Commun. Math. Phys. 133, 181–196 (1990)

Communications in
Mathematical
Physics

Dimension of the Commutant for the $SU(N)$ Affine Algebras

Ph. Ruelle[*,**]

Institut de Physique Théorique, Université Catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium

Received December 10, 1989

Abstract. Explicit formulae are obtained, giving the number of independent matrices which commute with the matrices S and T describing the modular transformations of the $SU(N)$ affine characters.

I. Introduction

In the context of rational conformal field theories, the construction and the classification of modular invariants remains one of the major problems. In a statistical mechanics language, this corresponds to the classification of all fixed-points of the renormalization group in two dimensions.

As the Wess-Zumino-Witten models are thought to be the building blocks in the construction of RCFT's, much attention has been focused on their modular invariants. But although many such invariants are known [1], there is so far no exhaustive list, except in the cases $SU(2)$ [2] and $SU(N)$ at level 1 [3].

Affine modular invariants are sesquilinear forms in the affine characters

$$Z(\tau,\tau^*)=\Sigma\,[\chi_\lambda(\tau)]^*\,N_{\lambda\lambda'}\,[\chi_{\lambda'}(\tau)]\ ,$$

where the coefficients $N_{\lambda\lambda'}$ are subject to appropriate conditions to make $Z(\tau,\tau^*)$ a partition function [2].

For the affine $SU(N)$ algebras, a systematic approach has been initiated by Bauer and Itzykson [4]. They have given a description of the commutant of the (extended) modular transformations carried by the characters. Indeed the modular invariance of $Z(\tau,\tau^*)$ requires that the matrix $N_{\lambda\lambda'}$ belongs to this commutant.

Within the strategy adopted in [2] which led to the ADE classification for the $SU(2)$ invariants, finding the commutant is the first step in the classification program. An interesting alternative is the study of $SU(N)$ lattice integrable models

[*] Chercheur IISN

[**] Address after October 1: Dublin Institute for Advanced Studies, Dublin, Ireland

[5]. The authors of [4] succeeded in finding a basis of the commutant, abstractly written in terms of finite quantum mechanics operators. The description they gave allowed them to compute the dimension of the commutant only in the $SU(2)$ and $SU(3)$ cases.

It is the purpose of this article to provide explicit formulae for the dimension of the commutant for any $SU(N)$, at any level. The method relies on the main result of [4], which states, among other things, that the dimension of the commutant is given by the number of orbits of $SL(2,\mathbb{Z})$ acting on the set $G_n \times G_n = [Z_n^{N-2} \times Z_{nN}]^2$ (there is a minor change in case N is even and $n = N+k$), and on the extensive use of a theorem in group theory, relating the number of orbits to the mean number of fixed-points of $SL(2,\mathbb{Z})$ in $G_n \times G_n$.

The results are too long to be written down here, but most of them are summarized in Eqs. (3.3), (3.14), and (4.4). Only for $SU(2)$ and $SU(3)$ are the answers simple. The general feature is that the dimension of the commutant for $SU(N)$ is a function which grows very rapidly as n^{2N-5}, for large N and n. Section 2 consists of a summary of the main features of the $SU(N)$ characters, includes those results of [4] that are needed here and explains how a solution can be obtained. Sections 3 and 4 establish the final result for the dimension of the commutant.

II. $SU(N)$ Affine Characters

The $SU(N)$ affine algebras at level k have a finite number of unitary integrable representations $[\lambda_i]$ labelled by highest weights of representations of the finite underlying $SU(N)$ algebra [6]. The admissible λ's are those for which the condition $\psi \cdot \lambda \leqq k$ is fulfilled, where ψ is the highest root. From this constraint, one finds that the number of affine representations is equal to $\binom{N+k-1}{N-1} = \binom{n-1}{N-1}$. (For what follows it is easier to define the height $n = N+k =$ dual Coxeter number + level.)

Each affine representation contains an infinite number of states, which are (partially) organized according to their L_0 eigenvalue. The low-lying states transform in the (finite) representation specified by the weight λ and they have an L_0 eigenvalue equal to $h_\lambda = C_2(\lambda)/2n$, with $C_2(\lambda)$ the quadratic Casimir in the representation λ. For $q = \exp(2i\pi\tau) = e(\tau)$, $\operatorname{Im}\tau > 0$, the restricted affine characters are [7]

$$\chi_\lambda(\tau) = q^{-k(N^2-1)/24n}\,\mathrm{Tr}_{[\lambda]}\, q^{L_0}$$

$$= [\eta(\tau)]^{1-N^2} \sum_{t \in M} \left(\prod_{\alpha>0} \frac{(\alpha \cdot (\lambda+\varrho+nt))}{(\alpha \cdot \varrho)} \right) q^{(\lambda+\varrho+nt)^2/2n}\,. \tag{2.1}$$

In Eq. (2.1), α runs over all the positive roots of $SU(N)$, ϱ is half the sum of the positive roots ($\varrho = (1, \ldots, 1)$ in Dynkin components), M is the root lattice of $SU(N)$ and $\eta(\tau) = q^{1/24} \prod_{n \geqq 1} (1-q^n)$ is the Dedekind eta-function. All scalar products are performed with the weight space metric. As is suggested by Eq. (2.1), the characters are more easily described in terms of $p = \varrho + \lambda$; also the characters will be noted χ_p, defined by Eq. (2.1) with $\varrho + \lambda$ replaced by p.

The modular transformations of the characters (2.1) can be calculated with the help of the Poisson summation formula,

$$\chi_p(-1/\tau)=\sum_{p'} S_{pp'}\chi_{p'}(\tau)\ ; \qquad \chi_p(\tau+1)=\sum_{p'} T_{pp'}\chi_{p'}(\tau)\ ,$$

$$S_{pp'}=\frac{i^{N(N-1)/2}}{(Nn^{N-1})^{1/2}}\sum_{w\in W}(\det w)\left(-\frac{p\cdot w(p')}{n}\right)\,, \tag{2.2}$$

$$T_{pp'}=e\left(\frac{p^2}{2n}-\frac{N^2-1}{24}\right)\delta_{p,p'}\ . \tag{2.3}$$

In Eqs. (2.2–3), the sum on p' runs over the fundamental domain $B_n=\{p\in M^*\colon p_i\geqq 1$ and $p\cdot\psi\leqq n-1\}$. $W=S_N$ is the Weyl group of $SU(N)$. Since the two transformations $S(\tau)=-1/\tau$ and $T(\tau)=\tau+1$, satisfying $S^2=(ST)^3=1$, generate the whole modular group, Eqs. (2.2–3) define a unitary representation of $PSL(2,\mathbb{Z})$. As a function on the weight space M^*, χ_p has the periodicity property $\chi_{p+nt}=\chi_p$ for any root t in the root lattice M. Moreover when p is subjected to a Weyl transformation w, one verifies the transformation $\chi_{w(p)}=(\det w)\chi_p$, already used to derive Eq. (2.2).

As a result of these properties, instead of considering the $\binom{n-1}{N-1}$ linearly independent characters χ_p with p in B_n, one may look at a larger set of characters, namely those χ_p's for p in M^*/nM. With this extended definition, there are now Nn^{N-1} characters which are no longer linearly independent. Some of these are identically zero, due to the antisymmetry under the Weyl group. For instance, $\chi_{p=0}(\tau)=0$.

Under modular transformations, this set of characters transform in an extended unitary representation of dimension Nn^{N-1} specified by the two matrices [it is now a unitary representation of $SL(2,\mathbb{Z})$]

$$S_{pp'}=\frac{i^{N(N-1)/2}}{(Nn^{N-1})^{1/2}}\cdot e\left(-\frac{p\cdot p'}{n}\right)\,, \tag{2.4}$$

$$T_{pp'}=e\left(\frac{p^2}{2n}-\frac{N^2-1}{24}\right)\delta_{p,p'}\ , \tag{2.5}$$

for p and p' in M^*/nM. The matrix in Eq. (2.4) is just the matrix of the Fourier transform on the additive group M^*/nM.

To compute the commutant of the extended representation carried by the characters amounts to look for all the matrices which commute with the matrices S and T of Eq. (2.4–5). Its dimension is the number of matrices which are linearly independent (over $\mathbb{Q}$) and which commute with S and T. Of course the problem originates in the fact that they must commute with S and T. It is instructive to give estimates of the dimensions of the commutant of S and T, considered separately. This is much simpler since the dimension of the commutant of a diagonalizable matrix is equal to the sum of the squared degeneracies of its eigenvalues. For simplicity, let us take N and n two different odd primes. Since S in Eq. (2.4) is a Fourier transform, it has ± 1, $\pm i$ as eigenvalues. By computing $\operatorname{Tr} S$ (it is a quadratic Gauss' sum) and $\operatorname{Tr} S^2$, one finds that the degeneracies of the four eigenvalues are approximately equal [8].

Therefore a rough estimate is

$$\text{dimension of the commutant of } S \sim N^2 n^{2N-2} \ . \tag{2.6}$$

The eigenvalues of T are explicit in Eq. (2.5), but counting their multiplicity requires knowing the number of p's in M^*/nM that give $Np \cdot p$ the same value mod $2nN$. (Due to the metric, $p \cdot p$ is not an integer but a multiple of $1/N$ instead.) This can be solved by using first the equivalence of any quadratic form with a diagonalized one, a theorem valid on finite fields of characteristic different from 2 [9], and then using standard number theoretic techniques to evaluate how many times such a diagonal quadratic form takes the same value in the congruence ring [10]. The outcome is the following asymptotic behaviour

$$\text{dimension of the commutant of } T \sim N n^{2N-3} \ , \tag{2.7}$$

so that the commutation with T is a more stringent constraint than the commutation with S.

Let $Z_m^{(\text{even})}$ denote the additive group of (even) residues mod m. Concerning the dimension of the commutant (of S and T), the authors of [4] have obtained the following result: for $SU(N)$ at height n, the dimension of the commutant is equal to the number of orbits of $SL(2,\mathbb{Z})$ acting on $G_n \times G_n$, where $G_n = Z_n^{N-2} \times Z_{nN}$ in case N is odd, while $G_n = Z_n^{N-2} \times Z_{nN}^{(\text{even})}$ in case N is even. If x and x' belong to G_n and if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is in $SL(2,\mathbb{Z})$, the action of $SL(2,\mathbb{Z})$ is

$$(x, x') \to (x, x') \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ax + cx', bx + dx')$$

and the multiplication of x, x' by the integers a, b, c, d is componentwise. (x and x' are to be thought of as vectors with $N-1$ components.)

Using the prime decomposition of n and N, the action of $SL(2,\mathbb{Z})$ can be accordingly factorized.

Let us suppose that $N = \prod_p p^{\alpha(p)}$ and $n = \prod_p p^{\gamma(p)}$. Let us also define a parameter $\varepsilon(p)$, equal to 1 if N is even and if p is 2, and equal to 0 otherwise. The group G_n factorizes as

$$G_n = \prod_p \{ Z_{p^{\gamma(p)}}^{N-2} \times Z_{p^{\gamma(p)+\alpha(p)-\varepsilon(p)}} \} \ , \tag{2.8}$$

so that one can write the following formula for the dimension of the commutant of $SU(N)$ at height n:

$$\dim_N(n) = \prod_p \{ \#\text{orbits of } SL(2,\mathbb{Z}) \text{ on } [Z_{p^{\gamma(p)}}^{N-2} \times Z_{p^{\gamma(p)+\alpha(p)-\varepsilon(p)}}]^2 \} \ . \tag{2.9}$$

The number of orbits appearing in (2.9) is of the general form

$$M(\alpha, \gamma, k) = \#\text{orbits of } SL(2,\mathbb{Z}) \text{ on } [Z_{p^\gamma}^k \times Z_{p^{\alpha+\gamma}}]^2 \tag{2.10}$$

for some prime number p.

The full determination of $M(\alpha, \gamma, k)$ is possible by the following theorem, that relates the number of orbits of a group acting on some set to the existence and to the number of fixed-points the group has in the set [11].

Let G be a finite group acting on a set X. Denote by X^g the subset of X consisting of elements of X which are left invariant under a fixed g in G: $X^g = \{x \in X : g(x) = x\}$.

Then

$$\#\,\text{orbits of } G \text{ on } X=\frac{1}{\operatorname{card} G}\sum_{g\in G}\operatorname{card} X^g\ . \tag{2.11}$$

Because of the congruence $\operatorname{mod} p^{\alpha+\gamma}$ in (2.10), the group $SL(2,\mathbb{Z})$ is only effective $\operatorname{mod} p^{\alpha+\gamma}$, so that the invariant subgroup $\Gamma(p^{\alpha+\gamma})=\{g\in SL(2,\mathbb{Z}): g=\mathbb{1}\ (\operatorname{mod} p^{\alpha+\gamma})\}$ acts trivially. As a result, the group G in (2.11) is identified with $SL(2,\mathbb{Z})/\Gamma(p^{\alpha+\gamma})=SL(2,Z_{p^{\alpha+\gamma}})=SL(2,\alpha+\gamma)$, whose order is equal to $p^{3(\alpha+\gamma)-2}(p^2-1)$ [12].

One can prove [11] that the cardinal of X^g and X^h are equal if g and h are conjugate, so that one can reformulate Eq. (2.11) in

$$\#\,\text{orbits of } G \text{ on } X=\frac{1}{\operatorname{card} G}\sum_{\text{classes of } G}\operatorname{card}(\text{class})\cdot\operatorname{card}(X^g)\ .$$

Therefore one could look at the problem by first finding the classes of $SL(2,\alpha+\gamma)$ and then calculating the number of fixed-points of a representative g for each class. But actually, this is more information than needed since different classes with the same number of fixed-points need not be distinguished. The method adopted below avoids the determination of the classes.

For the sequel, the following simple remark will prove very useful. The set $X=[Z^k_{p^\gamma}\times Z_{p^{\alpha+\gamma}}]^2$ on which $SL(2,\alpha+\gamma)$ acts is itself an (additive) group. Since the sum of two fixed-points is a fixed-point, the subset X^g is a subgroup of $[Z^k_{p^\gamma}\times Z_{p^{\alpha+\gamma}}]^2$, whose order is necessarily a power of p, between 1 and $p^{2(\alpha+\gamma+k\gamma)}$. From this remark one can compute the dimension of the commutant, for N and n two different (odd) primes, in an extremely simple way, and then obtain a rough estimate of the asymptotic behaviour.

From the above discussion, $\alpha(N)$ and $\gamma(n)$ are equal to 1, so that $\dim_N(n)=M(0,1,0)\cdot M(0,1,N-2)$. In case $SL(2,Z_N)$ acts on $Z_N\times Z_N$, there can be N^2, N or 1 fixed-points. That an element g in $SL(2,Z_N)$ has only one fixed-point implies that the equation $(x,x')(g-\mathbb{1})=0$ has the only solution $(x,x')=(0,0)$ in $Z_N\times Z_N$. This implies that $\det(g-\mathbb{1})\neq 0\ (\operatorname{mod} N)$. The number of such g's is equal to $N(N^2-N-1)$. Since the matrix $g=\mathbb{1}$ is the only one which has N^2 fixed-points, the number of g's that have N fixed-points is equal to $N(N^2-1)-1-N(N^2-N-1)=N^2-1$. Therefore one gets

$$M(0,1,0)=\frac{1}{N(N^2-1)}\,[N^2+(N^2-1)N+N(N^2-N-1)]=2\ . \tag{2.12}$$

When $SL(2,Z_n)$ acts on $Z_n^{N-1}\times Z_n^{N-1}=[Z_n\times Z_n]^{N-1}$, it is clear that the number of fixed-points of a given g in $SL(2,Z_n)$ is a $(N-1)$-th power of n, since the group acts "diagonally" on the $(N-1)$ copies of $Z_n\times Z_n$. The possible numbers of fixed-points are thus $n^{2(N-1)}$, n^{N-1} or 1, and the same reasoning as above leads to

$$M(0,1,N-2)=\frac{1}{n(n^2-1)}\,[n^{2(N-1)}+(n^2-1)n^{N-1}+n(n^2-n-1)]\ . \tag{2.13}$$

Equations (2.12–13) already give the dimension of the commutant of $SU(N)$ at height n, when N and n are two different odd primes. Note the asymptotic behaviour

$$\dim_N(n)=M(0,1,0)\cdot M(0,1,N-2)\sim n^{2N-5}\ . \tag{2.14}$$

This result should be compared with Eqs. (2.6–7).

III. Counting the Orbits

This section and the next one are mainly devoted to the computation of $M(\alpha,\gamma,k)$, the number of orbits of $SL(2,\alpha+\gamma)=SL(2,p^{\alpha+\gamma})$ acting on $X=[Z_{p^\gamma}^k\times Z_{p^{\alpha+\gamma}}]^2$.

By the theorem stated in Eq. (2.11), one is led to calculate the number of fixed-points in X of each matrix g in $SL(2,\alpha+\gamma)$. To a large extent, this is a problem of linear algebra on finite congruence rings.

Let g be a matrix of $SL(2,\alpha+\gamma)$ and $x=(x^{(1)},\dots,x^{(k)},y)$ an element of $Z_{p^\gamma}^k\times Z_{p^{\alpha+\gamma}}$, i.e. $x^{(i)}$ is taken mod p^γ, while y is taken mod $p^{\alpha+\gamma}$. The fixed-points of g are the solutions (x,x') of

$$(x,x')(g-\mathbb{1})=0 \pmod{p^{\alpha+\gamma}} \Leftrightarrow (x^{(i)},x'^{(i)})(g-\mathbb{1})=0 \pmod{p^\gamma}$$

$$(y,y')(g-\mathbb{1}) \pmod{p^{\alpha+\gamma}}\ . \qquad (3.1)$$

If g has p^j fixed-points (y,y') in $Z_{p^{\alpha+\gamma}}^2$ and p^l fixed-points $(x^{(i)},x'^{(i)})$ in $Z_{p^\gamma}^2$ $(0\leqq j\leqq 2\alpha+2\gamma$ and $0\leqq l\leqq 2\gamma)$, it is clear that g has p^{j+kl} fixed-points in X.

Therefore the problem is twofold: (i) to count the g's in $SL(2,\alpha+\gamma)$ which have p^j fixed-points in $Z_{p^{\alpha+\gamma}}^2$ and (ii) among these, to count how many have p^l fixed-points when they are reduced to $SL(2,\gamma)$?

Let us denote by $F_{(\gamma)}^{(\alpha+\gamma)}(j,l)$ the number of matrices in $SL(2,\alpha+\gamma)$ with p^j fixed-points in $Z_{p^{\alpha+\gamma}}^2$ and p^l fixed-points in $Z_{p^\gamma}^2$.

Then by Eq. (2.11)

$$M(\alpha,\gamma,k)=\#\text{ orbits of } SL(2,\mathbb{Z}) \text{ on } X=[Z_{p^\gamma}^k\times Z_{p^{\alpha+\gamma}}]^2$$

$$=\frac{1}{p^{3(\alpha+\gamma)-2}(p^2-1)}\sum_{j=0}^{2\alpha+2\gamma}\sum_{l=0}^{2\gamma}F_{(\gamma)}^{(\alpha+\gamma)}(j,l)\cdot p^{j+kl}\ , \qquad (3.2)$$

and from Eq. (2.9), one gets the dimension of the commutant by

$$\dim_N(n)=\prod_p M(\alpha(p)-\varepsilon(p),\gamma(p),N-2)\ . \qquad (3.3)$$

In order to explicitly determine $F_{(\gamma)}^{(\alpha+\gamma)}(j,l)$, we collect some preliminary results, first dealing with the case $\alpha=0$.

To fix the notations, let p be any fixed prime number. An element x in Z_{p^γ}, the set of integers mod p^γ, can be represented as a power series $x=x_0+x_1\cdot p+\ldots+x_{\gamma-1}\cdot p^{\gamma-1}$, where the "digits" x_i are taken mod p. Z_{p^γ} is an additive group with p^γ elements. Those x's such that $x\not\equiv 0 \pmod p$, i.e. $x_0\not\equiv 0 \pmod p$, are invertible mod p^γ and form the multiplicative group $Z_{p^\gamma}^*$ with $p^{\gamma-1}(p-1)$ elements. The notation $\operatorname{ord}_p x=k$ (k is called the ordinal of x) means that p^k divides x but p^{k+1} does not. We will also frequently use the following expansion of $g\in SL(2,\gamma)$ in power series of $p: g=\mathbb{1}+g_0+g_1\cdot p+\ldots+g_{\gamma-1}\cdot p^{\gamma-1}$, where the g_i's are two-by-two matrices whose entries are taken mod p. Finally $[x]$ is the largest integer smaller or equal to x, for x real.

Lemma 1. *For $0\leqq j\leqq\gamma-1$, the number of g's in $SL(2,\gamma)$ which have exactly p^j fixed-points in $Z_{p^\gamma}^2$ is equal to $F_{(\gamma)}^{(\gamma)}(j,j)=\operatorname{card}\{g\in SL(2,g):\operatorname{ord}_p\det(g-\mathbb{1})=j\}$.*

The case $j=0$ is clear because if g has only one fixed-point, the equation $(x,x')(g-\mathbb{1})=0$ should admit as the only solution the trivial one, $(x,x')=(0,0)$. Therefore $g-\mathbb{1}$ is invertible, which implies that $\det(g-\mathbb{1})\not\equiv 0 \pmod p$.

Let $g-\mathbb{1}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$. From $\det(g-\mathbb{1})=ad-bc=0\ (\mathrm{mod}\,p^j)$ and $\det g=1+a+d+ad-bc=1\ (\mathrm{mod}\,p^\gamma)$, one finds that $\mathrm{Tr}\,(g-\mathbb{1})=a+d=0\ (\mathrm{mod}\,p^j)$. The characteristic equation of $g-\mathbb{1}$ is

$$\det(g-\mathbb{1}-\lambda\mathbb{1})=\lambda^2-\lambda(a+d)+ad-bc=\lambda^2=0\ (\mathrm{mod}\,p^j)\ .$$

Therefore, if b or c is invertible, the matrix $g-\mathbb{1}$ is equivalent to the Jordan form

$$g-\mathbb{1}=\begin{pmatrix}a'\cdot p^j & 1\\ c'\cdot p^j & d'\cdot p^j\end{pmatrix}=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}(\mathrm{mod}\,p^j)\ . \tag{3.4}$$

The ordinal of $\det(g-\mathbb{1})$ equal to j implies $c'\neq 0\ (\mathrm{mod}\,p)$. The fixed-points of g are the solutions of $(x,x')(g-\mathbb{1})=0$, i.e.

$$a'p^jx+c'p^jx'=0\ (\mathrm{mod}\,p^\gamma)\ , \tag{3.5a}$$

$$x+d'p^jx'=0\ (\mathrm{mod}\,p^\gamma)\ . \tag{3.5b}$$

Equation (3.5b) gives x in terms of x' and Eq. (3.5a) implies the following condition on $x':(a'd'p^j-c')x'=0\ (\mathrm{mod}\,p^{\gamma-j})$ or $x'=0\ (\mathrm{mod}\,p^{\gamma-j})$. There are p^j solutions $x'=x'_{\gamma-j}\cdot p^{\gamma-j}+\ldots+x'_{\gamma-1}\cdot p^{\gamma-1}$, and therefore p^j fixed-points (x,x') for g.

If neither b nor c is invertible (i.e. they are divisible by p), the condition on the determinant of $g-\mathbb{1}$ implies ad $=0\ (\mathrm{mod}\,p^2)$ for $j\geqq 2$. The only possibility consistent with the condition on the trace is $a=d=0\ (\mathrm{mod}\,p)$. Hence $g-\mathbb{1}=0\ (\mathrm{mod}\,p)$ and one may set $g-\mathbb{1}=p(\bar{g}-\mathbb{1})$, $\det(\bar{g}-\mathbb{1})=0\ (\mathrm{mod}\,p^{j-2})$ and $\mathrm{Tr}(\bar{g}-\mathbb{1})=0\ (\mathrm{mod}\,p^{j-1})$. One repeats the above argument for $\bar{g}-\mathbb{1}$, by taking into account that the number of fixed-points of g in $Z^k_{p^\gamma}$ is that of $\bar{g}$ in $Z^2_{p^{\gamma-1}}$ times p^2.

The first lemma allows an explicit calculation of the number of elements in $SL(2,\gamma)$ which have at most $p^{\gamma-1}$ fixed-points in $Z^2_{p^\gamma}$. In dealing with matrices g with more fixed-points, the following result proves extremely useful.

Lemma 2. *If* $g=\mathbb{1}\ (\mathrm{mod}\,p)$ *and* $j\geqq\gamma+1$, $g=\mathbb{1}+g_1\cdot p+g_2\cdot p^2+\ldots$ *has exactly* p^j *fixed-points in* $Z^2_{p^\gamma}$ *if and only if* $\bar{g}=\mathbb{1}+g_1+g_2\cdot p+g_3\cdot p^2+\ldots$ *belonging to* $SL(2,\gamma-1)$ *has* p^{j-2} *fixed-points in* $Z^2_{p^{\gamma-1}}$. *Moreover* $\det(g-\mathbb{1})=0\ (\mathrm{mod}\,p^{\gamma+1})$.

Let $g=\mathbb{1}+g_1\cdot p+g_2\cdot p^2+\ldots=\mathbb{1}+(\bar{g}-\mathbb{1})p$ be a matrix in $SL(2,\gamma)$ with at least $p^{\gamma+1}$ fixed-points in $Z^2_{p^\gamma}$. By the first lemma, $\det(g-\mathbb{1})=\det((\bar{g}-\mathbb{1})p)=0\ (\mathrm{mod}\,p^\gamma)$ or $\det(\bar{g}-\mathbb{1})=0\ (\mathrm{mod}\,p^{\gamma-2})$. Moreover let us assume that $\det(\bar{g}-\mathbb{1})=0\ (\mathrm{mod}\,p^{\gamma-1})$, a fact that will be proved here below. That g belongs to $SL(2,\gamma)$ implies that $\mathrm{Tr}(\bar{g}-\mathbb{1})=0\ (\mathrm{mod}\,p^{\gamma-1}):\det g=\det(\mathbb{1}+(\bar{g}-\mathbb{1})p)=1+p\cdot\mathrm{Tr}(\bar{g}-\mathbb{1})+p^2\cdot\det(\bar{g}-\mathbb{1})=1\ (\mathrm{mod}\,p^\gamma)$. This makes of $\bar{g}$ an element of $SL(2,\gamma-1):\det\bar{g}=\det(\mathbb{1}+\bar{g}-\mathbb{1})=1+\mathrm{Tr}(\bar{g}-\mathbb{1})+\det(\bar{g}-\mathbb{1})=1\ (\mathrm{mod}\,p^{\gamma-1})$. The number of fixed-points of g in $Z^2_{p^\gamma}$, i.e. the solutions (x,x') of

$$(x,x')(g-\mathbb{1})=(x,x')\,[p(\bar{g}-\mathbb{1})]=(px,px')(\bar{g}-\mathbb{1})=0\ (\mathrm{mod}\,p^\gamma) \tag{3.6}$$

is thus the number of fixed-points of $\bar{g}$ in $Z^2_{p^{\gamma-1}}$ times p^2, because in Eq. (3.6) the digits $x_{\gamma-1}$ and $x'_{\gamma-1}$ are unconstrained.

One concludes that for g to have p^j fixed-points, $\bar{g}$ must have p^{j-2} fixed-points in $Z^2_{p^{\gamma-1}}$ and conversely. It remains to prove that if $g=\mathbb{1}+p(\bar{g}-\mathbb{1})$ has at least $p^{\gamma+1}$ fixed-points, then $\det(\bar{g}-\mathbb{1})=0\ (\mathrm{mod}\,p^{\gamma-1})$ or $\det(g-\mathbb{1})=0\ (\mathrm{mod}\,p^{\gamma+1})$. By the first lemma, it is equivalent to prove that if $g=\mathbb{1}\ (\mathrm{mod}\,p)$ and $\mathrm{ord}_p\det(g-\mathbb{1})=\gamma$, g has exactly p^γ fixed-points.

Let $g=\mathbb{1}+p\cdot\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. The matrix $h=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is taken $\bmod p^{\gamma-1}$. As in Eq. (3.6), the number of fixed-points of g is p^2 times the number of fixed-points of h. That g belongs to $SL(2,\gamma)$ implies $\operatorname{Tr} h=a+d=0 \pmod{p^{\gamma-1}}$ and by hypothesis $\operatorname{ord}_p(ad-bc)=\gamma-2$. The characteristic equation of h is $\lambda^2=0 \pmod{p^{\gamma-2}}$. Applying the same methods as in Lemma 1, one finds that h has $p^{\gamma-2}$ fixed-points. This concludes the proof of the lemma.

We are now able to characterize the matrices of $SL(2,\gamma)$ which have p^γ or more fixed-points, thus extending the result of Lemma 1.

Lemma 3. *For* $1 \leqq j \leqq \gamma$, *if* g *in* $SL(2,\gamma)$ *has at least* $p^{\gamma+j}$ *fixed-points in* $Z^2_{p^\gamma}$, *then* $g=\mathbb{1} \pmod{p^j}$. *Moreover the number of matrices in* $SL(2,\gamma)$ *which have exactly* p^γ *fixed-points is equal to* $F^{(\gamma)}_{(\gamma)}(\gamma,\gamma)=\operatorname{card}\{g\in SL(2,\gamma):\operatorname{ord}_p\det(g-\mathbb{1})=\gamma\}$, *and* $F^{(\gamma)}_{(\gamma)}(\gamma+k,\gamma+k)=F^{(\gamma-k)}_{(\gamma-k)}(\gamma-k,\gamma-k)$ *for* $1\leqq k\leqq\gamma$.

Lemma 3 is a direct consequence of Lemma 2 and of the following weaker statement that if g has at least $p^{\gamma+1}$ fixed-points, then $g=\mathbb{1} \pmod p$. One rather proves the converse: if $g \neq \mathbb{1} \pmod p$, the number of fixed-points of g is at most p^γ. Clearly this is true for $\gamma=1$, because the only element in $SL(2,1)$ with p^2 fixed-points in Z_p^2 is the identity $g=\mathbb{1}$. Let $(x,x')=(x_0+\ldots+x_\gamma p^\gamma, x'_0+\ldots+x'_\gamma p^\gamma)$ an element of $Z^2_{p^{\gamma+1}}$. (x,x') is a fixed-point of g in $SL(2,\gamma+1)$ if $(x,x') \pmod{p^\gamma}$ is a fixed-point of $g \pmod{p^\gamma}$ and if the following equation is satisfied:

$$(x_\gamma,x'_\gamma)g_0=-(x_{\gamma-1},x'_{\gamma-1})g_1-(x_{\gamma-2},x'_{\gamma-2})g_2-\ldots-(x_0,x'_0)g_\gamma \pmod p \ . \quad (3.7)$$

Going from γ to $\gamma+1$, one thus adds the two equations (3.7) for the two new digits x_γ and x'_γ, each taking p values. In the process, the number of fixed-points can be multiplied by $1, p$ or p^2. The last possibility only occurs when the Eqs. (3.7) do not put any constraint on x_γ and x'_γ, i.e. when $g_0=0$ or $g=\mathbb{1} \pmod p$. By recurrence, the number of fixed-points of $g \neq \mathbb{1} \pmod p$ in $SL(2,\gamma)$ is at most p^γ.

Assume now that g in $SL(2,\gamma)$ has at least $p^{\gamma+2}$ fixed-points and let $g=\mathbb{1}+p(\bar{g}-\mathbb{1})$. By Lemma 2, the matrix $\bar{g}$ in $SL(2,\gamma-1)$ has at least p^γ fixed-points, and this implies that $\bar{g}=\mathbb{1} \pmod p$ by the result just above. Therefore $g=\mathbb{1} \pmod{p^2}$. Iterating the argument proves the first part of the lemma.

The matrices of $SL(2,\gamma)$ which have at least p^γ fixed-points are such that $\det(g-\mathbb{1})=0 \pmod{p^\gamma}$ by the first lemma. Those which have at least $p^{\gamma+1}$ fixed-points are such that $\det(g-\mathbb{1})=0 \pmod{p^{\gamma+1}}$, by the second lemma. Therefore those with $\operatorname{ord}_p\det(g-\mathbb{1})=\gamma$ have exactly p^γ fixed-points. Finally the last formula follows from Lemma 2: if g has $p^{\gamma+k}$ fixed-points, $g=\mathbb{1} \pmod p$ and it states that $F^{(\gamma)}_{(\gamma)}(\gamma+k,\gamma+k)=F^{(\gamma-1)}_{(\gamma-1)}(\gamma+k-2,\gamma+k-2)$.

Lemmas 1–3 completely characterize the elements of $SL(2,\gamma)$ with a prescribed number of fixed-points in $Z^2_{p^\gamma}$: a matrix g has p^j fixed-points if and only if the ordinal of $\det(g-\mathbb{1})$ is equal to j, for any j between 0 and 2γ. When j is greater or equal to γ and since g is taken $\bmod p^\gamma$, the precise meaning of this statement is the following: for g to have p^j fixed-points, g must belong to the set $\{g\in SL(2,\gamma): g=\mathbb{1} \pmod{p^{j-\gamma}}$ and $\det(g-\mathbb{1})=0 \pmod{p^j}\}$ but not to $\{g\in SL(2,\gamma): g=\mathbb{1} \pmod{p^{j+1-\gamma}}$ and $\det(g-\mathbb{1})=0 \pmod{p^{j+1}}\}$. The computation of the cardinality of these sets enables us to give the explicit form of the coefficients $F^{(\gamma)}_{(\gamma)}(j,j)$ and eventually the expression of $M(\alpha,\gamma,k)$ in case $\alpha=0$. For reasons that will be clear in Sect. 4, one considers instead the more constrained set

$$S^{(\gamma)}_{k;l} = \{g \in SL(2,\gamma) \colon\ g = \mathbb{1}\ (\operatorname{mod} p^l) \quad \text{and} \quad \det(g-\mathbb{1}) = 0\ (\operatorname{mod} p^{2l+k})\}\ , \tag{3.8}$$

for $0 \leqq l \leqq \gamma$ and $0 \leqq k \leqq \gamma - l$. We separate the cases $l=0$ and $l \geqq 1$.

1) $l=0$: $S^{(\gamma)}_{k;0} = \{g \in SL(2,\gamma) \colon \det(g-\mathbb{1}) = 0\ (\operatorname{mod} p^k)\}$.

Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $S^{(\gamma)}_{k;0}$, so that $ad-bc=1\ (\operatorname{mod} p^\gamma)$ and $a+d=2\ (\operatorname{mod} p^k)$. The entry b is an integer taken $\operatorname{mod} p^\gamma$. Let us assume that its ordinal is equal to $m \leqq \gamma - 1 : b = 0\ (\operatorname{mod} p^m)$ but $b \neq 0\ (\operatorname{mod} p^{m+1})$.

The two equations to be solved are

$$ad-bc=1\ (\operatorname{mod} p^\gamma) \Rightarrow ad=1\ (\operatorname{mod} p^m)\ , \tag{3.9a}$$

$$a+d=2\ (\operatorname{mod} p^k)\ . \tag{3.9b}$$

If $k \geqq m$, Eqs. (3.9) imply $ad=1\ (\operatorname{mod} p^m)$ and $a+d=2\ (\operatorname{mod} p^m)$, hence $(a-1)^2=0$ $(\operatorname{mod} p^m)$, the solution of which is $a=1\ (\operatorname{mod} p^{[(m+1)/2]})$. Since b and $ad-1$ are divisible by p^m, Eq. (3.9a) is equivalent to $p^{-m}bc = p^{-m}(ad-1)\ (\operatorname{mod} p^{\gamma-m})$ or $c = (p^{-m}b)^{-1} \cdot p^{-m}(ad-1)\ (\operatorname{mod} p^{\gamma-m})$. Therefore the conditions dictated by the Eqs. (3.9) are: a belongs to Z_{p^γ} but is equal to 1 $\operatorname{mod} p^{[(m+1)/2]}$, $p^{-m}b$ belongs to $Z^*_{p^{\gamma-m}}$, c belongs to Z_{p^γ} but is fixed $\operatorname{mod} p^{\gamma-m}$ by a, b and d, and finally d belongs to Z_{p^γ} but is fixed $\operatorname{mod} p^k$ by a (Eq. (3.9b)). As a result a, b, c and d can take $p^{\gamma-[(m+1)/2]}$, $p^{\gamma-m-1} \cdot (p-1)$, p^m and $p^{\gamma-k}$ different values respectively. The number of solutions to Eqs. (3.9) is thus $p^{3\gamma-k-[(m+1)/2]-1} \cdot (p-1)$.

If $k \leqq m$, $ad=1\ (\operatorname{mod} p^k)$ and $a+d=2\ (\operatorname{mod} p^k) : d$ is fixed $\operatorname{mod} p^k$ by a through $d=a^{-1}\ (\operatorname{mod} p^k)$ and $a=1\ (\operatorname{mod} p^{[(k+1)/2]})$. As before, c is determined $\operatorname{mod} p^{\gamma-m}$ by $c=(p^{-m}b)^{-1} \cdot p^{-m}(ad-1)\ (\operatorname{mod} p^{\gamma-m})$. The number of solutions to Eqs. (3.9) is equal to $p^{3\gamma-m-[(k+1)/2]-1} \cdot (p-1)$.

Finally, if $b=0\ (\operatorname{mod} p^\gamma)$, then $ad=1\ (\operatorname{mod} p^\gamma)$ and $a+d=2\ (\operatorname{mod} p^k)$. Therefore $d=a^{-1}\ (\operatorname{mod} p^\gamma)$, $a=1\ (\operatorname{mod} p^{[(k+1)/2]})$ and c is unconstrained. In this case the number of solutions is $p^{2\gamma-[(k+1)/2]}$.

Summing up the different contributions yields

$$\operatorname{card} S^{(\gamma)}_{k;0} = p^{3\gamma-k-1}\,[(p+1) - p^{-[k/2]}]\ . \tag{3.10}$$

2) $l \geqq 1$. Let $g = \mathbb{1} + p^l \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $S^{(\gamma)}_{k;l}$, so that the entries a, b, c and d, which are taken $\operatorname{mod} p^{\gamma-l}$, are constrained by the two equations

$$ad-bc=0\ (\operatorname{mod} p^k)\ , \tag{3.11a}$$

$$a+d+(ad-bc)p^l = 0\ (\operatorname{mod} p^{\gamma-l})\ . \tag{3.11b}$$

Equation (3.11b) completely fixes a in terms of the other entries: $a=(1+dp^l)^{-1} \cdot (bcp^l - d)\ (\operatorname{mod} p^{\gamma-l})$. Plugging this value of a in Eq. (3.11a) leads to $bc = -d^2$ $(\operatorname{mod} p^k)$. Proceeding as in the first part 1), one finds that this equation has $p^{3\gamma-3l-k-[(m+1)/2]-1} \cdot (p-1)$ solutions if the ordinal of b is equal to $m \leqq k-1$ and $p^{3\gamma-3l-k-[(k+1)/2]}$ solutions if $b=0\ (\operatorname{mod} p^k)$. Summing up the number of solutions for the various values of $\operatorname{ord}_p b$ yields

$$\operatorname{card} S^{(\gamma)}_{k;l} = p^{3(\gamma-l)-k-1}\,[(p+1) - p^{-[k/2]}] = \operatorname{card} S^{(\gamma-l)}_{k;0}\ . \tag{3.12}$$

From Eqs. (3.10, 3.12), one gets the number of matrices in $SL(2,\gamma)$ which have p^j fixed-points in $Z^2_{p^\gamma}$,

$$F^{(\gamma)}_{(\gamma)}(0,0)=\operatorname{card} SL(2,\gamma)-\operatorname{card} S^{(\gamma)}_{1;0}=p^{3\gamma-2}(p^2-p-1)\ , \tag{3.13a}$$

$$\begin{aligned}F^{(\gamma)}_{(\gamma)}(j,j)&=\operatorname{card} S^{(\gamma)}_{j;0}-\operatorname{card} S^{(\gamma)}_{j+1;0}\\&=p^{3\gamma-j-2}(p^2-1+p^{-[(j+1)/2]}-p^{-[(j-2)/2]})\quad (1\leqq j\leqq\gamma-1)\ ,\end{aligned} \tag{3.13b}$$

$$\begin{aligned}F^{(\gamma)}_{(\gamma)}(j,j)&=\operatorname{card} S^{(\gamma)}_{2\gamma-j;j-\gamma}-\operatorname{card} S^{(\gamma)}_{2\gamma-j-1;j+1-\gamma}\\&=p^{4\gamma-2j-3}(p+1)(p^2-1)+p^{[(6\gamma-3j-4)/2]}-p^{[(6\gamma-3j-1)/2]}\\&\quad(\gamma\leqq j\leqq 2\gamma-1)\ ,\end{aligned} \tag{3.13c}$$

$$F^{(\gamma)}_{(\gamma)}(2\gamma,2\gamma)=1\ . \tag{3.13d}$$

By using Eq. (3.2) with $\alpha=0$, namely

$$M(0,\gamma,k)=\frac{1}{p^{3\gamma-2}(p^2-1)}\cdot\sum_{j=0}^{2\gamma}F^{(\gamma)}_{(\gamma)}(j,j)p^{(k+1)j}\ ,$$

one has the following

Proposition 1. *The number of orbits of $SL(2,\mathbb{Z})$ acting on $Z^{k+1}_{p^\gamma}\times Z^{k+1}_{p^\gamma}$ is equal to*

$$\begin{aligned}M(0,\gamma,k)=&\,p^{(2k-1)\gamma-1}\frac{(p^{k+1}-1)(p^{2k}-1)}{(p^2-1)(p^{k-1}-1)(p^{2k-1}-1)}-p^{k\gamma-1}\frac{(p^{k+1}-1)}{(p^k-1)(p^{k-1}-1)}\\&-\frac{p(p^{k-2}-1)}{(p+1)(p^k-1)(p^{2k-1}-1)}-\frac{1}{(p^2-1)}\ .\end{aligned} \tag{3.14}$$

In relation to our original problem, formula (3.14) is all what is needed in order to compute the dimension of the commutant for $SU(N)$, at height n, provided that N and n are coprime integers. (See Eq. (3.3) and use $M(\alpha(p)-\varepsilon(p),0,N-2)=M(0,\alpha(p)-\varepsilon(p),0)$.) It is useful and illustrative to list the expression of $M(0,\gamma,k)$ for some small values of k. The cases $k=0$ and $k=1$ (relevant for $SU(2)$ and $SU(3)$ respectively) are somewhat particular since the expression (3.14) has apparent singularities. These two cases are the only ones in which the answer is simple. One gets for k up to 3

$$M(0,\gamma,0)=\gamma+1\ ;\qquad M(0,\gamma,1)=(\gamma+1)p^\gamma+\gamma p^{\gamma-1}\ , \tag{3.15a,b}$$

$$M(0,\gamma,2)=\frac{1}{(p^2-1)}\,[p^{3\gamma+2}+p^{2\gamma-1}(p^\gamma-1)(p^2+p+1)-1]\ , \tag{3.15c}$$

$$\begin{aligned}M(0,\gamma,3)=\frac{1}{(p^2-1)}\Bigg[&p^{5\gamma-1}\frac{(p^2+1)(p^6-1)}{(p^5-1)}\\&-p^{3\gamma-1}\frac{(p^4-1)}{(p^3-1)}-\frac{p(p-1)^2}{(p^3-1)(p^5-1)}-1\Bigg]\ .\end{aligned} \tag{3.15d}$$

IV. The Case $(N, n) \neq 1$

Section 3 gave criteria to decide how many fixed-points a given matrix in $SL(2,\gamma)$ has in $Z^2_{p^\gamma}$. Here one considers the question of how the number of fixed-points of a matrix g varies when g is reduced from $SL(2,\alpha+\gamma)$ down to $SL(2,\gamma)$.

We want to establish a kind of branching rule for the number of fixed-points that a matrix of $SL(2,\mathbb{Z})$ may have, and thereby calculate the coefficients $F^{(\alpha+\gamma)}_{(\gamma)}(j,l)$, i.e. the number of matrices which have p^j fixed-points in $Z^2_{p^{\gamma+\alpha}}$ and p^l fixed-points in $Z^2_{p^\gamma}$. Clearly, the important step is to solve the case $\alpha=1$.

We first describe in which limits the number of fixed-points may vary. As mentioned in the proof of Lemma 3, when going from $SL(2,\gamma+1)$ to $SL(2,\gamma)$, the number of fixed-points can be divided by $1, p$ or p^2. If the matrix g in $SL(2,\gamma+1)$ has $p^j \leqq p^\gamma$ fixed-points, the ordinal of $\det(g-\mathbb{1})$ is equal to j, by Sect. 3. When g is reduced to $SL(2,\gamma)$, it is modified to the γ^{th} order in p, but this truncation process can certainly not decrease the ordinal of $\det(g-\mathbb{1})$. On the other hand, the ordinal of $\det(g-\mathbb{1})$ cannot increase, because that would mean that the number of fixed-points increases too. Therefore, as a matrix of $SL(2,\gamma)$, g still has p^j fixed-points. If g has $p^{\gamma+1}$ fixed-points, the ordinal of $\det(g-\mathbb{1})$ is equal to $\gamma+1$. By modifying g to the $p^{\gamma th}$ order, the ordinal of $\det(g-\mathbb{1})$ may change to γ, but not to $\gamma-1$. Thus the number of fixed-points of g cannot be divided by p^2. When g has between $p^{\gamma+2}$ and $p^{2\gamma+1}$ fixed-points, one uses one more time the recurrence property of Lemma 2 to prove that in these cases too, the number of fixed-points cannot be divided by p^2. For instance, if the number of fixed-points of $g=\mathbb{1}+p\cdot(\bar{g}-\mathbb{1})$ in $SL(2,\gamma+1)$ was to change from $p^{\gamma+2}$ to p^γ, then by Lemma 2, the number of fixed-points of $\bar{g}$ in $SL(2,\gamma)$ would change from p^γ to $p^{\gamma-2}$, a branching forbidden by the above argument. The only case where the number of fixed-points is divided by p^2 is when the matrix g is the identity in $SL(2,\gamma+1)$.

To summarize, when g in $SL(2,\gamma+1)$ has p^j fixed-points and is reduced to $SL(2,\gamma)$, the following branchings are possible: for $0\leqq j\leqq\gamma$, the number of fixed-points is unchanged; for $\gamma+1\leqq j\leqq 2\gamma+1$, it is divided by 1 or p and for $j=2\gamma+2$, it is divided by p^2. Not only are these branchings possible, in fact they all occur as the following result proves.

Lemma 4. *For g a matrix in $SL(2,\gamma+1)$ and $0\leqq j\leqq\gamma-1$, the numbers of fixed-points of g in $Z^2_{p^{\gamma+1}}$ and in $Z^2_{p^\gamma}$ are equal to $p^{\gamma+1+j}$ if and only if $g=\mathbb{1}$ $(\mathrm{mod}\, p^{j+1})$.*

Let us first consider the case $j=0$ and g an element of $SL(2,\gamma+1)$ with $p^{\gamma+1}$ fixed-points in $Z^2_{p^{\gamma+1}}$. If $g\neq\mathbb{1}$ $(\mathrm{mod}\, p)$, then obviously the number of fixed-points of g in $Z^2_{p^\gamma}$ must equal p^γ, for if it was equal to $p^{\gamma+1}$, Lemma 3 would imply that $g=\mathbb{1}$ $(\mathrm{mod}\, p)$. Conversely, if $g=\mathbb{1}$ $(\mathrm{mod}\, p)$, let us show that the number of fixed-points is not altered in the reduction process.

Let $g=\mathbb{1}+h\cdot p$, with $\det(g-\mathbb{1})=p^2\cdot\det h=0$ $(\mathrm{mod}\, p^{\gamma+1})$, since g has $p^{\gamma+1}$ fixed-points (Lemma 1). Therefore $\det h=0$ $(\mathrm{mod}\, p^{\gamma-1})$. When g is reduced from $SL(2,\gamma+1)$ to $SL(2,\gamma)$, h is taken $\mathrm{mod}\, p^{\gamma-1}$ instead of $\mathrm{mod}\, p^\gamma$ and as a consequence, its determinant is still zero $\mathrm{mod}\, p^{\gamma-1}$, and $\deg(g-\mathbb{1})=0$ $(\mathrm{mod}\, p^{\gamma+1})$ with g considered as an element of $SL(2,\gamma)$. By the results of Sect. 3, g has a least $p^{\gamma+1}$ fixed-points in $Z^2_{p^\gamma}$, hence exactly $p^{\gamma+1}$ fixed-points.

For the case $j\geqq 1$, one uses the recurrence of Lemma 2: if g has $p^{\gamma+1+j}$ fixed-points in $Z^2_{p^\gamma}$, g can be written $g=\mathbb{1}+p^j(\bar{g}-\mathbb{1})$ by Lemma 3, where the matrix $\bar{g}$ belongs to $SL(2,\gamma+1-j)$ and has $p^{\gamma+1-j}$ fixed-points.

The results obtained so far for the branching rules are graphically summarized in Fig. 1.

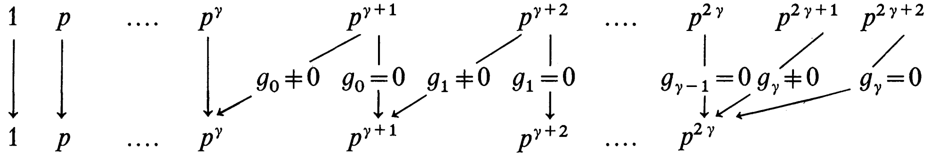

Fig. 1. Branching rules for the number of fixed-points of $g = 1\!\!1 + g_0 + g_1 p + \ldots$ when going from $SL(2,\gamma+1)$ to $SL(2,\gamma)$

To solve the branching problem for any $\alpha \geqq 1$, one just superposes several diagrams like that of Fig. 1, the upper line for $SL(2,\gamma+\alpha)$ and the lower one for $SL(2,\gamma)$. One chooses a point on each of these two lines and one reads on the picture which are the possible paths connecting these two points. To each path is associated a set of conditions on g which are non-contradictory for only one path. For instance, in the case $\alpha=3$, the picture one gets is that of Fig. 2.

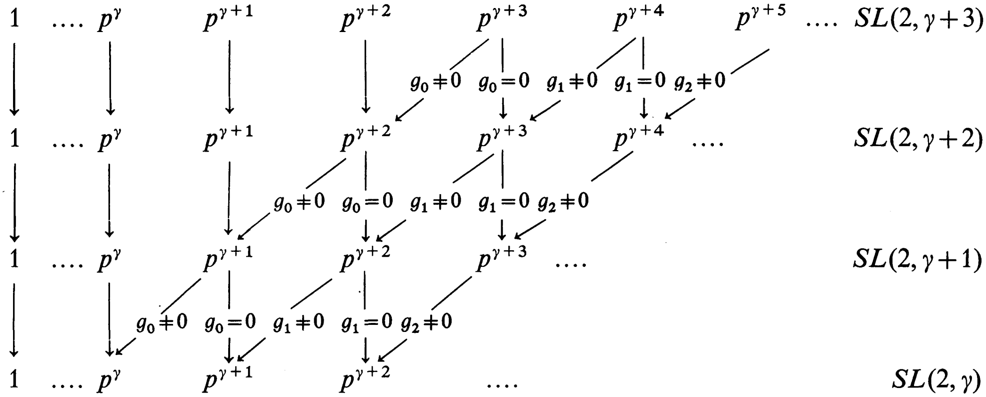

Fig. 2. Branching rules from $SL(2,\gamma+3)$ to $SL(2,\gamma)$

The conditions under which the number of fixed-points of g changes from $p^{\gamma+4}$ to $p^{\gamma+2}$ when g is reduced from $SL(2,\gamma+3)$ to $SL(2,\gamma)$ can be read off from Fig. 2: they are $g_0 = g_1 = 0$ and $g_2 \neq 0$ in the expansion of $g = 1\!\!1 + g_0 + g_1 p + g_2 p^2 + \ldots + g_{\gamma+\alpha-1} p^{\gamma+\alpha-1}$. Therefore $F_{(\gamma)}^{(\gamma+3)}(\gamma+4,\gamma+2) = \operatorname{card}\{g \in SL(2,\gamma+3)\colon \operatorname{ord}_p \det(g - 1\!\!1) = \gamma+4,\ g = 1\!\!1 \ (\bmod p^2)$ but $g \neq 1\!\!1 \ (\bmod p^3)\}$.

More generally, one gets the following results for the coefficients ($\alpha \geqq 1$):

$0 \leqq j \leqq \gamma - 1$

$$F_{(\gamma)}^{(\gamma+\alpha)}(j,j) = \operatorname{card}\{g \in SL(2,\gamma+\alpha)\colon \operatorname{ord}_p \det(g - 1\!\!1) = j\} = F_{(\gamma+\alpha)}^{(\gamma+\alpha)}(j,j)\ , \tag{4.1a}$$

$0 \leqq j \leqq \gamma + \alpha - 1$

$F_{(\gamma)}^{(\gamma+\alpha)}(\gamma+j,\gamma+l) = \operatorname{card}\{g \in SL(2,\gamma+\alpha)\colon \operatorname{ord}_p \det(g - 1\!\!1) = \gamma + j$ and

$$\left[\begin{array}{l} g=\mathbb{1}\ (\mathrm{mod}\, p^{l}),\ g\neq\mathbb{1}\ (\mathrm{mod}\, p^{l+1}) \quad \text{if} \quad \max(0, j-\alpha) \leqq l < \min(j, \gamma)\} \\ g=\mathbb{1}\ (\mathrm{mod}\, p^{l}) \quad \text{if} \quad l=\min(j, \gamma)\} \end{array}\right. , \qquad (4.1\mathrm{b})$$

$$0 \leqq j \leqq \alpha$$

$$\begin{aligned} F_{(\gamma)}^{(\gamma+\alpha)}(2\gamma+\alpha+j, 2\gamma) &= \mathrm{card}\,\{g \in SL(2, \gamma+\alpha)\colon\ \mathrm{ord}_p \det(g-\mathbb{1}) = 2\gamma+\alpha+j \\ &\qquad \text{and} \quad g=\mathbb{1}\ (\mathrm{mod}\, p^{\gamma+j})\} \\ &= F_{(\gamma+\alpha)}^{(\gamma+\alpha)}(2\gamma+\alpha+j, 2\gamma+\alpha+j)\ . \end{aligned} \qquad (4.1\mathrm{c})$$

The other coefficients are equal to zero. The expressions for the coefficients in Eqs. (4.1) are easily calculated with the help of Eqs. (3.10) and (3.12). For $0 \leqq j \leqq \gamma+\alpha-1$, they are

$$\begin{aligned} F_{(\gamma)}^{(\gamma+\alpha)}(\gamma+j, \gamma+l) &= \mathrm{card}\, S_{\gamma+j-2l;l}^{(\gamma+\alpha)} - \mathrm{card}\, S_{\gamma+j+1-2l;l}^{(\gamma+\alpha)} - \mathrm{card}\, S_{\gamma+j-2-2l;l+1}^{(\gamma+\alpha)} \\ &\quad + \mathrm{card}\, S_{\gamma+j-1-2l;l+1}^{(\gamma+\alpha)}\ , \end{aligned} \qquad (4.2\mathrm{a})$$

for $0 \leqq l < \min(j, \gamma)$ if $j < \alpha$ and for $j-\alpha < l < \min(j, \gamma)$ if $j \geqq \alpha$,

$$F_{(\gamma)}^{(\gamma+\alpha)}(\gamma+j, \gamma+j-\alpha) = \mathrm{card}\, S_{\gamma+2\alpha-j;j-\alpha}^{(\gamma+\alpha)} - \mathrm{card}\, S_{\gamma+2\alpha-j-2;j-\alpha+1}^{(\gamma+\alpha)} \qquad (4.2\mathrm{b})$$

if $j \geqq \alpha$, and

$$F_{(\gamma)}^{(\gamma+\alpha)}(\gamma+j, \gamma+l) = \mathrm{card}\, S_{\gamma+j-2l;l}^{(\gamma+\alpha)} - \mathrm{card}\, S_{\gamma+j+1-2l;l}^{(\gamma+\alpha)} \qquad (4.2\mathrm{c})$$

for $l = \min(j, \gamma)$.

Having provided explicit formulae for all the coefficients, the summation involved in

$$M(\alpha, \gamma, k) = \frac{1}{p^{3(\alpha+\gamma)-2}(p^2-1)} \sum_{j=0}^{2(\alpha+\gamma)} \sum_{l=0}^{2\gamma} F_{(\gamma)}^{(\gamma+\alpha)}(j, l) \cdot p^{j+kl} \qquad (4.3)$$

can be carried out completely, but the final result for arbitrary values of α, γ and k is cumbersome and not particularly enlightening. We prefer to restrict ourselves to the special case $\alpha=1$.

Proposition 2. *The number of orbits of* $SL(2, \mathbb{Z})$ *acting on* $[Z_{p^\gamma}^k \times Z_{p^{\gamma+1}}]^2$ *is equal to*

$$\begin{aligned} M(1, \gamma, k) &= p^{(2k-1)\gamma-1}\, \frac{2p^{3k+1} - p^{3k-1} + p^2 - p^k(p^{k-1}+1)(p^2+p-1)}{(p^2-1)(p^{k-1}-1)(p^{2k-1}-1)} \\ &\quad - p^{k\gamma}\, \frac{2p^k - p^{k-1} - 1}{(p^k-1)(p^{k-1}-1)} - \frac{p^{3k-1} - p^{2k-1} - p^{k-1} - p^2 + p + 1}{(p^2-1)(p^k-1)(p^{2k-1}-1)}\ . \end{aligned} \qquad (4.4)$$

For small values of k, Eq. (4.4) yields

$$M(1, \gamma, 0) = M(0, \gamma+1, 0) = \gamma+2\ ; \qquad M(1, \gamma, 1) = 2p^\gamma(\gamma+1)\ , \qquad (4.5\mathrm{a,b})$$

$$M(1, \gamma, 2) = \frac{1}{p^2-1} \cdot [2p^{3\gamma+1}(p+1) - 2p^{2\gamma+1} - p^{2\gamma} - 1]\ , \qquad (4.5\mathrm{c})$$

$$\begin{aligned} M(1, \gamma, 3) = \frac{1}{p^2-1} \cdot \Bigg[& p^{5\gamma+1}\, \frac{2p^6 + p^4 - p^3 - p - 1}{p^5-1} - p^{3\gamma}\, \frac{2p^3 - p^2 - 1}{p^3-1} \\ & - \frac{p^8 - p^5 - 2p^2 + p + 1}{(p^3-1)(p^5-1)} \Bigg]\ . \end{aligned} \qquad (4.5\mathrm{d})$$

Propositions 1 and 2, Eqs. (3.14) and (4.4), allow an explicit determination of the dimension of the commutant for $SU(N)$, for N $(N/2)$ squarefree if N is odd (even), at any height n, although the general problem for any N and any n has been solved, with Eqs. (3.2), (3.3), (3.13), and (4.2).

For $SU(2)$, at height $n=k+2=\prod_p p^{\gamma(p)}$, one recovers the formula found in [2],

$$\dim_2(n)=\prod_p M(0,\gamma,0)=\prod_p (\gamma(p)+1)=\sigma_0(n) \ , \tag{4.6}$$

where $\sigma_0(n)$ is the number of divisors of n.

For $SU(3)$, at height $n=k+3=\prod_p p^{\gamma(p)}$, the formula obtained in [4] by completely different methods is also recovered,

$$\begin{aligned}\dim_3(n)&=M(1,\gamma(3),1)\prod_{p\neq 3} M(0,\gamma(p),1)\\ &=2n(1+\gamma(3))\cdot\prod_{p\neq 3}(1+\gamma(p)+\gamma(p)/p)\,.\end{aligned} \tag{4.7}$$

The dimensions for the next few $SU(N)$'s, at height $n=k+N=\prod_p p^{\gamma(p)}$ are

$$\begin{aligned}\dim_4(n)=&\left[4.2^{3\gamma(2)}-\frac{5}{3}\cdot 2^{2\gamma(2)}-\frac{1}{3}\right]\\ &\cdot\prod_{p\neq 2}\left[\frac{p^{3\gamma(p)+2}+p^{2\gamma(p)-1}(p^{\gamma(p)}-1)(p^2+p+1)-1}{p^2-1}\right],\end{aligned} \tag{4.8}$$

$$\begin{aligned}\dim_5(n)=&\left[\frac{4960}{2343}\cdot 5^{5\gamma(5)}-\frac{7}{93}\cdot 5^{3\gamma(5)}-\frac{1009}{24211}\right]\\ &\cdot\prod_{p\neq 5}\left[p^{5\gamma(p)-1}\frac{(p^2+1)(p^6-1)}{(p^2-1)(p^5-1)}-p^{3\gamma(p)-1}\frac{p^2+1}{p^3-1}\right.\\ &\left.-\frac{p(p-1)^2}{(p^2-1)(p^3-1)(p^5-1)}-\frac{1}{p^2-1}\right],\end{aligned} \tag{4.9}$$

$$\begin{aligned}\dim_6(n)=&\left[\frac{31110}{14209}\cdot 3^{7\gamma(3)}-\frac{67}{1040}\cdot 3^{4\gamma(3)}-\frac{10933}{87440}\right]\\ &\cdot\prod_{p\neq 3}\left[p^{7\gamma(p)-1}\frac{(p^5-1)(p^8-1)}{(p^2-1)(p^3-1)(p^7-1)}-p^{4\gamma(p)-1}\frac{p^5-1}{(p^3-1)(p^4-1)}\right.\\ &\left.-\frac{p}{(p+1)(p^2+1)(p^7-1)}-\frac{1}{p^2-1}\right].\end{aligned} \tag{4.10}$$

We close this section by displaying the numerical values of the dimension of the commutant for small values of N and n. As discussed in Sect. 2, it grows very fast with both N and n and, like many arithmetical functions, it is very erratic, i.e. it strongly depends on the prime decomposition of the numbers involved.

Table 1. Dimension of the commutant for $SU(N)$ at height n. (Large numbers are not tabulated)

$n=$	1	2	3	4	5	6	7	8	9	10
$N=$ 2	1	2	2	3	2	4	2	4	3	4
3	2	10	12	32	22	60	30	88	54	110
4	2	25	80	229	312	2000	800	1941	2342	7800
5	2	102	602	3422	6606	30702	35002	110622	147842	673812
6	2	374	4783	48486	164012	1788842	1686204			$\sim 3.10^7$
7	2	1430	44774	734582	4075262					$\sim 3.10^9$
8	3	6955	600060							$\sim 1.10^{12}$
9	3	33153	3987363							$\sim 4.10^{13}$
10	2	87894	32298164							$\sim 5.10^{15}$

For any N, the dimension of the commutant is a multiplicative function in the sense that (the argument of σ_0 is respectively for N odd and for N even)

$$\dim_N(n)\cdot\dim_N(n')=\dim_N(1)\cdot\dim_N(n\cdot n')=\sigma_0(N \text{ or } N/2)\cdot\dim_N(n\cdot n') \quad (4.11)$$

for n and n' two coprime numbers.

V. Conclusion

In this paper we have shown how to compute the dimension of the commutant of the extended representation of the modular group carried by the affine characters of the untwisted $SU(N)$ Kac-Moody algebras.

The starting point of our analysis is the characterization of the commutant obtained by Bauer and Itzykson through finite quantum mechanics constructions, already used in the case of $SU(2)$ by Capelli, Itzykson and Zuber. Following their results, the problem of the dimension of the commutant is related to the number of orbits of $SL(2,\mathbb{Z})$ acting on the sets $[Z_n^{N-2}\times Z_{nN}]^2$, where $n=k+N$ is the height of the KM algebra. Using group-theoretic techniques, we have obtained general and explicit formulae, thereby generalizing the known results for $SU(2)$ and $SU(3)$ to any $SU(N)$. The relevance of these expressions to the classification of the affine modular invariants is obvious if one adopts the strategy initiated in [2]. Unfortunately, a fact that one cannot hide is the complexity of the expressions giving the dimensions of the commutant, except in the cases $SU(2)$ and $SU(3)$ where they remain simple.

Acknowledgements. I would like to thank E. Thiran and J. Weyers for valuable discussions and comments during the completion of this work. I am also grateful to J.P. Tignol for discussions about some technicalities of matrix algebra on congruence rings.

References

1. Bernard, D.: Nucl. Phys. B**288**, 628 (1987)
Altschüler, D., Lacki, J., Zaugg, Ph.: Phys. Lett. **205**B, 281 (1988)
Christe, P., Ravanini, F.: Int. J. Mod. Phys. A**4**, 897 (1989)
Bouwknegt, P.: Nucl. Phys. B**290**, 507 (1987)
Moore, G., Seiberg, N.: Nucl. Phys. B**313**, 16 (1989)

2. Capelli, A., Itzykson, C., Zuber, J.B.: Commun. Math. Phys. **113**, 1 (1987)
Kato, A.: Mod. Phys. Lett. A**2**, 585 (1987)
3. Itzykson, C.: Level one Kac-Moody characters and modular invariance. In: Binetruy, P., Sorba, P., Stora, R. (eds.) Conformal field theories and related topics. Nucl. Phys. B Proc. [Suppl.] 5. Amsterdam: North-Holland 1988
4. Bauer, M., Itzykson, C.: Affine characters and modular transformations. Saclay preprint SPhT/89/071, to appear in the Proceedings of Les Houches, March 1989, 'Physique et Théorie des Nombres'. Berlin, Heidelberg, New York: Springer
5. Di Francesco, P., Zuber, J.B.: *SU*(*N*) Lattice integrable models associated with graphs. Saclay preprint, SPhT/89/092
6. Goddard, P., Olive, D.: Int. J. Mod. Phys. A**1**, 303 (1986)
7. Goddard, P., Kent, A., Olive, D.: Commun. Math. Phys. **103**, 105 (1986)
8. Auslander, L., Tolimieri, R.: Bull. Am. Math. Soc. **1**, 847 (1979)
9. Serre, J.P.: Cours d'arithmétique. Paris: Presses Universitaires de France, 1970
10. Ireland, K., Rosen, M.: A classical introduction to modern number theory. Berlin, Heidelberg, New York: Springer 1972
11. Armstrong, M.A.: Groups and symmetry. Berlin, Heidelberg, New York: Springer 1988
12. Apostol, T.A.: Modular functions and Dirichlet series in number theory. Berlin, Heidelberg, New York: Springer 1976
13. Bauer, M., Itzykson, C.: Modular transformations of *SU*(*N*) affine characters and their commutant. Saclay preprint SPhT/89/123

Communicated by K. Gawedzki

Note added in proof. After completion of the manuscript, I received a preprint by Bauer and Itzykson [13], in which Propositions 1 and 2 of [4] are extended and proven to hold for any finite abelian group G. These new results could provide an alternative approach to the calculation of the dimension of the commutant.