×2 blocks to r. Consider first the recursion relation for $A(n_0, n_1, n_A + 1, n_B)$. Define $N = n_0 + n_1 + 2n_A + 2n_B$. We write the r-matrix in a basis labelled by $i = 1, 2, 3, \ldots, N+2$, where the additional 2×2 block is in the first two components. The number of automorphisms μ_{ij} in the last N components of the basis (i.e. $\mu_{1j} = \mu_{2j} = \mu_{i1} = \mu_{i2} = 0$) is equal to $A(n_0, n_1, n_A, n_B)$. First we add, following the prescription of [8], all allowed second rows of the form $\mu_{2j} = m_j$, with $m_1 = 0$. They are obtained by considering all 2^N possibilities for $m_j, j \geqq 3$, and solving the equation

$$m_2 + \frac{1}{2} \sum_{i=3}^{N+2} m_i r_{ij} m_j \bmod 2$$

for m_2. Because $r_{22} = 0$ this equation is linear in m_2, and has always one solution.

Thus in this first step the number of automorphisms is increased by a factor 2^N.

Now we add all allowed first rows, $\mu_{1j} = l_j$. The equation for l_1 is

$$l_1(1+l_2)+\frac{1}{2}\sum_{i=3}^{N+2} l_i r_{ij} l_j \bmod 2.$$

The $l_1 l_2$ term is due to the off-diagonal term in r. The number of solutions for l_1 depends on the value of $\langle l,l\rangle \equiv \sum_{i=3}^{N+2} l_i r_{ij} l_j$ and the value of l_2:

$\langle l,l\rangle$	l_2	l_1
0	0	0
0	1	0, 1
2	0	1
2	1	none.

Now we have to consider the second condition of [8], namely the existence of an auxiliary vector $\vec{v}$ (which was called $\vec{n}$ in [8]). This condition is only required if $l_1 = 0$, and trivially satisfied for diagonal r-matrices, which explains we did not encounter it before. The vector $\vec{v}$ satisfy $v_1 \neq 0$ and

$$v_1 + v_2 l_1 + v_1 l_2 + \langle l, v\rangle \neq 0 \bmod 2.$$

This second term vanishes because we only need to consider $l_1 = 0$. Furthermore only off-diagonal entries of r contribute to $\langle l, v\rangle$, since the diagonal ones are even integers. This equation has solutions unless $l_2 = 1$ and $l_i = 0$ for all $i > 3$ for which r has an off-diagonal entry.

The resulting factor in the recursion relation can now be computed as follows. If we ignore the existence of the auxiliary vector, one gets three solutions if $\langle l,l\rangle = 0 \bmod 4$ and one if $\langle l,l\rangle = 2 \bmod 4$. Hence the enhancement factor would then be $3I_0(n_0, n_1, n_A, n_B) + I_1(n_0, n_1, n_A, n_B)$. However, there does not exist an auxiliary vector for $l_1 = 0, l_2 = 1, l_i = 0$ if i belongs to one of the blocks of type A or B. The number of values of l for which there is no auxiliary vector, $I_0(n_0, n_1, 0, 0)$, has to be subtracted from the enhancement factor. For the recursion relation we find then finally

$$A(n_0, n_1, n_A+1, n_B) = [3I_0(n_0, n_1, n_A, n_B) + I_1(n_0, n_1, n_A, n_B) - I_0(n_0, n_1, 0, 0)] \cdot A(n_0, n_1, n_A, n_B).$$

In the rest of the discussion we distinguish two cases. If $n_1 \neq 0$ we may choose a basis so that $n_B = 0$ and $n_1 = 1$. By recursion in n_A we find then

$$A(n_0, 1, n_A, 0) = 2^{(2n_0+1)n_A} \prod_{l=0}^{n_A-1} 2^{2l}[2^{2l+2}-1] A(n_0, 1, 0, 0).$$

Recursion in n_0 is completely straightforward, and in no essential way different for $p = 2$ and p odd. The result is

$$A(n_0, 1, n_A, 0) = 2^{(1/2)n_0(n_0+1)+1} 2^{(2n_0+1)n_A} \prod_{l=0}^{n_A-1} 2^{2l}[2^{2l+2}-1]. \tag{4.43}$$

If $n_1 = 0$ we have to distinguish again two cases, $n_B = 0$ and $n_B = 1$. If $n_B = 0$ we perform exactly the same calculation as above, except that a different formula for I_0 and I_1 has to be used (see Appendix C). One easily derives now

$$A(n_0, 0, n_A, 0) = 2^{(1/2)n_0(n_0-1)} 2^{2n_0 n_A} \prod_{l=0}^{n_A-1} [2^{2l+1} + 2^l - 1] 2^{2l}. \tag{4.44}$$

To obtain $A(n_0, 0, n_A, 1)$ we add one block of the form $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ to r. The computation of this recursion step is essentially the same as that for adding a block $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, discussed in detail above. Now we find

$$A(n_0, 0, n_A, 1) = [3I_0(n_0, 0, n_A, 0) + I_1(n_0, 0, n_A, 0) - I_1(n_0, 0, 0, 0)] A(n_0, 0, n_A, 0).$$

(Note that $I_1(n_0, 0, 0, 0)$ vanishes, so that the auxiliary vector always exists in this case.) This yields, after substituting $A(n_0, 0, n_A, 0)$ and the results for I_0 and I_1 from Appendix C,

$$A(n_0, 0, n_A, 1) = 2^{2n_A + 2n_0} 2^{2n_0 n_A} 2^{(1/2)n_0(n_0-1)} (2^{n_A+1} + 1)(2^{n_A} + 1) \cdot \prod_{l=0}^{n_A-1} 2^{2l} (2^{2l+1} + 2^l - 1). \tag{4.45}$$

The Total Number of Modular Invariants. The derivation of the total number of invariants is now very similar to the one for odd p. The proof of conjecture (4.18) is analogous to the one for p even, and therefore we will only give details where there are differences. We begin with the cases $n_0 = n_1 = n_B = 0$. First of all we need to know what happens to the matrix r if we extend the algebra with one current. As for p odd, it is sufficient to compute the new r-matrix for just one of the possible extensions, since all currents are of type B. Choose for example the current J_1. If the algebra is extended by the current J_1, the current J_2 is projected out, and J_1 becomes part of the identity. Hence one 2×2 block of type A disappears, and n_A is reduced by 1.

We can now immediately write down a formula for the total number of invariants:

$$T(0, 0, n_A, 0) = \sum_{l=0}^{n_A} B_l(0, 0, n_A, 0) A(0, 0, n_A - l, 0),$$

where

$$B_l(0, 0, n_A, 0) = \prod_{m=0}^{n_A-1} \left(\frac{I_0(0, 0, n_A - m, 0) - 1}{2^{m+1} - 1} \right)^2$$

is the total number of extensions by $l + 1$ orbits. Just as for p odd we consider now

$$T(0, 0, n_A + 1, 0) - (1 + 2^{2n_A+1})(1 + 2^{2n_A}) T(0, 0, n_A, 0), \tag{4.46}$$

a quantity that we expect to be zero. Now one defines R_l as in (4.28) and (4.29) (with $N = 2n_A$, $T(N) \equiv T(0, 0, n_A, 0)$ and analogously for B_l) and solves the recursion for R_l. In this case the solution is

$$R_l = 2^{2n_A} [2^{2n_A+1} + 2^{n_A-l} + 1 - 2^{1-l}]. \tag{4.47}$$

After substituting the recursion (4.29) repeatedly into (4.46), we are finally left with

$$R_{n_A} - (1 + 2^{2n_A+1})(1 + 2^{2n_A})B_{n_A}(0, 0, n_A, 0) + B_{n_A+1}(0, 0, n_A + 1, 0), \quad (4.48)$$

which vanishes if one substitutes (4.47).

We repeat this computation for $n_0 = n_1 = 0$, $n_B = 1$. Again the effect of extending the chiral algebra is to reduce n_A by 1, so that there can be at most n_A extensions. The rest of the argument is exactly as before. We will just write down the solution to the recursion for R_l,

$$R_l = 2^{2n_A+2}[2^{2n_A+3} - 2^{n_A+1-l} + 1 - 2^{1-l}].$$

One may substitute this in the rest term, which has exactly the same form as (4.48) except for the fact that the last argument of B is 1 instead of 0.

To deal with the case $n_0 = 0$, $n_1 = 1$, $n_B = 0$ we repeat this entire computation once more. Again, the only essential difference is in the solution to the recursion relation for R_l, which is now

$$R_l = 2^{4n_A+3} + [2^{2-l}(2^{l-1} - 1)]2^{2n_A}.$$

Finally we have to allow non-zero values for n_0. This can be done in exactly the same way as for p odd (see Eqs. (4.34)–(4.41)). In this computation it is important that the formula for the number of automorphisms has the following universal dependence on n_0:

$$A(n_0, n_1, n_A, n_B) = 2^{n_0 N} 2^{(1/2)n_0(n_0-1)} A(0, n_1, n_A, n_B),$$

where $N = n_1 + 2n_A + 2n_B$. This formula may be verified in the explicit expressions (4.43), (4.44) and (4.45), but more directly it follows from (4.14), which holds for any p.

In all cases the rest term vanishes. This proves that our conjecture (4.18) holds for any prime number p.

5. Conclusions

We have classified all modular invariant partition functions that can be obtained with simple currents in any generic RCFT, except when the center contains subgroups $\mathbf{Z}_{p^n}$, $n \geqq 2$.

A remarkable result that has emerged from our analysis of $(\mathbf{Z}_p)^k$ is that the total number of invariants does not depend on the monodromy matrix r. It depends only on p and k in a universal way, despite the fact that the individual invariants are very r-dependent, and different for $p = 4m + 1$, $p = 4m - 1$ and $p = 2$, as well as for k odd and k even. It would be extremely interesting to know if this result is valid for any center, and what the generalization of formula (4.18) is. Unfortunately we do not have any insight in the origin of this universality. Our proof is based on detailed computations in which we had to distinguish many separate cases, and does not provide any deeper understanding of this phenomenon.

Applied to string theory, this result is a step towards the classification of all modular invariant partition functions of a given RCFT, and is a small part of a program to classify all string theories. Our results may be used for the systematic enumeration of subclasses of theories. For example in [17] and [18] partial listings of all simple current invariants of tensor products of $N=2$ minimal models were produced. We are now able to complete these lists (except for factors $\mathbf{Z}_{p^n}, n \geqq 2$) and be certain that nothing is missed, apart from "exceptional" invariants. The latter are, by definition, modular invariants in which some matrix elements of M_{ab} are non-vanishing even though a and b do not lie on the same orbit of any simple current.

It is clear from (4.18) that the number of modular invariants grows very rapidly with the number of $\mathbf{Z}_p$ factors of the center. In practical applications this may be somewhat unrealistic, since (4.18) is based on the assumption that all factors $\mathbf{Z}_p$ are distinct. If in fact they come from identical factors in a tensor product there will be many modular invariants that, though formally different, yield identical spectra. It would be quite useful to have a procedure to generate all distinct invariants modulo such interchange symmetries.

Our results apply to any center $\mathbf{Z}_{N_1} \times \cdots \times \mathbf{Z}_{N_k}$ as long as there are no subgroups $\mathbf{Z}_{p^n}$, with $n \geqq 2$. In the latter case our classification is incomplete, and we are faced with several additional technical problems: the monodromy matrix cannot always be diagonalized, not even for p odd, more classes for the conformal weights of the currents have to be distinguished, and, most importantly, we do not yet know in general which left-moving algebras can be combined with which right-moving ones. A related problem is that the group structure of subgroups of the center is no longer uniquely determined by the order of the subgroup. Nevertheless, we hope to complete this analysis in the future for any possible center.

Appendix A. Some Number Theoretic Results

Most of the results in this Appendix can be found in any good textbook on number theory, see for example [19].

The integer numbers modulo a prime number p fall into three classes: $0, \frac{1}{2}(p-1)$ numbers that are squares modulo p (quadratic residues), and $\frac{1}{2}(p-1)$ numbers that are not squares (quadratic non-residues). We will call these sets of numbers $\{0\}, \{1\}$ and $\{n\}$ respectively, and we will often refer to the numbers in the last two sets as "squares" and "non-squares" (note that 0 is not referred to as a square). A universal representative of the squares is 1. The non-squares, however, do not have a universal representative (for $p=2$ they do not even exist). For example, 2 is a square for $p=8m+1$ and $p=8m+7$, but it is a non-square for $p=8m+3$ and $p=8m+5$.

The product of two squares is a square, the product of two non-squares is a square, and the product of a square and a non-square is a non-square. Moreover, the product of the whole set of squares by a square (a non-square) yields the whole set of squares (non-squares).

For $p=4m+1$, $-\{1\}=\{1\}$ (the set of negative squares coincide with the set of squares), while for $p=4m-1$, $-\{1\}=\{n\}$. This is a non-trivial result first proved by Fermat. Many other proofs have been found since.

Defining the "addition" of two sets, $\{a\} * \{b\}$, as the addition of all the elements of $\{a\}$ with all the elements of $\{b\}$, one finds the following "addition" rules:

(a) For $p = 4m + 1$

$$\{0\} * \{a\} = \{a\}, \quad \text{for any set } \{a\},$$

$$\{1\} * \{1\} = \frac{p-1}{2}\{0\} + \frac{p-5}{4}\{1\} + \frac{p-1}{4}\{n\},$$

$$\{1\} * \{n\} = \frac{p-1}{4}\{1\} + \frac{p-1}{4}\{n\},$$

$$\{n\} * \{n\} = \frac{p-1}{2}\{0\} + \frac{p-1}{4}\{1\} + \frac{p-5}{4}\{n\}.$$

(b) For $p = 4m - 1$

$$\{0\} * \{a\} = \{a\}, \quad \text{for any set } \{a\},$$

$$\{1\} * \{1\} = \frac{p-3}{4}\{1\} + \frac{p+1}{4}\{n\},$$

$$\{1\} * \{n\} = \frac{p-1}{2}\{0\} + \frac{p-3}{4}\{1\} + \frac{p-3}{4}\{n\},$$

$$\{n\} * \{n\} = \frac{p+1}{4}\{1\} + \frac{p-3}{4}\{n\}.$$

Appendix B. Simplification of Monodromy Matrices

In this appendix we try to bring the monodromy matrix r in the simplest possible form by exploiting the freedom to choose the basic currents. We will only consider the case $(\mathbf{Z}_p)^k$, with p prime.

(A) $p > 2$. In this case r can be diagonalized by fairly standard methods. Start with the first row and column. We have to distinguish two cases.

(i) If $r_{11} \neq 0 \bmod p$ we can remove any non-zero entry $r_{1i} (= r_{i1})$ in the first row (and column) by replacing J_i by $J'_i = J_i J_1^{\alpha_i}$, obtaining the new matrix $r'_{ij} = pQ_{J'_j}(J'_i)$. We can always choose α_i so that $r'_{1i} = r_{1i} + \alpha_i r_{11} = 0 \bmod p$. This transformation is obviously invertible.

(ii) If $r_{11} = 0 \bmod p$ we begin by defining $J'_1 = J_1 J_j^{\alpha}$, where j is the first column with $r_{1j} \neq 0 \bmod p$ (if there is no such column the problem is already solved). Then

$$r'_{11} = 2\alpha r_{1j} + \alpha^2 r_{jj}.$$

If $p > 2$ this takes at least two different values, obtained by choosing $\alpha = 1$ and $\alpha = -1$. Hence there exists a choice for α so that $r'_{11} \neq 0 \bmod p$. Now we proceed as in case (i).

Obviously this process can be repeated for the other rows since the necessary transformations in dealing with the j^{th} row do not affect the zeroes on the previous rows. Thus we finally get a diagonal matrix r (we omit the primes from now on).

We may be able to simplify the matrix further by replacing, for some i, J_i by $(J_i)^\lambda$. This transformation is invertible if $\lambda \neq 0 \bmod p$. The effect of this transformation is to replace r_{ii} by $\lambda^2 r_{ii}$.

For $\lambda = 1, \ldots, p-1$, λ^2 takes $\frac{1}{2}(p-1)$ different values modulo p. To see why, suppose $\lambda^2 = (\lambda')^2 \bmod p$. Then $(\lambda - \lambda')(\lambda + \lambda') = 0 \bmod p$. Since p is prime the only solutions are $\lambda = \lambda' \bmod p$ and $\lambda = -\lambda' \bmod p$. Thus the squares of the first $\frac{1}{2}(p-1)$ values of λ all are different and they are repeated for the second $\frac{1}{2}(p-1)\lambda$-values.

The non-zero values of r_{ii} (which are always even) can be written as two times a square or two times a non-square. In either case we can choose a value for λ such that $\lambda^2 r_{ii}$ is equal to two times a fixed representative of the class $\{1\}$ or $\{n\}$ (see Appendix A). Thus the matrix r is characterized by three numbers: the number of values of $\frac{1}{2}r_{ii}$ belonging to $\{0\}, \{1\}$ and $\{n\}$ respectively. (Note that this is the $\mathbf{Z}_p$-equivalent of reducing a metric over the real numbers to a diagonal matrix with diagonal elements $0, 1$ or -1.)

There is still one further simplification possible: two non-squares can be changed simultaneously to two squares, or *vice versa.* Suppose we replace two basis currents J_1 and J_2 by $J'_1 = J_1 J_2^\alpha$ and $J'_2 = J_1 J_2^\beta$, with $\alpha \neq \beta$ so that this basis-transformation is invertible. To preserve diagonality we have to require

$$r'_{12} = r_{11} + r_{22}\alpha\beta = 0 \bmod p. \tag{B1}$$

The new diagonal matrix elements are

$$\begin{aligned} r'_{11} &= r_{11} + r_{22}\alpha^2, \\ r'_{22} &= r_{11} + r_{22}\beta^2. \end{aligned}$$

If $\frac{1}{2}r_{11} \in \{1\}$ and $\frac{1}{2}r_{22} \in \{1\}$ we may assume that both are equal to 1. There must exist an element α^2 of $\{1\}$ so that $1 + \alpha^2 \in \{n\}$, since otherwise it would follow that all $\frac{1}{2}(p-1)$ squares are consecutive numbers, with the last one equal to $p-1$ (if the largest number were $l < p-1$, $l+1$ would be a non-square). However, this set would not include the number 1. Thus we can arrange $\frac{1}{2}r'_{11}$ to be a non-square. Then (B1) can always be satisfied for some value of β, satisfying $\beta\alpha = -1$. Then $(1+\alpha^2)(1+\beta^2) = (\alpha - \beta)^2 \in \{s\}$. Since by construction the first factor is not a square, the second factor cannot be a square either. Hence $\frac{1}{2}r'_{22} \in \{n\}$.

There is only one remaining concern, and that is the condition $\alpha \neq \beta$. However, if $\alpha = \beta$ then $\alpha^2 = -1 \bmod p$, so that $\alpha^2 + 1 = 0 \notin \{n\}$, in contradiction with the above.

Hence we can convert any pair of squares into a pair of non-squares and vice-versa (by inverting this transformation). Thus the inequivalent matrices r are characterized by the number n_0 of diagonal elements equal to 0, the number n_1 of diagonal elements equal to 2 ($\in 2\{1\}$), and a number n_n, which is either zero or one, and which indicates the number of eigenvalues equal to some fixed representative $2n \in 2\{n\}$. By counting the number of currents of integer and fractional spin one can demonstrate that these matrices are indeed all inequivalent.

The set of simple currents divides into type A and B in the following way: all currents that lie entirely within the subspace with eigenvalue zero of r are of type

A, and all others are of type B. Examples of RCFT's for any of the allowed monodromy matrices can easily be constructed by tensoring $SU(p)$ Kac–Moody algebras.

(B) $p=2$. The r-matrices for $p=2$ have even integers defined modulo 4 on the diagonal, and off-diagonal elements equal to 0 or 1 (mod 2).

It is easy to check explicitly that if J_1 and J_i have $r_{1i}=1$, then no basis change within this system will remove this off-diagonal matrix element. Thus in general the r-matrix cannot be diagonalized.

However, suppose there is a third current J_j with $r_{1j}=r_{1i}=1$. Then define $J'_j=J_jJ_1^\alpha J_i^\beta$. One finds

$$r'_{1j}=r_{1j}+\beta r_{1i},$$
$$r'_{ij}=r_{ij}+\alpha r_{1i}.$$

Thus by choosing $\beta=1$ and $\alpha=r_{ij}$ we can decouple J'_j from the doublet J_1, J_i.

Proceeding in this way, we can combine all currents into doublets, by pairing each current that has not been paired yet with the first current that is non-local with respect to it. Any other current can be transformed to a current that is local with respect to the doublet. Thus the matrix r block-diagonalizes into 2×2 blocks, plus some diagonal entries corresponding to currents that are local with respect to all other currents. One can furthermore derive a basis transformation between the matrices

$$\begin{pmatrix}0&1\\1&0\end{pmatrix} \quad\text{and}\quad \begin{pmatrix}0&1\\1&2\end{pmatrix}.$$

Thus any matrix is characterized by the multiplicities of the following 2×2 and 1×1 blocks:

$$n_A:\begin{pmatrix}0&1\\1&0\end{pmatrix}$$
$$n_B:\begin{pmatrix}2&1\\1&2\end{pmatrix}$$
$$n_1:(2)$$
$$n_0:(0).$$

Further simplifications are possible. First of all, one may use

$$\begin{pmatrix}2&0\\0&2\end{pmatrix} \Leftrightarrow \begin{pmatrix}2&0\\0&0\end{pmatrix}$$

$(J'_2=J_1J_2)$ to reduce n_1 to zero or one. Secondly, one may use the equivalence

$$\begin{pmatrix}2&1&0\\1&2&0\\0&0&2\end{pmatrix} \Leftrightarrow \begin{pmatrix}0&1&0\\1&0&0\\0&0&2\end{pmatrix}$$

$(J'_1=J_1J_3$ and $J'_2=J_2J_3)$ to reduce n_B to zero if $n_1=1$. Finally, one can replace an even number of blocks of type B by the same number of blocks of type A using the equivalence

$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} \Leftrightarrow \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

obtained with a basis transformation $J'_1 = J_1 J_3$; $J'_2 = J_2 J_3$; $J'_3 = J_1 J_2 J_4$ and $J'_4 = J_1 J_2 J_3 J_4$. Thus n_B can be reduced to zero or one.

Thus the possible choices for the four numbers (n_0, n_1, n_A, n_B) are $(n_0, 0, n_A, 0)$, $(n_0, 0, n_A, 1)$ and $(n_0, 1, n_A, 0)$.

The type A currents are those that lie entirely within the subspace labelled by n_0 and n_1. All others are of type B. Explicit realizations for any of these monodromy matrices can be obtained for example by tensoring A_1 and D_n Kac–Moody algebras with various levels.

Appendix C. Formulas for the Number of Currents of Given Spin

Here we compute the quantities $I_a(n_0, n_1, n_n)$, $a = 0, 1, n$ and the analogous quantities for $p = 2$.

Let us start with p odd, and consider a general monodromy matrix

$$r = \mathrm{diag}(0^{n_0}, 2^{n_1}, (2n)^{n_n}).$$

For each current $[\vec{\alpha}]$ define

$$g([\vec{\alpha}]) = -ph([\vec{\alpha}]) = \sum_{ij} \frac{r_{ij}}{2} \alpha_i \alpha_j, \tag{C1}$$

where $h([\vec{\alpha}])$ is the conformal weight of $[\vec{\alpha}]$. Observe that for any current $[\lambda\vec{\alpha}]$ in the orbit of $[\vec{\alpha}]$, one has $g([\lambda\vec{\alpha}]) = \lambda^2 g([\vec{\alpha}])$. Since λ runs over all integers $\mathrm{mod}\, p$, and the product by a square does not change the square or non-square character of a number, the values of $g(\lambda[\vec{\alpha}])$ in an orbit will form either the set $p\{0\}$ or the set $\{0\} + 2\{s\}$, or $\{0\} + 2\{n\}$. This implies that the complete set $\{G\}$ of values of $g([\vec{\alpha}])$ for all simple currents can be divided into complete sets $\{0\}, \{1\}$ and $\{n\}$. Therefore we can write

$$\{G\} = I_0(n_0, n_1, n_n)\{0\} + I_1(n_0, n_1, n_n)\{1\} + I_n(n_0, n_1, n_n)\{n\}, \tag{C2}$$

where $I_a(n_0, n_1, n_n)$ denote the multiplicity of the set $\{a\}$ among the values of $g([\vec{\alpha}])$. These quantities can be computed using the following recursion method.

Suppose that the matrix r is enlarged with the addition of one zero on the diagonal. The new set of values of $g([\vec{\alpha}])$ is obtained by "adding" to the previous set the new p sets $\{0\}$, using the "$*$" operation defined in Appendix A. The result is

$$pI_0(n_0, n_1, n_n)\{0\} + pI_1(n_0, n_1, n_n)\{1\} + pI_n(n_0, n_1, n_n)\{n\} \tag{C3}$$

so that one obtains the recursion relation

$$I_a(n_0 + 1, n_1, n_n) = pI_a(n_0, n_1, n_n), \quad a = 0, 1, n. \tag{C4}$$

Similarly, by enlarging r with one 2 (or $2n$) on the diagonal, the new set of values of $g([\vec{\alpha}])$ is obtained by "adding" $\{0\}+2\{1\}$ (or $\{0\}+2\{n\}$) to the previous set. In this way one gets straightforwardly the recursion relations for $I_a(n_0, n_1+1, n_n)$ and $I_a(n_0, n_1, n_n+1)$, $a=0,1,n$. These relations are most easily solvable when two arguments are set to zero, giving the results:

(a) For n odd

$$\begin{aligned} I_0(0,n,0) &= I_0(0,0,n) = p^{n-1}, \\ I_1(0,n,0) &= I_n(0,0,n) = p^{n-1} + j^{(n-1)/2} p^{(n-1)/2}, \\ I_n(0,n,0) &= I_1(0,0,n) = p^{n-1} - j^{(n-1)/2} p^{(n-1)/2}. \end{aligned} \tag{C5}$$

(b) For n even

$$\begin{aligned} I_0(0,n,0) &= I_0(0,0,n) = p^{n-1} + j^{n/2} p^{(n/2)-1}(p-1), \\ I_1(0,n,0) &= I_1(0,0,n) = p^{n-1} - j^{n/2} p^{(n/2)-1}, \\ I_n(0,n,0) &= I_n(0,0,n) = p^{n-1} - j^{n/2} p^{(n/2)-1}, \end{aligned} \tag{C6}$$

where $j=\pm 1$, corresponding to $p=4m+j$.

To obtain $I_a(0, n_1, n_n)$ one simply computes

$$\begin{aligned} &[I_0(0,n_1,0)\{0\} + I_1(0,n_1,0)\{1\} + I_n(0,n_1,0)\{n\}] \\ &*[I_0(0,0,n_n)\{0\} + I_1(0,0,n_n)\{1\} + I_n(0,0,n_n)\{n\}]. \end{aligned}$$

Using the results (C5) and (C6) one obtains, with $\varepsilon = (-1)^{n_1}$:

(a) For $N = n_1 + n_n$ odd,

$$\begin{aligned} I_0(0,n_1,n_n) &= p^{N-1}, \\ I_1(0,n_1,n_n) &= p^{N-1} - j^{(N-1)/2} \varepsilon p^{(N-1)/2}, \\ I_n(0,n_1,n_n) &= p^{N-1} + j^{(N-1)/2} \varepsilon p^{(N-1)/2}. \end{aligned} \tag{C7}$$

(b) For N even,

$$\begin{aligned} I_0(0,n_1,n_n) &= p^{N-1} + j^{N/2} \varepsilon (p-1) p^{(N/2)-1}, \\ I_1(0,n_1,n_n) &= p^{N-1} - j^{N/2} \varepsilon p^{(N/2)-1}, \\ I_n(0,n_1,n_n) &= p^{N-1} - j^{N/2} \varepsilon p^{(N/2)-1}. \end{aligned} \tag{C8}$$

Finally, applying the recursion relation for the first argument, Eq. (C4), one gets

$$I_a(n_0, n_1, n_n) = p^{n_0} I_a(0, n_1, n_n), \quad a=0,1,n. \tag{C9}$$

For $p=2$ we have to repeat these computations. There are no subtleties worth mentioning, and we simply list the results. For $n_1 \neq 0$ we get

$$I_0(n_0, n_1, n_A, n_B) = I_1(n_0, n_1, n_A, n_B) = 2^{k-1},$$

where $k = n_0 + n_1 + 2n_A + 2n_B$. If $n_1 = 0$ the answer is slightly more complicated,

$$\begin{aligned} I_0(n_0, 0, n_A, n_B) &= 2^{n_0-1}[2^{2(n_A+n_B)} + (-1)^{n_B} 2^{n_A+n_B}], \\ I_1(n_0, 0, n_A, n_B) &= 2^{n_0-1}[2^{2(n_A+n_B)} - (-1)^{n_B} 2^{n_A+n_B}]. \end{aligned}$$

Appendix D. Fixed Points

In this appendix we discuss a variety of problems that arise when simple currents with fixed points are present. We begin with a useful result that rules out fixed points in some cases.

Theorem. *Only type A currents can have fixed points.*

Proof. Suppose f is a fixed point of a simple current J, $Jf = f$. Let K be any other simple current in the theory. Then $Kf = g$, and $Jg = JKf = KJf = Kf = g$, so that g is also a fixed point of J. The charge of a fixed-point field satisfies $h(f) = h(Jf) = h(f) + h(J) - Q_J(f) \bmod 1$, so that $Q_J(f) = h(J) \bmod 1$. Hence $Q_J(f) = Q_J(g) = h(J) \bmod 1$. This implies that $Q_J(f) = Q_J(Kf) = Q_J(K) + Q_J(f) \bmod 1$, or $Q_K(J) = 0 \bmod 1$.

Remarkably, for Kac–Moody algebras the correspondence between type A currents and the presence of fixed points is in fact one-to-one: *every* type A current has fixed points. All simple currents of these theories have been classified in [20]. All their fixed points have been classified in [15]. By inspection, every type A simple current in these theories has a fixed point. It is not clear, however, whether this is a general property of type A currents in any conformal field theory.

According to the theorem proved in Sect. 2, a current that is local with respect to any other current must appear in both the left and the right algebra (or in neither). Hence if b is a fixed point with respect to one or more currents in $\mathscr{A}_R$, and if $M_{ab} \neq 0$, then a (which differs from b only by the action of some simple currents) is a fixed point with respect to the same currents in $\mathscr{A}_L$.

The Matrix U. Now we will give the precise definition of the matrix U mentioned in Sect. 2. Consider the complete set of simple current monodromy charges $\mathscr{Q}$. For each set of integer spin simple currents $\mathscr{A}$ that closes under fusion we can define an equivalence relation among the elements $\vec{q}$ of $\mathscr{Q}$: $\vec{q}_1 \sim \vec{q}_2$ if $\mathscr{A} \cdot \vec{q}_1 = \mathscr{A} \cdot \vec{q}_2 \bmod 1$ (as in Sect. 2 this means that this equality should hold for all currents in $\mathscr{A}$.) If $\mathscr{A}$ has a group structure $(\mathbf{Z}_p)^l$ there are p^l equivalence classes, characterized by a set of charges $\frac{q_1}{p}, \ldots, \frac{q_l}{p}$, $0 \leqq q_i < p$ with respect to a current basis $J_1, \ldots, J_l$. In each of these classes we choose a set of representatives $\mathscr{Q}(\mathscr{A})$.

Now consider a chiral algebra $\mathscr{A}$ and field a. We can define an equivalence relation among the currents J_i in $\mathscr{A}$ in the following way: $J_1 \sim J_2$ if $J_1 a = J_2 a$. One can choose representatives of the resulting equivalence classes in such a way that they form a closed set $\mathscr{A}_a$ under fusion. This can be done as follows. For the identity class (whose elements satisfy $Ja = a$) one chooses the identity as a representative. If there are other equivalence classes, choose one of them, and choose an arbitrary representative J_1. The orbit of this representative fixes the choice of representative $(J_1)^n$ of the corresponding equivalence classes. Then choose an arbitrary representative J_2 in one of the remaining classes (if any). In theories with a center $(\mathbf{Z}_p)^k$ the products $(J_1)^n (J_2)^m$, $0 \leqq n, m < p$ are all different and fix a choice of representatives in the corresponding classes. One can continue this process until all representatives have been fixed. By construction the set of representatives closes under fusion. Obviously the choice of representatives is not unique.

For each such set $\mathscr{A}_a$ there is a corresponding subset of charges $\mathscr{Q}(\mathscr{A}_a)$. This set of charges has precisely as many elements as there are distinct fields in the orbit of a. The matrix U is now defined as follows

$$U(\vec{q},[\vec{\alpha}])_{ab} = \frac{1}{\sqrt{N_a}} e^{2\pi i \vec{q}\cdot\vec{\alpha}} \delta_{ab}, \tag{D1}$$

where $[\vec{\alpha}] \in \mathscr{A}_a$, $\vec{q} \in \mathscr{Q}(\mathscr{A}_a)$, a and b label different $\mathscr{A}$ orbits, and N_a is the number of fields in the $\mathscr{A}$-orbit of a. This matrix is essentially independent of the choices of class representatives. The choice of $\vec{q}$ is irrelevant since different choices yield by definition the same phases in (D1) (up to integers), and any choice of the representatives of $\mathscr{A}_a$ leads to isomorphic subgroups of the center, which produces the same set of charges, up to permutation.

The characters $\hat{\mathscr{X}}$ defined in (2.5) can be obtained by means of the "Fourier transformation"

$$\hat{\mathscr{X}}_a(\vec{q}) = \sqrt{N} \sum_b \sum_{\alpha \in \mathscr{A}}^{N_b} U(\vec{q},[\vec{\alpha}])_{ab} \mathscr{X}_{[\vec{\alpha}]b}.$$

By restricting to the subspace with $\vec{q} = 0$ and to fields a that are local with respect to the algebra $\mathscr{A}$ one obtains the new characters (note that $\vec{q}$ should not be confused with the charge of the field a).

Fixed-Point Entries of M. Now we will prove that the non-vanishing matrix elements of M must all have the same value on each orbit generated by the left and right algebras, even on fixed-point orbits. For fields that are not fixed points it was shown in Sect. 2 that M_{ab} can only be zero or one. The argument was based on the observation that for any field a with $\mathscr{A}_L \cdot \vec{Q}(a) = 0$ the sum $\sum_b M_{ab}$ must be equal to the number of currents N in the algebra, whereas on the other hand the number of non-zero entries on the a^{th} row must also be equal to the number of currents because of the closure condition.

This argument does not hold if b is a fixed point of one of the currents of the right algebra. In that case the sum over the corresponding row and column must still be equal to N, but the number of entries that is required to be non-zero is smaller (and equal to a divisor of N). This leaves two possibilities open which we would like to rule out. First of all a row (or a column) of N could contain entries related by a simple current outside the right (or left) algebra. For example, suppose one has a theory with a center $\mathbf{Z}_2 \times \mathbf{Z}_2$ and integer spin currents J_1 and J_2. Suppose J_1 has two fixed points a and b connected by J_2: $J_1 a = a$, $J_1 b = b$, $J_2 a = b$, $J_2 b = a$. If we extend the algebra with J_1, the "standard" form of M on the subspace of the fields a and b is $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$. However, the rules derived in Sect. 2 would also allow the solution $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ on this subspace.

The second possibility we wish to rule out is that N is distributed unevenly over the entries of M for fields that are fixed points of only a subset of the currents in the algebra. In the foregoing example, suppose we extend the algebra by both

J_1 and J_2. The standard form of M on the same subspace is now $\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$, but the arguments of Sect. 2 would also allow $\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$ or $\begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix}$.

We will first show that the sum $\sum_b M_{ab}$ must be distributed *within* the right algebra, i.e.

Theorem. *If a is a fixed point* w.r.t. *one or more currents in $\mathscr{A}_L$,* with $M_{ab} \neq 0$ *and $M_{a,Kb} \neq 0$ for some simple current K, then $K \in \mathscr{A}_R$.*

Proof. According to the regularity condition formulated in the introduction, for any charge $\vec{Q}$ there exists a field c that is not a fixed point of any integer spin current. Thus in particular there exists such a field for all charges $\vec{Q}(c)$ satisfying $\mathscr{A}_R \cdot \vec{Q}(c) = 0$, i.e. all charges of representations of $\mathscr{A}_R$. Since c is not a fixed point, the corresponding column of M is given by the results of Sect. 2. Now we may use (2.1) to get

$$\begin{aligned} \sum_{[\vec{\alpha}]} M_{a,[\vec{\alpha}]a} e^{2\pi i \vec{\alpha} \cdot \vec{Q}(c)} &= \sum_{[\vec{\gamma}]} e^{2\pi i \vec{\gamma} \cdot \vec{Q}(a)} M_{[\vec{\gamma}]c,c} \\ &= e^{2\pi i \vec{\gamma}_0 \cdot \vec{Q}(a)} \sum_{[\vec{\gamma}_L] \in \mathscr{A}_L} M_{[\vec{\gamma}_0 + \vec{\gamma}_L]c,c} \\ &= e^{2\pi i \vec{\gamma}_0 \cdot \vec{Q}(a)} N_L . \end{aligned} \tag{D2}$$

Here $\vec{\gamma}_0$ is an overall shift of the orbit corresponding to a possible fusion rule automorphism. We see thus that the absolute value of the left-hand side of (D2) must be equal to N_L. This is only possible if all terms in the sum on the right-hand side of (D2) add coherently, since we know that $\sum_b M_{ab} = N_L$, and any relative phases can only lower the absolute value of the sum. Thus all phases must be the same, and hence $\vec{\alpha}_1 \cdot \vec{Q}(c) = \vec{\alpha}_2 \cdot \vec{Q}(c) \mod 1$ if $M_{a,[\vec{\alpha}_1]a} \neq 0$ and $M_{a,[\vec{\alpha}_2]a} \neq 0$. Hence the current $[\vec{\alpha}_1 - \vec{\alpha}_2]$ is local with respect to all fields in the right-moving sector, and therefore it belongs to $\mathscr{A}_R$.

Note that we only have equations like (D2) if $S_{ac} \neq 0$. The regularity condition guarantees that we get sufficiently many equations to constrain $\vec{\alpha}_1 - \vec{\alpha}_2$. It implies that there exist fields c with $S_{ac} \neq 0$, except when a is a fixed point w.r.t. some current, and c has a charge with respect to that current. If a is a fixed point of some current J, the charges of the fields c with $S_{ac} \neq 0$ cannot span the entire set of allowed charges, and hence the difference $\alpha_1 - \alpha_2$ is not restricted to lie within $\mathscr{A}_R$. However, it can move outside of $\mathscr{A}_R$ only by multiples of currents J that fix a, which is clearly irrelevant.

Finally we prove:

Theorem. *Suppose $\mathscr{A}_R$ has $N_R = N_L$ simple currents, and generates an orbit of N_a different fields when acting on some field a. Then the non-vanishing matrix elements M_{ab} must be equal to $\frac{N_R}{N_a}$.*

Proof. According to the previous theorem, the non-vanishing matrix elements M_{ab} occur only for b's of the form $b = [\vec{\alpha}_0 + \vec{\alpha}]a$, with $[\vec{\alpha}] \in \mathscr{A}_R$, where α_0 is some fixed vector that depends on a. The complete set of conditions on the matrix elements is

$$\sum_{[\vec{\alpha}]\in\mathscr{A}_R}^{N_a} M_{a,[\vec{\alpha}_0+\vec{\alpha}]a}\, e^{2\pi i(\vec{\alpha}_0+\vec{\alpha})\cdot\vec{Q}(c)} = e^{2\pi i\vec{\gamma}_0\cdot\vec{Q}(a)} N_L, \tag{D3}$$

if $\mathscr{A}_R\cdot\vec{Q}(c)=0$ (this condition follows from (D2)), and

$$\sum_{[\vec{\alpha}]\in\mathscr{A}_R}^{N_a} M_{a,[\vec{\alpha}_0+\vec{\alpha}]a}\, e^{2\pi i(\vec{\alpha}_0+\vec{\alpha})\cdot\vec{Q}(c)} = 0, \tag{D4}$$

if $\mathscr{A}_R\cdot\vec{Q}(c)\neq 0$ and $S_{ac}\neq 0$. The upper limit N_a on the sums indicates that one should only sum over the distinct fields generated by $\mathscr{A}_R$, i.e. the action of currents for which a is a fixed point must be omitted. Earlier in this appendix, in the description of the matrix U, we have shown that one can choose the N_a currents $[\alpha]$ in such a way that they form a set $\mathscr{A}_{R,a}$ that closes under fusion. Since $\vec{\alpha}\cdot\vec{Q}(c)=0$ in condition (D3), the overall phases must be the same: $\vec{\alpha}_0\cdot\vec{Q}(c)=\vec{\gamma}_0\cdot\vec{Q}(a) \bmod 1$.

The two conditions (D3) and (D4) can now be combined as follows

$$\sum_{[\vec{\alpha}]\in\mathscr{A}_{R,a}} M_{a,[\vec{\alpha}_0+\vec{\alpha}]a}\, e^{2\pi i\vec{\alpha}\cdot\vec{Q}(c)} = N_L\delta(\mathscr{A}_R\cdot\vec{Q}(c)), \quad \text{for all } c \text{ with } S_{ac}\neq 0, \tag{D5}$$

where $\delta(\mathscr{A}_R\cdot\vec{Q}(c))=1$ if the argument vanishes for all currents in $\mathscr{A}_R$, and equal to zero otherwise.

This yields an equation for the N_a unknown quantities $M_{a,[\vec{\alpha}_0+\vec{\alpha}]a}$ for each value of $\vec{Q}(c)$ for which one can find a field with $S_{ac}\neq 0$. Obviously not all these equations are independent. The maximal set of independent ones is precisely characterized by the N_a charges in the set $\mathscr{Q}(\mathscr{A}_{R,a})$. The regularity condition guarantees that there exists at least one equation for each such charge. Hence we may write (D5) as

$$\sum_{[\vec{\alpha}]\in\mathscr{A}_{R,a}} M_{a,[\vec{\alpha}_0+\vec{\alpha}]a}\sqrt{N_a}\,U(\vec{q},\vec{\alpha})_{aa} = N_L\delta(\mathscr{A}_R\cdot\vec{q}), \quad \vec{q}\in\mathscr{Q}(\mathscr{A}_{R,a}), \tag{D6}$$

using one block of the matrix U defined above. Note that $\delta(\mathscr{A}_R\cdot\vec{q})=1$ if $\vec{q}=0$ and vanishes otherwise. On the left-hand side M is transformed by a unitary $N_a\times N_a$ matrix, and hence the equations have a *unique* solution:

$$M_{a,[\vec{\alpha}_0+\vec{\alpha}]a} = \frac{N_L}{N_a}. \tag{D7}$$

The Regularity Condition. Here we would like to identify some theories that satisfy the regularity condition described in the introduction. There is a large class of theories where this condition is automatically satisfied, namely all theories that do not have currents of type A. Type B currents cannot have fixed points, and furthermore they have charges with respect to themselves and/or each other. The analysis of the monodromy matrices in Appendix B shows that these currents, J, provide a complete set of charges. Furthermore their matrix elements S_{J_a} with a field a are always equal, up to a phase, to S_{0a}, which never vanishes. Hence the type B currents themselves can play the rôle of the fields referred to in the regularity condition.

A second important fact is that the regularity condition is not affected by tensoring or by extending the chiral algebra by integer spin simple currents. The former is obvious, and the latter is true because after extension of the algebra all fields of a given charge are either projected out, or absorbed into representations of the extended algebra, between which S has the same matrix elements up to normalization. Furthermore fields that were not fixed points of any current before extension cannot become fixed points after extension of the algebra. An immediate consequence is that the regularity condition holds for coset theories if it holds for the Kac–Moody algebras used in the construction of these coset theories: coset theories with field identifications can be thought of, for purposes related to modular invariance and the fusion algebra, as tensor products with an extension of the algebra.[4]

Hence a very large set of theories is automatically included if we verify the regularity condition for Kac–Moody algebras (of course only those with type A currents have to be examined). It is straightforward to verify whether for any charge there is a field that is not a fixed point, but analyzing the matrix elements of S is harder. By inspection, we found that it holds for all Kac–Moody algebras of sufficiently low rank and level, except B_n level 1 and D_{2n} level 2. The number of fields that satisfy the regularity condition grows rapidly with the rank and the level, so that it is unlikely that any pathologies have been overlooked.

The theories that do not satisfy the regularity condition do indeed display some irregular behavior. First of all one finds that some invariants expected to be distinct are in fact identical. More importantly, some of these theories have additional invariants not included in our classification (however, these invariants are unlikely to correspond to meaningful conformal field theories).

This shows that the regularity condition cannot be dropped altogether. However, it can certainly be weakened without affecting the results. For example, it is not necessary that *all* matrix elements of S mentioned in it are non-zero. It is sufficient that for every complete set of charges there exists a set of fields Φ_0 which are not fixed points, and with the property that the series $\Phi_0 \subset \Phi_1 \subset \cdots \subset \Phi_i \subset \cdots$ converges to the complete set of fields. Here Φ_i is defined recursively: Φ_{i+1} consists of all fields in Φ_i, plus all fields b that are linked by non-vanishing matrix elements of S to a complete set of charges in Φ_i (if b is a fixed point of some currents, it has to be linked to the maximally allowed subspace of the charges). The regularity condition corresponds to the much stronger requirement that already Φ_1 is equal to the complete set of fields. Obviously also with the weaker condition the action of the currents on the fields in Φ_0 determine the action on the rest of the theory completely. Although we have not encountered situations where the weaker condition is satisfied, and the stronger one is not, it might be useful to keep it in mind. The requirement that for every charge there should be a field that is not a fixed point can presumably be weakened as well, but attempts in that direction tend to lead to very complicated conditions.

Acknowledgements. We thank Luis Alvarez-Gaumé for conversations on Number Theory. B. G.-R. acknowledges the "Fundación Banco Exterior" (Spain) for financial support. The algebraic program FORM by Jos Vermaseren has been used to check some of the algebra.

[4] Here we only consider simple currents that originate from those of the KM-algebra. In rare cases there may be extra simple currents coming from resolved fixed points, which require a separate discussion

References

1. Cappelli, A., Itzykson, C., Zuber, J.-B.: Nucl. Phys. **B280**, 445 (1987); Commun. Math. Phys. **113**, 1 (1987)
2. Schellekens, A. N., Yankielowicz, S.: Nucl. Phys. **B327**, 673 (1989); Phys. Lett. **B227**, 387 (1989)
3. Bernard, D.: Nucl. Phys. **B288**, 628 (1987)
4. Altschuler, D., Lacki, J., Zaugg, P.: Phys. Lett. **B205**, 281 (1988)
5. Felder, G., Gawedzki, K., Kupiainen, A.: Commun. Math. Phys. **117**, 127 (1988)
6. Itzykson, C.: Proceedings of the Annecy workshop on Conformal Field Theory. Nucl. Phys. (Proc. Suppl), **5B**, 150 (1988)
7. Ahn, C., Walton, M.: Phys. Lett. **B223**, 343 (1989)
8. Gato-Rivera, B., Schellekens, A. N.: Nucl. Phys. **B353**, 519 (1991)
9. Dijkgraaf, R., Verlinde, E.: Nucl. Phys. (Proc. Suppl.) **5B**, 87 (1988)
10. Intriligator, K.: Nucl. Phys. **B332**, 541 (1990)
11. Schellekens, A. N.: Phys. Lett. **B244**, 255 (1990)
12. Moore, G., Seiberg, N.: Nucl. Phys. **B313**, 16 (1988)
13. Brustein, R., Yankielowicz, S., Zuber, J.-B.: Nucl. Phys. **B313**, 321 (1989)
14. Schellekens, A. N., Yankielowicz, S.: Nucl. Phys. **B334**, 67 (1990)
15. Schellekens, A. N., Yankielowicz, S.: Int. J. Mod. Phys. **A5**, 2903 (1990)
16. Schellekens, A. N.: Phys. Lett. **B237**, 363 (1990)
17. Schellekens, A. N., Yankielowicz, S.: Nucl. Phys. **B330**, 103 (1990); Tables Supplement CERN-TH.5440T/89 (1989) (unpublished)
18. Fuchs, J., Klemm, A., Scheich, C., Schmidt, M.: Phys. Lett. **B232**, 317 (1989); Ann. Phys. **204**, 1 (1990)
19. Ireland, K., Rosen, M.: A classical introduction to modern number theory. Berlin, Heidelberg, New York: Springer 1990
20. Fuchs, J.: Commun. Math. Phys. **136**, 345 (1991)

Communicated by K. Gawedzki