Commun. Math. Phys. 127, 617–636 (1990)

Communications in Mathematical Physics

Modular Transformations of $SU(N)$ Affine Characters and Their Commutant

M. Bauer and C. Itzykson

Service de Physique Théorique* de Saclay, F-91191 Gif-sur-Yvette Cedex, France

Abstract. We describe the algebra of matrices commuting with the action of the modular group on characters of $SU(N)_k$ integrable representations. Using methods of finite quantum mechanics we find a canonical basis for this commutant over $\mathbb{C}$ and prove the existence of an equivalent basis over $\mathbb{Q}$ with integral matrix elements. A final section is devoted to the case of $SU(3)$.

1. Introduction

One of the goals in conformal field theory is to classify all rational models. Automorphisms of the algebra of fusion rules and conformal embeddings enable one to construct new modular invariant partition functions from previously known ones. The Wess-Zumino-Witten models associated to simple Lie groups are among the most tractable examples and are believed to be the basic bricks for the construction of all rational theories. However, even in this case it has only been possible to exhibit an exhaustive list of modular invariants in a limited number of instances ($SU(2)_k$ and $SU(N)_1$ and corresponding coset models being the most conspicuous) and the proof of completeness (of arithmetical nature) used methods radically different from the above mentioned ones. In the present work we describe partial results pertaining to a more general situation following the arithmetical path. It is not unlikely that a number of arguments collected in the next sections appear in one form or another in the mathematical literature. We thought it however useful to present them in some detail for a nonexpert reader.

For a simple Lie group and a given level k, the associated Kac-Moody algebra admits only a finite number of integrable representations, with (restricted) characters $\chi_\lambda(\tau)$, indexed by λ, depending on a complex variable τ in the upper half plane $\mathrm{Im}\,\tau > 0$, which carry a unitary representation of the modular group acting on τ [1]. The space of states of the theory decomposes as a sum $\bigoplus_{\lambda,\lambda'} Z_{\lambda,\lambda'} \mathscr{H}_\lambda \otimes \mathscr{H}_{\lambda'}$,

* Laboratoire de l'Institut de Recherche Fondamentale du Commissariat à l'Energie Atomique

where $\mathscr{H}_\lambda$ is an irreducible representation space for the semi direct product of the affine algebra and the Virasoro algebra, and $Z_{\lambda,\lambda'}$ are non-negative integers giving rise to a partition function $Z=\sum_{\lambda,\lambda'} Z_{\lambda,\lambda'}\chi_\lambda(\tau)\overline{\chi_{\lambda'}(\tau)}$. Modular invariance requires the commutation of the representation of the modular group with the matrix $Z_{\lambda,\lambda'}$. A systematic search for such invariants can be carried out in three successive steps of increasing difficulty.

(i) Find a basis for the algebra of matrices commuting with generators S and T of the modular group acting on characters extended by means of the Weyl group.
(ii) Obtain a basis of the subalgebra over rational numbers $\mathbb{Q}$ of the preceding one with integral matrix elements.
(iii) Impose the integrality and positivity condition, taking into account the folding on a fundamental domain.

Restricting ourselves to the case of $SU(N)$ at any level we carry out steps (i) and (ii) proving in fact that the whole commutant has a basis consisting of matrices with integral matrix elements. It is likely that similar properties extend to any affine algebra. For $SU(2)$ see [2].

In the last section we will give some illustrations in the case of $SU(3)$ showing how to express all known invariants in terms of the integral basis using an interpretation of the weight lattice as a quadratic field. A partial account of this work is also presented as a contribution to the proceedings of the Les Houches meeting on "Number Theory and Physics," to be published in Springer Proceedings in Physics, Vol. L 7.

2. Affine $SU(N)$ Characters [1]

Let $\mathbf{e}_\mu$, $\mu=1,2,\ldots,N$, be an orthonormal basis in $\mathbb{R}^N$. One chooses the $N-1$ simple roots of $SU(N)$ equal to the vectors $\boldsymbol{\alpha}_i=\mathbf{e}_i-\mathbf{e}_{i+1}$, $i=1,2,\ldots,N-1$, lying in the hyperplane V orthogonal to $\sum_\mu \mathbf{e}_\mu$. The metric in V is given by the Cartan matrix $g_{ij}=\boldsymbol{\alpha}_i\cdot\boldsymbol{\alpha}_j$ equal to 2, -1, or 0 according to $|i-j|=0,1$ or >1. The simple roots generate the root lattice M, while the dual weight lattice M^* is generated by a basis of $N-1$ fundamental weights $\boldsymbol{\alpha}^i$ such that $\boldsymbol{\alpha}^i\cdot\boldsymbol{\alpha}_j=\delta^i_j$, hence $\boldsymbol{\alpha}^i=g^{ij}\boldsymbol{\alpha}_j$, where g^{ij} is the inverse of the matrix g_{ij}: $\boldsymbol{\alpha}^i\cdot\boldsymbol{\alpha}^j=g^{ij}=\mathrm{Inf}(i,j)-\frac{ij}{N}$. It is readily verified that V, M and M^* are invariant under permutations of the basis vectors $\mathbf{e}_\mu$. The action of these permutations in V is given by products of reflections with respect to hyperplanes orthogonal to the simple roots, giving rise to the Weyl group W of $SU(N)$.

Integrable representations of the corresponding affine Lie algebra at level k (we will call height the integer $n=N+k\geqq N$) are labeled by (strictly) positive weights $\mathbf{p}$ satisfying $p_i=\mathbf{p}\cdot\boldsymbol{\alpha}_i>0$ and $\sum_i p_i<N$. We call B_n this fundamental domain of weights (a simplex). Computing the traces over these representations using the standard gradation generated by the element L_0 in the associated Virasoro algebra of central

charge

$$c=\frac{(N^2-1)k}{N+k}=(N^2-1)\left(1-\frac{N}{n}\right)$$

one defines the (restricted) characters for $\operatorname{Im}\tau>0$ and $\mathbf{p}\in B_n$,

$$\chi_{\mathbf{p}}(\tau)=\operatorname{Tr}_{\mathbf{p}} e\left(\tau\left[L_0-\frac{c}{24}\right]\right),$$

where $e(z)$ stands for $\exp 2i\pi z$. There are $\binom{n-1}{N-1}$ weights in B_n but equivalent weights under charge conjugation (see below) correspond to equal restricted characters. The character formula admits an extension to all $\mathbf{p}$'s in M^*. According to this extension $\chi_{\mathbf{p}}(\tau)$ is antisymmetric in $\mathbf{p}$ under the action of the Weyl group and invariant under translations by elements in the sublattice nM. Taken together the semi-direct product of Weyl transformations and translations in nM form a Euclidean discrete subgroup called the affine Weyl group generated by N reflections in the hyperplanes bounding B_n, which appears as a fundamental domain for its action on non-zero characters.

As stated above when we deal with restricted characters (i.e. ignore a further possible dependence on angles in the Cartan subgroup) there exists a further charge conjugation symmetry. It is the product of the Weyl permutation reversing the order of the basis vectors in $\mathbb{R}^N: \mathbf{e}_\mu\to\mathbf{e}_{N+1-\mu}$, $1\leqq\mu\leqq N\left(\text{of signature } (-1)^{\frac{N(N-1)}{2}}\right)$ with the inversion $\mathbf{p}\to-\mathbf{p}$. It corresponds to the replacement $\boldsymbol{\alpha}^i\to\boldsymbol{\alpha}^{N-i}$ on fundamental weights, hence $c(\mathbf{p})=\Sigma_i p_i\boldsymbol{\alpha}^{N-i}$ and $(C\chi)_{\mathbf{p}}(\tau)=\chi_{c(\mathbf{p})}(\tau)=\chi_{\mathbf{p}}(\tau)$.[1]

At height $n=N$ (level $k=0$), B_n contains a unique element $\mathbf{p}_0$ corresponding to a trivial theory with $\chi_{\mathbf{p}_0}(\tau)\equiv 1$. We have $(\mathbf{p}_0)_i=1$, $1\leqq i\leqq N-1$, $\mathbf{p}_0^2=\dfrac{N(N^2-1)}{12}$.

Characters of integrable representations at a given height exhibit a close relationship with heat kernels (with τ playing the role of time) and share with them the fact that short and large time (corresponding to $\tau\to-\tau^{-1}$) are related. More precisely the characters carry a unitary representation of $SL(2,\mathbb{Z})$ (or $PSL(2,\mathbb{Z})$ if we use restricted characters as we shall do in the sequel). The two generators of the modular group S and T are represented as

$$S\quad \chi_{\mathbf{p}}(-\tau^{-1})=\frac{i^{\frac{N(N-1)}{2}}}{(Nn^{N-1})^{1/2}}\sum_{\mathbf{p}'\in B_n}\left(\sum_{w\in W}\det w\, e\left(-\frac{\mathbf{p}\cdot{}^w\mathbf{p}'}{n}\right)\right)\chi_{\mathbf{p}'}(\tau),$$

$$T\quad \chi_{\mathbf{p}}(\tau+1)=e\left(\frac{\mathbf{p}^2}{2n}-\frac{\mathbf{p}_0^2}{2N}\right)\chi_{\mathbf{p}}(\tau).$$

[1] It is interesting to note that the isometry C on the weight lattice acts as a reflection in a hyperplane when $N=3$ or 4. While the $SU(N)$ characters are even under C the Weyl group can in the above cases be extended to a larger similar group pertaining to the weight lattices for the Lie algebras G_2 in the case $N=3$ or $B_3(SO(7))$ in the case $N=4$. Thus the present work on the $SU(N)$ commutant can presumably be extended to those

Using Gauss's sums one checks that $(ST)^3 = S^2 = C$, $C^2 = 1$, where charge conjugation C acts as the identity on restricted characters. The representative matrices S and T are both unitary and symmetric.

For $\mathbf{p} \in M^*$ and $\mathbf{x} \in V/M$ we define $\psi_{\mathbf{p}}(\mathbf{x}) = \sum_{w \in W} \det w \, e(\mathbf{p} \cdot {}^w\mathbf{x})$ in such a way that for strictly positive weights the classical Weyl formula for $SU(N)$ characters reads

$$ch_{\mathbf{p}}(\mathbf{x}) = \frac{\psi_{\mathbf{p}}(\mathbf{x})}{\psi_{\mathbf{p}_0}(\mathbf{x})} .$$

The S matrix takes the form

$$S_{\mathbf{p},\mathbf{p}'} = \frac{i^{\frac{N(N-1)}{2}}}{(Nn^{N-1})^{1/2}} \overline{\psi_{\mathbf{p}'}\left(\frac{\mathbf{p}}{n}\right)} .$$

From the classical character decomposition

$$ch_{\mathbf{p}_1} ch_{\mathbf{p}_2} = \sum_{\mathbf{p}_3} \mathcal{N}_{\mathbf{p}_1,\mathbf{p}_2}^{\mathbf{p}_3} ch_{\mathbf{p}_3}$$

with $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$ strictly positive, we get by restricting the argument x to the division points $\frac{1}{n} B_n$, the Verlinde fusion rules at height n with $\mathbf{p}, \mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3 \in B_n$,

$$ch_{\mathbf{p}_1}\left(\frac{\mathbf{p}}{n}\right) ch_{\mathbf{p}_2}\left(\frac{\mathbf{p}}{n}\right) = \sum_{\mathbf{p}_3 \in B_n} N_{\mathbf{p}_1,\mathbf{p}_2}^{\mathbf{p}_3} ch_{\mathbf{p}_3}\left(\frac{\mathbf{p}}{n}\right) .$$

The coefficients $N_{\mathbf{p}_1,\mathbf{p}_2}^{\mathbf{p}_3}$ are obviously integers but the folding on B_n as a consequence of the periodicity mod nM in $\mathbf{p}_3$ of $ch_{\mathbf{p}_3}\left(\frac{\mathbf{p}}{n}\right)$ makes it not obvious that they are non-negative.

3. Preliminaries

Before constructing the commutant we collect here some facts concerning the action of the modular group on finite abelian groups.

When the integers $a_1, \ldots, a_l$ are not all zero we denote by $[a_1, \ldots, a_l]$ their greatest common (positive) divisor (we could take zero if all a's are vanishing). Bezout's theorem then implies the existence of integers $b_1, \ldots, b_l$ such that $\Sigma a_i b_i = [a_1, \ldots, a_l] c$ for any integer c. The following property will be useful in the sequel.

Lemma 1. *For any triplet of integers $u, v, w, v \neq 0$, such that $[u, v, w] = 1$, there exists an integer y satisfying $[u + yw, v] = 1$.*

To prove this we assign to each integer x the non-zero divisor of v $\delta_x = [u + xw, v]$. If $[x, u] = 1$, then $[\delta_x, u] = [u + xw, v, u] = [xw, v, u] = [w, v, u] = 1$. Let I denote the set of values δ_x as x runs over integers prime to u. This set is non-empty as $[1, u] = 1$ and $\delta_1 \in I$, and is finite since δ_x divides v. Elements of I, hence their product y are prime to u, consequently $\delta_y \in I$, $[\delta_y, u] = 1$. By the definition of y, δ_y divides y, and it also divides $u + yw$ by the definition of δ_y, thus also u. Being prime to u and positive δ_y has to be equal to one, which means $[u + yw, v] = 1$, concluding the proof.

Now let G be a finite abelian group denoted additively. It is a result of Kronecker's divisor theory[3] that G is isomorphic to a direct product $\mathbb{Z}_{a_1}\times\mathbb{Z}_{a_2}\times\ldots\times\mathbb{Z}_{a_l}$, $(\mathbb{Z}_a\equiv\mathbb{Z}/a\mathbb{Z})$, with a_i dividing a_{i+1} for $i=1,2,\ldots,l-1$. This decomposition is unique, and if $G_1\supset G_2$ the number of factors in G_1 is larger than or equal to the same number in G_2. We shall say that $g_1,\ldots,g_l$ in G is a factorized basis implementing this decomposition if the map j, $\mathbb{Z}^l\to G$, given by $(\lambda_1,\ldots,\lambda_l)\to\Sigma\lambda_i g_i$ is onto with a kernel $a_1\mathbb{Z}\times\ldots\times a_l\mathbb{Z}$.

The ring $\mathbb{M}_2(\mathbb{Z})$ of 2×2 matrices with integral entries acts on $G\times G$ through right multiplication as $(g,g')\to(ag+cg',bg+dg')$, for $(g,g')\in G\times G$ and $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathbb{M}_2(\mathbb{Z})$. Hence a fortiori $SL(2,\mathbb{Z})$ acts on $G\times G$. To any pair $h,h'\in G$ let us associate the subgroup $H\subset G$ that they generate (obviously h and h' belong to H). The subgroup H is invariant when the ordered pair (h,h') is replaced by any other one deduced by the (right) action of $SL(2,\mathbb{Z})$. Thus in general we can talk of the subgroup H associated to the $SL(2,\mathbb{Z})$ orbit of an ordered pair $(h,h')\in G\times G$ (the pairs (h,h') and (h',h) generate the same subgroup H but are not related (in general) by an $SL(2,\mathbb{Z})$ transformation, thus we could instead act with $GL(2,\mathbb{Z})$). Obviously $H\times H$ is also stable under $SL(2,\mathbb{Z})$, and we will give in the following a classification of its orbits in $H\times H$, distinguishing those with associated subgroup equal precisely to H, which we assume $\neq\{0\}$.

The subgroup H generated by (h,h') is isomorphic to some direct product $\mathbb{Z}_p\times\mathbb{Z}_{pq}$ for p and q positive integers not both equal to 1. This means that we can find a factorized basis $g,g'\in H$ implementing this decomposition. By construction for any pair $(f,f')\in H\times H$ there exists a matrix $M\in\mathbb{M}_2(\mathbb{Z})$ such that $(f,f')=(h,h')M$, in other words with $M=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$, $(f,f')=(ah+ch',bh+dh')$, and of course M is not unique.

Lemma 2. (i) $\det M$ *is well defined* $\bmod p$.
(ii) *If the pair* (f,f') *also generates* H, *given any integer* m *one can find a second matrix* $\tilde{M}\in\mathbb{M}_2(\mathbb{Z})$ *such that* $(f,f')=(h,h')\tilde{M}$ *and* $\det\tilde{M}=\det M+pm$.

To prove the first point we note that since the factorized pair (g,g') also generates H we have both $(g,g')=(h,h')M$ and $(h,h')=(g,g')N$, thus $(g,g')=(g,g')NM$, i.e. $NM=I+\begin{pmatrix}p & 0\\ 0 & pq\end{pmatrix}R$ with R an integral matrix. Hence $NM\equiv I\bmod p$, $\det N\det M\equiv 1\bmod p$ and any other choice $\tilde{M}$ will lead to the same determinant $(\det N)^{-1}\bmod p$, an element in $\mathbb{Z}_p^*$, the set of invertible elements $\bmod p$, with the convention that $\mathbb{Z}_1^*=\mathbb{Z}_1=\{0\}$. For any other pair (f,f') and any choices $(f,f')=(h,h')M=(h,h')\tilde{M}$ we have $(g,g')NM=(g,g')N\tilde{M}$, hence as before $NM=N\tilde{M}\bmod p$. Taking determinants and using the fact that $\det N\in\mathbb{Z}_p^*$ we conclude that $\det M\equiv\det\tilde{M}\bmod p$.

To prove the second point we use again (g,g') a factorized basis in an intermediate step. Assume that (f,f') also generates H. Thus $(f,f')=(g,g')M$ and $(g,g')=(f,f')\bar{M}$ for some $\bar{M}$. Given any integer m we want to show the existence of another integral matrix $\tilde{M}$ with the property that $(f,f')=(g,g')\tilde{M}$ and $\det\tilde{M}=\det M+pm$. Setting $M=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ and knowing that $\tilde{M}-M$ has to be of

the form $\begin{pmatrix} p & 0 \\ 0 & pq \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ we translate these conditions into

$$(A) \quad pq(\alpha\delta-\beta\gamma)+d\alpha+qa\delta-c\beta-qb\gamma=m \ .$$

From $(g,g')M\bar{M}=(g,g')$ and looking at the lower right element of $M\bar{M}$ we deduce the existence of two integers $\bar{b}$ and $\bar{d}$ such that $c\bar{b}+d\bar{d}\equiv 1 \bmod pq$ proving that $(c,d)\neq(0,0)$ and $[c,d,pq]=1$. Assume $c\neq 0$ (a similar argument is valid if $d\neq 0$). We use the first lemma to pick δ such that $[c,d+pq\delta]=1$ and set $\gamma=0$. Condition (A) reduces to $\alpha(d+pq\delta)-\beta c=m-aq\delta$ which admits a solution in α,β since from the above c and $d+pq\delta$ are relatively prime. We now replace the factorized basis (g,g') by an arbitrary pair (h,h') generating H, thus $(h,h')=(g,g')N$. Taking any Δ such that $\Delta \det N\equiv 1 \bmod p$ we can write $(h,h')=(\det N\, g,g')\begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix}N$. Clearly $(\det N\, g,g')$ is also a factorized basis, so that changing (g,g') into $(\det N\, g,g')$ and N into $\begin{pmatrix} \Delta & 0 \\ 0 & 1 \end{pmatrix}N$, we can henceforth assume $(h,h')=(g,g')N$, $\det N\equiv 1 \bmod p$. From the above we can even choose an equivalent matrix, call it N again, such that N belongs to $SL(2,\mathbb{Z})$. If now (f,f') is yet another pair generating H we have $(f,f')=(h,h')M=(g,g')NM$. Again from the above we know that given the integer m, L exists with the property that $(f,f')=(g,g')L$ and $\det L=\det NM+pm$ $=\det M+pm$. But N is invertible and setting $\tilde{M}=N^{-1}L$ we have $(f,f')=(g,g')L$ $=(h,h')\tilde{M}$ and $\det\tilde{M}=\det L=\det M+pm$ concluding the proof. We note that if two elements in $SL(2,\mathbb{Z})$ are called equivalent when the two matrices have equal entries mod p (written $M\sim \mathrm{M}'$) the above reasoning for $q=1$ yields a proof of the well known isomorphism between $SL(2,\mathbb{Z})/\sim$ and $SL(2,\mathbb{Z}_p)$.

As a corollary we obtain that in $G\times G$ there are exactly $\varphi(p)=\mathrm{Card}\,\mathbb{Z}_p^*$ orbits with associated subgroup H (recall that $H\cong\mathbb{Z}_p\times\mathbb{Z}_{pq}$). Indeed if two pairs on distinct orbits (h,h') and (f,f') generate H then $(f,f')=(h,h')M$ and from the second part of the lemma $\det M\equiv 1 \bmod p$ would contradict the hypothesis while we know that $\det M\in\mathbb{Z}_p^*$. Thus there can be at most $\varphi(p)$ such distinct orbits while if (g,g') is a factorized basis for H and σ is any integer invertible mod p, $(\sigma g,g')$ gives at least $\varphi(p)$ representative points on distinct orbits.

More generally we are interested in classifying all orbits under $SL(2,\mathbb{Z})$ included in $H\times H$, i.e. also those that generate subgroups of H. Take a factorized basis (g,g') in H. When matrices M act to the right on such a row vector we now understand that their first line is mod p their second mod pq when no confusion is possible. Set $M=\begin{pmatrix} \bar{x} & \bar{y} \\ \bar{x}' & \bar{y}' \end{pmatrix}$. Clearly $\delta=[\bar{x},\bar{y},p]$ and $\delta'=[\bar{x}',\bar{y}',pq]$ are well defined and invariants of the right $SL(2,\mathbb{Z})$ orbit associated to $(g,g')M$. Writing $\bar{x}=\delta x$, $\bar{y}=\delta y$, $\bar{x}'=\delta' x'$ and $\bar{y}'=\delta' y'$ we deal exclusively in the sequel with the $SL(2,\mathbb{Z})$ orbit generated by $(g,g')M=(\delta g,\delta' g')\begin{pmatrix} x & y \\ x' & y' \end{pmatrix}$. If we define $r=p/\delta$, $s=pq/\delta'$ (of course r will not divide s in general) and remark that $(\delta g,\delta' g')$ is a factorized basis for a group isomorphic to $\mathbb{Z}_r\times\mathbb{Z}_s$ we can forget about δ and δ' for the time being. and assume $x,y \bmod r$, $x',y' \bmod s$ such that $[x,y,r]=[x',y',s]=1$.

We then define ϱ and κ through $\varrho=[r,s]$ and $\kappa\varrho=rs$. The determinant $\Delta=xy'-yx'$ is well defined mod ϱ and is obviously an invariant of the orbit.

By hypothesis the equation $xu+yv\equiv 1 \bmod r$ admits solutions. We pick one of them and denote by Ω' the quantity $x'u+y'v$.

Lemma 3. (i) *Ω' is well defined and invertible* mod $[\Delta,\varrho]$ (i.e. *one can find $\Omega\in\mathbb{Z}^*_{[\Delta,\varrho]}$ such that $\Omega\Omega'\equiv 1 \bmod [\Delta,\varrho]$*).
(ii) *$\Omega' \bmod [\Delta,\varrho]$ is an invariant of the corresponding orbit (hence also its inverse $\Omega \bmod [\Delta,\varrho]$).*

Let $xu_0+yv_0\equiv xu+yv\equiv 1 \bmod r$. Setting $\Omega'_0=x'u_0+y'v_0$, $\Omega'=x'u+y'v$, we have

$$\begin{pmatrix} x & y \\ x' & y' \end{pmatrix}\begin{pmatrix} u_0 & u \\ v_0 & v \end{pmatrix}\equiv\begin{pmatrix} 1 & 1 \\ \Omega'_0 & \Omega' \end{pmatrix},$$

where equality is mod r for the first line and mod s for the second. Hence the determinant of both sides is well defined mod $\varrho=[r,s]$ and we find $\Omega'-\Omega'_0 \equiv\Delta(u_0v-uv_0) \bmod \varrho$ showing that Ω' is well defined mod $[\varrho,\Delta]$.

If we interchange the roles of x, y and x', y' we also define an integer $\Omega \bmod [\varrho,\Delta]$. We deduce from the set of relations $xu+yv\equiv 1 \bmod r$ $\Omega'=x'u+y'v$, $x'\bar{u}+y'\bar{v}\equiv 1 \bmod s$ and $\Omega=x\bar{u}+y\bar{v}$ that

$$\begin{pmatrix} x & y \\ x' & y' \end{pmatrix}\begin{pmatrix} u & \bar{u} \\ v & \bar{v} \end{pmatrix}\equiv\begin{pmatrix} 1 & \Omega \\ \Omega' & 1 \end{pmatrix} \bmod [\varrho,\Delta]$$

which is obviously unchanged if we substitute $\begin{pmatrix} x & y \\ x' & y' \end{pmatrix}A$ for $\begin{pmatrix} x & y \\ x' & y' \end{pmatrix}$ and $A^{-1}\begin{pmatrix} u & \bar{u} \\ v & \bar{v} \end{pmatrix}$ for $\begin{pmatrix} u & \bar{u} \\ v & \bar{v} \end{pmatrix}$ with $A\in SL(2,\mathbb{Z})$ from which we deduce (i) that $1-\Omega\Omega'\equiv 0 \bmod [\varrho,\Delta]$ by taking determinants and recalling that $\det\begin{pmatrix} x & y \\ x' & y' \end{pmatrix}=\Delta$ and (ii) that Ω and Ω' are invariants of the orbit.

Theorem 1. *The four invariants δ a divisor of p, δ' a divisor of pq, Δ* mod $[p/\delta, pq/\delta']$ *and Ω in $\mathbb{Z}^*_{[p/\delta',pq/\delta',\Delta]}$ as defined above characterise an orbit*, i.e. *two pairs in $H\times H$ with the same invariants are related by an $SL(2,\mathbb{Z})$ transformation.*

As was seen before the dependence on δ and δ' factorizes and we can deal with the orbits of pairs of elements in a subgroup of H isomorphic to $\mathbb{Z}_r\times\mathbb{Z}_s$ of the form $(\delta g,\delta' g')\begin{pmatrix} x & y \\ x' & y' \end{pmatrix}$ with $x,y \bmod r=p/\delta$, $x',y' \bmod s=qp/\delta'$ and $[x,y,r]=[x',y',s]=1$. Using Lemma 1 we substitute if necessary for x', y' an equivalent pair of integers again denoted by x', y', shifted possibly by multiples of s such that $[x',y']=1$. This ensures the existence of two integers z and t such that the matrix

$$K=\begin{pmatrix} y' & z \\ -x' & t \end{pmatrix}$$

belongs to $SL(2,\mathbb{Z})$. Acting on the right with K on M yields an equivalent matrix with elements on the second row equal to 0 and 1 respectively. So up to equivalence

we can assume M of the form $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ and the problem is reduced to showing that two matrices

$$\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} X & Y \\ 0 & 1 \end{pmatrix}$$

correspond to the same orbit if and only if they have the same invariants Δ and Ω, which amounts to saying that $x \equiv X \bmod [r,s]$ and $y = Y \bmod [x,r,s]$, and we recall that $[x,y,r]=[X,Y,r]=1$. This implies that one can find integers μ, ν, σ, τ such that

$$\text{(B)} \quad x[r,s]\mu + ys\nu \equiv X - x \bmod r \ ,$$

$$\text{(C)} \quad x\sigma + ys\tau \equiv Y - y \bmod r \ .$$

Indeed from $[x[r,s], ys, r] = [r,s]\left[x, y\frac{s}{[r,s]}, \frac{r}{[r,s]}\right] = [r,s]\left[x, y, \frac{r}{[r,s]}\right] = [r,s]$ and $X - x \equiv 0 \bmod [r,s]$ it follows that $X-x$ can be represented as a linear combination of $x[r,s]$, ys, and r as expressed by (B). Similarly from $[x, ys, r] = [[x,r], ys] = [x, rs]$ (the second equality being due to the fact that $[[x,r], y] = 1$) and $Y - y \equiv 0 \bmod [x,r,s]$ it follows similarly that $Y-y$ can be expressed as a linear combination of x, ys and r as shown in (C). It is then readily verified that

$$\text{(D)} \quad \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} M = \begin{pmatrix} X & Y \\ 0 & 1 \end{pmatrix} \quad \text{with} \quad M = \begin{pmatrix} 1+[r,s]\mu & \sigma \\ s\nu & 1+s\tau \end{pmatrix} ,$$

the equality being understood first line mod r second line mod s. The two matrices play a similar role, hence we can also find an integral matrix with a similar property

$$\begin{pmatrix} X & Y \\ 0 & 1 \end{pmatrix} M' = \begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix} .$$

This proves that when acting on the factorized basis the two matrices $\begin{pmatrix} x & y \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} X & Y \\ 0 & 1 \end{pmatrix}$ generate the same subgroup of $\mathbb{Z}_r \times \mathbb{Z}_s$. This subgroup $\tilde{H}$ is of the form $\mathbb{Z}_u \times \mathbb{Z}_{uv}$ with u dividing $[r,s]$ and we note that the above matrix M constructed in (D) verifies $\det M \equiv 1 \bmod [r,s]$ and a fortiori $\bmod u$. The proof of Lemma 2 with $\tilde{H}$ playing the role of H implies the existence of a matrix equivalent to M of determinant equal to 1, hence in $SL(2,\mathbb{Z})$ which completes the proof of the theorem.

As a special case let the abelian group G be isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_{pq}$ and the prime factorizations of p and q be written

$$p = \prod_i P_i^{\alpha_i} \ , \qquad q = \prod_i P_i^{\beta_i} \ ,$$

where P_i run over a finite set of primes. We have the following.

Corollary. *For G as above the number of orbits in $G \times G$ under $SL(2,\mathbb{Z})$ is equal to*

$$p \prod_i \left[(\alpha_i+1)(\beta_i+1) + \frac{1}{P_i} \alpha_i (1-\beta_i) \right] .$$

The proof relies on the factorization of arithmetical properties for distinct primes so that it is sufficient to establish the result for $p=P^{\alpha}$ and $q=P^{\beta}$ and then take the product over primes, $N=\prod_i N_{P_i}$.

We have first to choose $\delta=P^d$, $\delta'=P^{d'}$ with $0\leqq d\leqq\alpha$, $0\leqq d'\leqq\alpha+\beta$. Then with $c=\inf(\alpha-d,\alpha+\beta-d')$, Δ is in $\mathbb{Z}_{p^c}$ of the form $P^b\Delta_0$, $\Delta_0\in\mathbb{Z}^*_{p^{c-b}}$. Finally Ω is in $\mathbb{Z}^*_{p^b}$. So the required number of choices is

$$N_P=\sum_{d=0}^{\alpha}\sum_{d'=0}^{\alpha+\beta}\sum_{b=0}^{\inf(\alpha-d,\alpha+\beta-d')}\varphi(P^b)\varphi(P^{\inf(\alpha-d,\alpha+\beta-d')-b}) ,$$

where $\varphi_n=\mathrm{Card}\,\mathbb{Z}^*_n(\varphi(1)\equiv 1)$ and explicitly for P a prime and $m>0$, $\varphi(P^m)=P^m\left(1-\frac{1}{P}\right)$. We rewrite the sum as

$$N_P=\sum_{c=0}^{\alpha}\sum_{\substack{0\leqq d\leqq\alpha\\ 0\leqq d'\leqq\alpha+\beta\\ c=\inf(\alpha-d,\alpha+\beta-d')}}\sum_{b=0}^{c}\varphi(P^b)\varphi(P^{c-b}) .$$

The middle sum yields a factor $2\alpha+\beta+1-2c$. We then split the sum over c into $c=0$ (hence $b=0$) and $c>0$ and in this case distinguish the terms with $b=0$ or c from those with $0<b<c$ getting

$$2\alpha+\beta+1+\sum_{c=1}^{\alpha}(2\alpha+\beta+1-2c)\left\{P^c 2\left(1-\frac{1}{P}\right)+(c-1)\left(1-\frac{1}{P}\right)^2\right\} .$$

The bracket is equal to $(c+1)P^c-2cP^{c-1}+(c-1)P^{c-2}$ so that the summand can be rewritten

$$\{(2\alpha+\beta+1)[(c+1)P^c-cP^{c-1}]-2c(c+1)[P^c-P^{c-1}]\}-\{c\to c-1\} ,$$

leading after summation over c to the expected result for N,

$$\begin{aligned}N_P&=(2\alpha+\beta+1)[(\alpha+1)P^{\alpha}-\alpha P^{\alpha-1}]-2\alpha(\alpha+1)[P^{\alpha}-P^{\alpha-1}]\\&=P^{\alpha}[(\alpha+1)(\beta+1)+\alpha(1-\beta)P^{-1}] .\end{aligned}$$

4. Finite Quantum Mechanics and the Commutant

As was mentioned in Sect. 2 the characters as well as the matrices S and T admit a natural extension to the whole weight lattice M^* with invariance under translations belonging to the sublattice nM. This allow one to consider S and T as acting as unitary operators on a finite dimensional Hilbert space with a basis indexed by the elements of the abelian group M^*/nM. This extension implies that for any element of the Weyl group

$$\chi_{\omega\mathbf{p}}(\tau)=\det\omega\chi_{\mathbf{p}}(\tau) ,$$

hence for $\mathbf{p}\in M^*/nM$

$$S\quad \chi_{\mathbf{p}}(-\tau^{-1})=\frac{i^{\frac{N(N-1)}{2}}}{(Nn^{N-1})^{1/2}}\sum_{\mathbf{p}'\in M^*/nM} e\left(-\frac{\mathbf{p}\cdot\mathbf{p}'}{n}\right)\chi_{\mathbf{p}'}(\tau)\ ,$$

$$T\quad \chi_{\mathbf{p}}(\tau+1)=e\left(\frac{\mathbf{p}^2}{2n}-\frac{\mathbf{p}_0^2}{2N}\right)\chi_{\mathbf{p}}(\tau)\ .$$

Let us introduce a Hilbert space E with orthonormal basis $|\mathbf{p}\rangle$, $\mathbf{p}\in M^*/nM$ and for convenience now rescale scalar products in M^* (and $M\subset M^*$) by a factor N so as to deal only with integers. We also redefine S and T by dropping irrelevant phases as operators in E such that

$$S|\mathbf{p}\rangle=\frac{1}{(Nn^{N-1})^{1/2}}\sum_{\mathbf{p}'} e\left(-\frac{\mathbf{p}\cdot\mathbf{p}'}{nN}\right)|\mathbf{p}'\rangle\ ,$$

$$T|\mathbf{p}\rangle=e\left(\frac{\mathbf{p}^2}{2nN}\right)|\mathbf{p}\rangle\ .$$

With a redefinition of C as the unitary matrix such that $C|\mathbf{p}\rangle=|-\mathbf{p}\rangle$, we have $S^2=C$ and obviously C commutes with S and T. The point is until we reinstate the antisymmetry of characters under the Weyl group, the search for this enlarged commutant is unsensitive to extra global phases in the various operators (reflecting a similar property in quantum mechanics). It is worth pointing out that T and S are indeed well defined on M^*/nM, since with the rescaled definition of scalar products if $\mathbf{p}\in M^*$ and $\mathbf{r}\in M$, $\mathbf{p}\cdot\mathbf{r}\in N\mathbb{Z}$ and $\mathbf{r}^2\in 2N\mathbb{Z}$. The key idea in constructing the commutant is to identify S and T as generators of a group of canonical transformations on an appropriate (and natural) set of conjugate operators identifying the action of the modular group with the metaplectic group of finite quantum mechanics. For this purpose we introduce the analogues of conjugate canonical variables (or rather their exponentials) as follows. Define for each $\mathbf{p}\in G_n=M^*/nM$ operators $P^{\mathbf{p}}$ and $Q^{\mathbf{p}}$ through

$$P^{\mathbf{p}}|\mathbf{p}'\rangle=|\mathbf{p}+\mathbf{p}'\rangle\ ,\qquad Q^{\mathbf{p}}|\mathbf{p}'\rangle=e\left(\frac{\mathbf{p}\cdot\mathbf{p}'}{nN}\right)|\mathbf{p}'\rangle\ .$$

The maps $\mathbf{p}\to P^{\mathbf{p}}$ and $\mathbf{p}\to Q^{\mathbf{p}}$ are unitary representations of G_n in $\mathrm{End}\,(E)(P^0=Q^0=I)$ intertwined by S the finite Fourier transform and verify the fundamental commutation rules

$$P^{\mathbf{p}'}Q^{\mathbf{p}}=e\left(-\frac{\mathbf{p}\cdot\mathbf{p}'}{nN}\right)Q^{\mathbf{p}}P^{\mathbf{p}'}\ .$$

This implies that these operators generate a representation of the finite Heisenberg group, a central extension of $G_n\times G_n$ by $\mathbb{Z}_{nN}$. This representation is irreducible and one verifies easily that the products $P^{\mathbf{p}'}Q^{\mathbf{p}}$ form a basis of $\mathrm{End}\,(E)$ in these sense that for any operator V with $|G_n|=\mathrm{Card}\,G_n$,

$$V=|G_n|^{-1}\sum_{\mathbf{p},\mathbf{p}'} P^{\mathbf{p}}Q^{\mathbf{p}'}\,\mathrm{Tr}\,(Q^{-\mathbf{p}'}P^{-\mathbf{p}}V)\ .$$

A simple calculation yields the adjoint action of S and T on P's and Q's,

$$S^\dagger P^{\mathbf{p}} S = Q^{\mathbf{p}} , \qquad S^\dagger Q^{\mathbf{p}} S = P^{-\mathbf{p}} ,$$

$$T^\dagger P^{\mathbf{p}} T = e\left(\frac{\mathbf{p}^2}{2nN}\right) P^{\mathbf{p}} Q^{-\mathbf{p}} , \qquad T^\dagger Q^{\mathbf{p}} T = Q^{\mathbf{p}} .$$

There exists a natural projection from G_{2n} to G_n (reduction of $\mathbf{p}$ mod $M^*/2nM$ to mod M^*/nM) and a map from $G_n \times G_n$ to Z_{nN} given by the scalar product assigning $\mathbf{p}\cdot\mathbf{p}'$ to a pair $\mathbf{p}, \mathbf{p}'$ in such a way that the following diagram is commutative

$$\begin{array}{ccc} G_{2n} \times G_{2n} & \to & \mathbb{Z}_{2nN} \\ \downarrow & & \downarrow \\ G_n \times G_n & \to & \mathbb{Z}_{nN} \end{array}$$

Let ξ stand for $e\left(\frac{1}{2nN}\right)$ a primitive $2nN$-th root of unity and for $\mathbf{k}, \mathbf{k}'$ in G_{2n} with projections $\mathbf{p}, \mathbf{p}'$ in G_n set

$$\{\mathbf{k}, \mathbf{k}'\} = \xi^{\mathbf{k}\cdot\mathbf{k}'} P^{\mathbf{p}} Q^{\mathbf{p}'} ,$$

$$\{\mathbf{k}, \mathbf{k}'\}^\dagger = \{-\mathbf{k}, -\mathbf{k}'\} .$$

Even though for any V we still have $\{\mathbf{k}, \mathbf{k}'\} \operatorname{Tr}(\{-\mathbf{k}, -\mathbf{k}'\} V) = P^{\mathbf{p}} Q^{\mathbf{p}'} \operatorname{Tr}(Q^{-\mathbf{p}'} P^{-\mathbf{p}} V)$ so that the full set of elements $\{\mathbf{k}, \mathbf{k}'\}$ still generates End (E) they are not linearly independent any more with two elements proportional if and only if the projections of their labels on $G_n \times G_n$ are equal.

The purpose of this definition is to make the action of S and T more transparent. One readily verifies that

$$S^\dagger \{\mathbf{k}, \mathbf{k}'\} S = \{-\mathbf{k}', \mathbf{k}\}$$

$$T^\dagger \{\mathbf{k}, \mathbf{k}'\} T = \{\mathbf{k}, \mathbf{k}' - \mathbf{k}\} .$$

Using the one to one correspondence between an ordered pair $(\mathbf{k}, \mathbf{k}')$ in $G_{2n} \times G_{2n}$ and an operator $\{\mathbf{k}, \mathbf{k}'\}$ in E we see that the adjoint action of S and T can be interpreted as multiplication to the right by the matrices $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ of the corresponding pair $(\mathbf{k}, \mathbf{k}')$ in $G_{2n} \times G_{2n}$. These operations generates an action of $SL(2, \mathbb{Z})$ which factors through a finite quotient group. Averaging over this finite group yields all elements of the required commutant.

Using the notations of Sect. 2 one checks that as a lattice over integers M^* admits a basis $\alpha^1, \alpha_1, \ldots, \alpha_{N-2}$ (reduced to α^1 if $N=2$) from which it follows that as an additive group M^*/nM is isomorphic to $\mathbb{Z}_{nN} \times \mathbb{Z}_n^{N-2}$. This proves, using a remark in Sect. 3 that the effective action is at most $SL(2, \mathbb{Z})$ mod $2nN$, i.e. $SL(2, \mathbb{Z}_{2nN})$. With $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $SL(2, \mathbb{Z}_{2nN})$, we write $\{\mathbf{k}, \mathbf{k}'\} K$ for $\{a\mathbf{k} + c\mathbf{k}', b\mathbf{k} + d\mathbf{k}'\}$. Thus

$$\sum_{K \in SL(2, \mathbb{Z}_{2nN})} \{\mathbf{k}, \mathbf{k}'\} K$$

commutes with S and T. On the other hand if an operator V commutes with S and T it commutes with the action of any element in $SL(2,\mathbb{Z})$, hence easily

$$V=\frac{1}{|G_{2n}|}\frac{1}{|SL(2,\mathbb{Z}_{2nN})|}\sum_{K,\mathbf{k},\mathbf{k}'}\{\mathbf{k},\mathbf{k}'\}K\,\mathrm{Tr}\,(\{-\mathbf{k},-\mathbf{k}'\}V)\ ,$$

showing that the above elements generate the commutant. What is left is to find a basis in this family.

First of all the elements generating the commutant only depend on $(\mathbf{k},\mathbf{k}')$ through its orbit under the action of $SL(2,\mathbb{Z})$ (to the right). So for $\mathcal{O}$ an orbit in $G_{2n}\times G_{2n}$ we set

$$I_{\mathcal{O}}=\sum_{(\mathbf{k},\mathbf{k}')\in\mathcal{O}}\{\mathbf{k},\mathbf{k}'\}\ ,$$

which differs only by a constant (the order of the isotropy group of a "point" on the orbit) from the generating element introduced above.

Next we want to relate orbits in $G_{2n}\times G_{2n}$ to orbits in $G_n\times G_n$. Let $(\mathbf{p},\mathbf{p}')$ be the projection in $G_n\times G_n$ of $(\mathbf{k},\mathbf{k}')$ in $G_{2n}\times G_{2n}$ and consider $K=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in SL(2,\mathbb{Z}_{2nN})$. We check that $(a\mathbf{k}+c\mathbf{k}')(b\mathbf{k}+d\mathbf{k}')-\mathbf{k}\cdot\mathbf{k}'\equiv ab\mathbf{p}^2+cd\mathbf{p}'^2-2bc\mathbf{p}\cdot\mathbf{p}'\bmod 2nN$, meaning that $\xi^{(a\mathbf{k}+c\mathbf{k}')\cdot(b\mathbf{k}+d\mathbf{k}')-\mathbf{k}\cdot\mathbf{k}'}$ depends only on the projection of $(\mathbf{k},\mathbf{k}')$ on $G_n\times G_n$. This proves that if two pairs $(\mathbf{k},\mathbf{k}')$ and $(\mathbf{l},\mathbf{l}')$ in $G_{2n}\times G_{2n}$ belong to the orbits $\mathcal{O}_1$ and $\mathcal{O}_2$ and have identical projection $(\mathbf{p},\mathbf{p}')$, then $I_{\mathcal{O}_1}\xi^{-\mathbf{k}\cdot\mathbf{k}'}=I_{\mathcal{O}_2}\xi^{-\mathbf{l}\cdot\mathbf{l}'}$, Hence $I_{\mathcal{O}_1}$ and $I_{\mathcal{O}_2}$ differ at most by a phase. On the other hand if $(\mathbf{q},\mathbf{q}')$ lies on the orbit of $(\mathbf{p},\mathbf{p}')$ in $G_n\times G_n$ there exists a matrix $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ in $SL(2,\mathbb{Z})$ such that $(\mathbf{q},\mathbf{q}')=(\mathbf{p},\mathbf{p}')\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$. Let $(\mathbf{k},\mathbf{k}')$ be a lift of $(\mathbf{p},\mathbf{p}')$ in $G_{2n}\times G_{2n}$, then $(\mathbf{k},\mathbf{k}')\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ projects on $(\mathbf{q},\mathbf{q}')$ proving that up to phases there exists a unique invariant for each orbit in $G_n\times G_n$. Disjoint orbits involve distinct sets of monomials $P^{\mathbf{p}}Q^{\mathbf{p}'}$, proving that the set of non-vanishing invariants attached to orbits in $G_n\times G_n$ form a linearly independent basis of the commutant (over $\mathbb{C}$).

An element of the commutant attached to an orbit in $G_n\times G_n$ can vanish only if the distinct terms projecting on the same pair at each point conspire to give zero. Consider all pairs $(\mathbf{k},\mathbf{k}')$, $(\mathbf{l},\mathbf{l}')\ldots$ projecting on the same pair $(\mathbf{p},\mathbf{p}')$ in $G_n\times G_n$ and lying on the same orbit $\mathcal{O}$. Then either $I_{\mathcal{O}}$ is zero or else they satisfy $\xi^{\mathbf{k}\cdot\mathbf{k}'}=\xi^{\mathbf{l}\cdot\mathbf{l}'}=\ldots$. If this condition is satisfied the contribution of the term $P^{\mathbf{p}}Q^{\mathbf{p}'}$ in $I_{\mathcal{O}}$ cannot be compensated by any other one and $I_{\mathcal{O}}$ cannot vanish. On the other hand let $(\mathbf{k},\mathbf{k}')$ belong to $\mathcal{O}$ and assume that $(\mathbf{k},\mathbf{k}')\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ as the same projection in $G_n\times G_n$, for $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ in $SL(2;\mathbb{Z}_{2nN})$. Write

$$\mathbf{k}=x_0\boldsymbol{\alpha}^1+\sum_1^{N-2}x_i\boldsymbol{\alpha}_i\ ,\qquad \mathbf{k}'=y_0\boldsymbol{\alpha}^1+\sum_1^{N-2}y_i\boldsymbol{\alpha}_i\ .$$

The assumptions are

$$(x_0, y_0)\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} - I\right] \equiv 0 \bmod nN \ ,$$

$$(x_i, y_i)\left[\begin{pmatrix} a & b \\ c & d \end{pmatrix} - I\right] \equiv 0 \bmod n \quad 1 \leqq i \leqq N-2 \ .$$

Let us compute the difference in scalar products modulo $2nN$. We have

$$\begin{aligned}(a\mathbf{k}+c\mathbf{k}')\cdot(b\mathbf{k}+d\mathbf{k}')-\mathbf{k}\cdot\mathbf{k}' &= (N-1)[ax_0+cy_0)(by_0+dy_0)-x_0y_0] \\ &+N[(ax_0+cy_0)(bx_1+dy_1)-x_0y_1+(bx_0+dy_0)(ax_1+cy_1)-y_0x_1] \\ &-N\sum_{i=1}^{N-3}[(ax_i+cy_i)(bx_{i+1}+dy_{i+1})-x_iy_{i+1} \\ &+(bx_i+dy_i)(ax_{i+1}+cy_{i+1})-y_ix_{i+1}] \\ &+2N\sum_{i=1}^{N-2}[(ax_i+cy_i)(bx_i+dy_i)-x_iy_i)] \ .\end{aligned}$$

By assumption the last term vanishes $\bmod 2nN$. Furthermore from $\alpha nN \equiv -\alpha nN \bmod 2nN$ we can change the sign of the combination $(bx_i+dy_i)\cdot(ax_{i+1}+cy_{i+1})-y_ix_{i+1}$ for $i=0,1,\ldots,N-3$ in the second and third term on the right-hand side and use $ad-bc=1$ to show that they vanish $\bmod 2nN$ so that we are left with

$$(a\mathbf{k}+c\mathbf{k}'\cdot b\mathbf{k}+d\mathbf{k}')-\mathbf{k}\cdot\mathbf{k}' \equiv (N-1)[(ax_0+cy_0)(bx_0+dy_0)-x_0y_0] \bmod 2nN \ ,$$

and the condition that $(ax_0+cy_0)(bx_0+dy_0)-x_0y_0 \equiv 0 \bmod nN$. If N is odd the right-hand side vanishes $\bmod 2nN$. If N is even the matrix $\begin{pmatrix} 1 & \beta nN \\ \gamma nN & 1 \end{pmatrix}$ of determinant $1+\beta\gamma n^2N^2 \equiv 1 \bmod 2nN$ (since N is even) can be lifted to a matrix in $SL(2,\mathbb{Z})$ and hence can be used for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in the above since it obviously transforms $(\mathbf{k},\mathbf{k}')$ into a pair with equal projection. Then the above difference in scalar products becomes $(\beta x_0^2+\gamma y_0^2)nN$. For β and γ arbitrary this expression is always zero $\bmod 2nN$ if and only if x_0 and y_0 are both even. Since N is even this condition on x_0y_0 is invariant along the orbit and under projection on $G_n \times G_n$. One sees easily that it is equivalent to saying that a pair $(\mathbf{p},\mathbf{p}')$ in $G_n \times G_n$ is such that $\mathbf{p}^2 \equiv \mathbf{p}'^2 \equiv 0 \bmod 4$ (consistent with the fact that $\mathbf{p}^2$ or $\mathbf{p}'^2$ is defined $\bmod 2nN$, a multiple of 4 for N even), a condition invariant under $SL(2,\mathbb{Z})$ along the orbit. Calling such orbits even we conclude that

Theorem 2. *If N is odd to every orbit in $G_n \times G_n$ we associate an element of the commutant, well defined up to a phase. These elements are linearly independent and generate the commutant. If N is even the same is true provided one restricts oneself to even orbits.*

We have thus succeeded to obtain a basis of the commutant over $\mathbb{C}$ even though the construction (not to mention the enumeration) is not as straightforward as one

might wish. However for small values of N one can be much more specific, as will be shown in the following section.

For the time being we will prove a stronger result using the analysis of Sect. 3. While the above construction is in a sense canonical (up to phases) it produces matrices with complex entries in general (in the standard basis of E, the one that is relevant). But it is possible to show that

Theorem 3. *By a linear transformation one can find an equivalent basis (over $\mathbb{C}$) of the commutant consisting of matrices with integral entries (even zeroes and ones only). The latter is obviously a basis over $\mathbb{Q}$ (rational numbers).*

This is the kind of basis we need, even if the following construction is not the most convenient for further applications. Consider an orbit $\mathcal{O}$ in $G_{2n} \times G_{2n}$. We know that any pair in $\mathcal{O}$ generates the same subgroup $G \subset G_{2n}$, isomorphic to some $\mathbb{Z}_p \times \mathbb{Z}_{pq}$. For any $(\mathbf{k}, \mathbf{k}') \subset \mathcal{O}$ and any pair $(\mathbf{l}, \mathbf{l}') \subset G \times G$ (not necessarily in $\mathcal{O}$) there exists a two by two matrix of integers M such that $(\mathbf{l}, \mathbf{l}') = (\mathbf{k}, \mathbf{k}')M$ with $\det M$ well defined mod p and changing the representative pair $(\mathbf{k}, \mathbf{k}')$ in $\mathcal{O}$ does not change $\det M \bmod p$. We therefore set

$$B_{\mathcal{O}}(\mathbf{l}, \mathbf{l}') = \det M \bmod p$$

bilinear in $\mathbf{l}$ and $\mathbf{l}'$ and antisymmetric in the interchange of its arguments reflecting similar properties of the determinant as a function of its columns. Moreover the pair $(\mathbf{l}, \mathbf{l}')$ generates an orbit in $G \times G \subset G_{2n} \times G_{2n}$ and $B_{\mathcal{O}}(\mathbf{l}, \mathbf{l}')$ is independent of the choice of $(\mathbf{l}, \mathbf{l}')$ in $\mathcal{O}'$ so we could write it $B_{\mathcal{O}}(\mathcal{O}')$. Let G be fixed, then we know that $\varphi(p)$ distinct orbits generate the same G, hence we get $\varphi(p)$ different $B_{\mathcal{O}}$. If $\mathcal{O}$ and $\tilde{\mathcal{O}}$ generate G and $\mathcal{O}'$ is an orbit in $G \times G$, we have $B_{\mathcal{O}}(\mathcal{O}') = B_{\mathcal{O}}(\tilde{\mathcal{O}}) B_{\tilde{\mathcal{O}}}(\mathcal{O}')$. Since $G \subset G_{2n}$ and since the abelian group G_{2n} is isomorphic to $\mathbb{Z}_{2nN} \times \mathbb{Z}_{2n}^{N-1}$ it follows that p, the order of an element in G, hence in G_{2n}, divides $2nN$ (to see this it suffices to write it in factorized form). As a result the following operator is well defined for any $t \bmod p$,

$$J_{\mathcal{O},t} = \frac{1}{|G|} \sum_{\mathbf{l},\mathbf{l}' \in G} \xi^{\frac{2nN}{p} t B_{\mathcal{O}}(\mathbf{l},\mathbf{l}')} \{\mathbf{l}, \mathbf{l}'\} \ ,$$

and $J_{\mathcal{O},t} = J_{\tilde{\mathcal{O}}, tB_{\mathcal{O}}(\tilde{\mathcal{O}})}$ when $\mathcal{O}$ and $\tilde{\mathcal{O}}$ both generate the same G. We now split the sum over orbits $\mathcal{O}'$ in $G \times G$ as

$$J_{\mathcal{O},t} = \frac{1}{|G|} \sum_{\mathcal{O}'} \xi^{\frac{2nN}{p} t B_{\mathcal{O}}(\mathcal{O}')} I_{\mathcal{O}'} \ ,$$

expressing J's as linear combination of the previous basic invariants, hence proving that they belong to the commutant.

Next we prove that the J's have integral matrix elements. Let $\mathbf{x}, \mathbf{x}'$ belong to G_n and $\mathbf{p}, \mathbf{p}'$ be the projections in G_n of $\mathbf{l}, \mathbf{l}' \in G$. Then

$$\langle \mathbf{x} | \{\mathbf{l}, \mathbf{l}'\} | \mathbf{x}' \rangle = \delta_{\mathbf{x}, \mathbf{p}+\mathbf{x}' \bmod G_n} \xi^{\mathbf{l} \cdot \mathbf{l}' + 2\mathbf{p}' \cdot \mathbf{x}'}$$

$\left(\text{recall that } \xi = e\left(\frac{1}{2nN}\right)\right)$.

For fixed $\mathbf{l}$ assume that there exists $\mathbf{k}'$ in G projecting on $\mathbf{q}'$ such that

$$\mathbf{l} \cdot \mathbf{l}' + 2\mathbf{q}' \cdot \mathbf{x}' + \frac{2nN}{p} t B_{\mathcal{O}}(\mathbf{l}, \mathbf{k}') \not\equiv 0 \bmod 2nN \ .$$

Then

$$\sum_{\mathbf{l}' \in G} \xi^{\frac{2nN}{p} tB_{\mathcal{O}}(\mathbf{l},\mathbf{l}') + 2\mathbf{p}'\cdot\mathbf{x}' + \mathbf{l}\cdot\mathbf{l}'} = 0 \ .$$

Indeed, we can replace $\sum_{\mathbf{l}' \in G}$ by $\sum_{\mathbf{l}' + m\mathbf{k}' \in G}$ for fixed m and $\mathbf{k}'$ since G is a group, the average over $m \bmod 2nN$ and it is this average which (easiy) yields zero. On the other hand if ($\mathbf{l}$ is still fixed) for every $\mathbf{l}'$ in G (projecting on $\mathbf{p}'$) we have $\mathbf{l}\cdot\mathbf{k}' + 2\mathbf{p}'\cdot\mathbf{x}' + \dfrac{2nN}{p} tB_{\mathcal{O}}(\mathbf{l},\mathbf{l}') \equiv 0 \bmod 2nN$, then the previous sum over $\mathbf{l}'$ yields instead of zero an integer, namely the order $|G|$ of the group G. We can now perform the summation over $\mathbf{l}$. Thus the matrix elements of $J_{\mathcal{O},t}$ are (non-negative) integers (this follows from our choice of averaging over G in their definition). We can say even a little more. The non-vanishing elements $\langle \mathbf{x}|J_{\mathcal{O},t}|\mathbf{x}'\rangle$ count the number of $\mathbf{l} \in G_{2n}$ with projection $\mathbf{p} = \mathbf{x} - \mathbf{x}'$ such that a linear form in $\mathbf{l}$ vanishes for all $\mathbf{l}' \in G$. When this number is non-zero it is independent of $\mathbf{x} - \mathbf{x}'$ since any such $\mathbf{l}$ is the sum of a particular solution and a solution of the same problem when $\mathbf{x} = \mathbf{x}' = 0$ (and the latter is obviously non-vanishing). We conclude that the matrices

$$\frac{J_{\mathcal{O},t}}{\langle \mathbf{0}|J_{\mathcal{O},t}|\mathbf{0}\rangle}$$

belong to the commutant and have entries 0 or 1. It now remains to prove that they generate the commutant.

To do this we appeal to the Jordan Hölder theorem [3] which states (in the case of a finite abelian group H) that the length m (the number of elements) in an increasing sequence of maximal proper subgroups $\{0\} \subsetneq H_1 \subsetneq H_2 \ldots \subsetneq H_m \equiv H$ is an intrinsic property of H independently of the possible arbitrariness on some subgroup H_i. Thus to an orbit $\mathcal{O}$ we can associate the length m of the corresponding subgroup G it generates. In particular for the trivial orbit $\mathcal{O}_0$ reduced to the pair $(\mathbf{0}, \mathbf{0})$ we have $m = 0$, then $J_{\mathcal{O}_0,0} = I_{\mathcal{O}_0} = I$ the unit operator. Assume now that $I_{\mathcal{O}}$'s of length smaller than m can be expressed as linear combinations of $J_{\mathcal{O},t}$'s. Let $\mathcal{O}_m$ be an orbit of length m with associated subgroup $G \cong \mathbb{Z}_p \times \mathbb{Z}_{pq}$ so that $G \times G$ contains $\varphi(p)$ orbits generating exactly G. In the definition of $J_{\mathcal{O}_m,t}$ we split the sum over $G \times G$ into orbits under $SL(2,\mathbb{Z})$ and call respectively $\mathcal{O}_1$ and $\mathcal{O}_2$ those associated to G or to proper subgroups of G with length necessarily smaller than m. Hence

$$J_{\mathcal{O}_m,t} = \frac{1}{|G|} \sum_{i=1,2} \sum_{\mathcal{O}_i} \xi^{\frac{2nN}{p} tB_{\mathcal{O}_m}(\mathcal{O}_i)} I_{\mathcal{O}_i} \ .$$

In the sum over orbits $\mathcal{O}_2$ the $I_{\mathcal{O}_2}$ are expressible as linear combinations of the J's by the recurrence hypothesis, we move these terms to the left-hand side. Then we perform a Fourier transform over $t \bmod p$. For $t \notin \mathbb{Z}_p^*$ we get relations among the J's (they could be identities). But for each $t \in \mathbb{Z}_p^*$ we get an expression for an element $I_{\mathcal{O}_1}$, where $\mathcal{O}_1$ runs over the orbits associated to G. In particular we get $I_{\mathcal{O}_m}$ as a linear combination of J's. Taking a maximal free subset among the J's we find the basis of the commutant as claimed in Theorem 3. Indeed that it is also a $\mathbb{Q}$ basis follows from a standard theorem on incomplete bases in vector spaces over a field.

One may wonder whether there is a short cut to deduce this theorem. It is clear that the whole discussion is based on the choice of a primitive nN-th (or possible $2nN$-th) root of unity. But the rational commutant is insensitive to such a choice. Thus getting rid of unwanted phases if S' and T' denote matrices similar to S and T with any other primitive root substituted for the original one the enveloping algebras generated over $\mathbb{Q}$ are identical as a result of the previous analysis.

We will now exhibit the structure of matrix elements of $J_{\mathcal{O},t}$ which we assume to be normalized by their $(\mathbf{0},\mathbf{0})$ entry. To a subgroup H of G_n we associate a dual $\hat{H}$ defined as follows:

$$\hat{H}=\{\hat{\mathbf{p}}\in G_n,\ \hat{\mathbf{p}}\cdot\mathbf{p}\equiv 0(n.N) \text{ for all } \mathbf{p}\text{'s in } H\}\ .$$

It is quickly checked that $S\left(\sum_{\mathbf{p}\in H}|\mathbf{p}\rangle\right)$ is proportional to $\sum_{\hat{\mathbf{p}}\in\hat{H}}|\hat{\mathbf{p}}\rangle$ proving that $\hat{\hat{H}}=H$. From

$$\langle\mathbf{x}|J_{\mathcal{O},t}|\mathbf{x}'\rangle=\begin{cases}1 & \text{if there is } \mathbf{l} \text{ in } G \text{ with projection } \mathbf{x}-\mathbf{x}' \text{ such that for all } \mathbf{k} \text{ in } G \\ & \text{(with projection denoted by } \mathbf{q})\\ & \mathbf{l}\cdot\mathbf{k}+2\mathbf{q}\cdot\mathbf{x}'+\dfrac{2nN}{p}tB_{\mathcal{O}}(\mathbf{l},\mathbf{k})\equiv 0 \bmod 2nN\\ 0 & \text{otherwise}\ ,\end{cases}$$

we easily see that $H=\{\mathbf{p}\in G_n, \exists\mathbf{x}\in G_n\langle\mathbf{x}|J_{\mathcal{O},t}|\mathbf{x}-\mathbf{p}\rangle=1\}$ is a subgroup of G_n, using that if $\mathbf{l}$ in G has projection $\mathbf{x}-\mathbf{x}'$ and $\mathbf{k}$ in G projection $\mathbf{q}$, then $\mathbf{l}\cdot\mathbf{k}+2\mathbf{q}\cdot\mathbf{x}'=-\mathbf{l}\cdot\mathbf{k}+2\mathbf{q}\cdot\mathbf{x}(2nN)$. Now let $\mathbf{p}\in H$ and $\mathbf{x}\in G_n$ such that $\langle\mathbf{x}|J_{\mathcal{O},t}|\mathbf{x}-\mathbf{p}\rangle=1$, $H'=\{\mathbf{y}\in G_n, \langle\mathbf{x}+\mathbf{y}|J_{\mathcal{O},t}|\mathbf{x}+\mathbf{y}-\mathbf{p}\rangle=1\}$ is also a subgroup of G_n, easily seen to be independent of $\mathbf{p}$ and $\mathbf{x}$, hence $H'=\{\mathbf{y}\in G_n\langle\mathbf{y}|J_{\mathcal{O},t}|\mathbf{y}\rangle=1\}$. This proves that if $\mathbf{p}\in H$, $\mathbf{x}$ is defined mod H'. But if $\langle\mathbf{x}|J_{\mathcal{O},t}|\mathbf{x}-\mathbf{p}\rangle=1$ and $\langle\mathbf{y}|J_{\mathcal{O},t}|\mathbf{y}-\mathbf{q}\rangle=1$ we can check that $\langle\mathbf{x}-\mathbf{y}|J_{\mathcal{O},t}|\mathbf{x}-\mathbf{y}-(\mathbf{p}-\mathbf{q})\rangle=1$. Hence we can define a homomorphism s from H to G_n/H' associating the class of $\mathbf{x}$ to $\mathbf{p}$. Then $\langle\mathbf{x}|J_{\mathcal{O},t}|\mathbf{x}'\rangle=\delta_{\mathbf{x}+H,\mathbf{x}'+H}\delta_{\mathbf{x}+H',s(\mathbf{x}-\mathbf{x}')}$. We can now compute $\mathrm{Tr}\,J_{\mathcal{O},t}G_{-\mathbf{p}'}P_{-\mathbf{p}}$, i.e. $\sum_{\mathbf{x}\in G_n}\langle\mathbf{x}|J_{\mathcal{O},t}|\mathbf{x}-\mathbf{p}\rangle\xi^{-2\mathbf{p}'\cdot(\mathbf{x}-\mathbf{p})}$. This is zero if $\mathbf{p}\notin H$. If $\mathbf{p}\in H$ we pick $\mathbf{x}_0$ such that $\mathbf{x}_0+H'=s(\mathbf{p})$ and get $\sum_{\mathbf{y}\in H'}\xi^{-2\mathbf{p}'(\mathbf{x}_0+\mathbf{y}-\mathbf{p})}$. This is $|H'|\xi^{-2\mathbf{p}'\cdot(\mathbf{x}_0-\mathbf{p})}$ if $\mathbf{p}'\in\hat{H}'$. Hence

$$\mathrm{Tr}\,J_{\mathcal{O},t}Q^{-\mathbf{p}'}P^{-\mathbf{p}}=|H'|\begin{cases}0 & \text{if } \mathbf{p}\notin H \text{ or } \mathbf{p}'\notin\hat{H}'\\ \xi^{-2\mathbf{p}'\cdot(\mathbf{x}_0-\mathbf{p})} & \text{otherwise}\ .\end{cases}$$

But we know that $J_{\mathcal{O},t}$ commutes with S and T and up to phases S and T act on $Q^{-\mathbf{p}'}P^{-\mathbf{p}}$ by an $SL(2,\mathbb{Z})$ transformation on $(\mathbf{p}',\mathbf{p})$. This implies that H and $\hat{H}'$ have to coincide. Consequently the scalar product between an element of H and any representative in a class of G_n/H' is well defined mod nN, and

$$\mathrm{Tr}\,(J_{\mathcal{O},t}Q^{-\mathbf{p}'}P^{-\mathbf{p}})=|\hat{H}|\delta_{\mathbf{p}\in H}\delta_{\mathbf{p}'\in H}\xi^{-2\mathbf{p}'\cdot(s(\mathbf{p})-\mathbf{p})}\ .$$

More generally let K be any subgroup of G_n and r a homomorphism from K to $G_n/\hat{K}$.

We can define Ω depending on K and r by

$$\mathrm{Tr}(\Omega Q^{-\mathbf{p}'}P^{-\mathbf{p}})=|\hat{K}|\delta_{\mathbf{p}\in K}\delta_{\mathbf{p}'\in K}\xi^{-2\mathbf{p}'\cdot(r(\mathbf{p})-\mathbf{p})}\ .$$

Demanding that Ω commutes with S and T requires

$$\mathbf{p}' \cdot r(\mathbf{p}) + \mathbf{p} \cdot r(\mathbf{p}') \equiv \mathbf{p} \cdot \mathbf{p}' \bmod nN \ ,$$

$$2\mathbf{p} \cdot r(\mathbf{p}) \equiv \mathbf{p}^2 \bmod 2nN \ .$$

Using the homomorphism property of r the second condition implies the first one. It is easy to check that the above homomorphism s defined for H satifies the required conditions, and that the matrix elements of Ω are

$$\langle \mathbf{x}|\Omega|\mathbf{x}'\rangle = \delta_{\mathbf{x}+K,\mathbf{x}'+K}\delta_{\mathbf{x}+\hat{K},r(\mathbf{x}-\mathbf{x}')} \ ,$$

hence are integers.

5. Specialization to $SU(3)$

Until now we have only used the additive group structure on $G_n = M^*/nM$. In special cases however it is also possible to take advantage of a natural multiplicative structure on G_n to define particular elements of the commutant with integral entries. These are necessarily linear combinations of the J's, but an explicit form of the coefficients is not defined until we make choice of a basis among the J's. We use $SU(3)$ as an illustration, but any semi simple rank two Lie group would allow for a similar treatment. (For instance, because we forget momentarily the antisymmetry constraints from the Weyl group the discussion of G_2 and $SU(3)$ invariants is essentially identical.)

We endow $\mathbb{C}$ with twice its usual scalar product $2\,\mathrm{Re}\, z\bar{z}'$, and set $\omega = e(\frac{1}{6})$. With our new normalization for scalar products the two fundamental weights of $SU(3)$ satisfy $\alpha^1 \cdot \alpha^1 = \alpha^2 \cdot \alpha^2 = 2$, $\alpha^1 \cdot \alpha^2 = 1$, and clearly 1 and ω satisfy these relations. Hence we take for M^* the quadratic ring $\mathbb{Z}(\omega)$. (It is well known that is it an unique factorization domain, and that primes $\neq 3$ in $\mathbb{Z}$ do or do not decompose in $\mathbb{Z}(\omega)$ according to their residue 1 or -1 mod 3.) The root lattice is a sublattice of M^* having scalar products with M^* equal to zero mod 3. This is equivalent to saying that M consists of multiples of $\varrho = 1+\omega$, hence is a prime ideal in M^*, and $G_n = M^*/nM$ has a natural ring structure. We can think of G_n as a $\mathbb{Z}(\omega)$ module, its ideals are principal, and are generated by divisors of $n\varrho$ (in the $\mathbb{Z}(\omega)$ sense), but of course there exist additive subgroups of G_n which are not ideals.

The basic constructions for a general Lie group admit here a compact expression in complex notation. For instance the Weyl group is generated by complex conjugation and multiplication by ω^2. The two Casimir invariants for $SU(3)$ are $C_2(\lambda) = \lambda\bar{\lambda}$, $C_3(\lambda) = \dfrac{\lambda^3 + \bar{\lambda}^3}{2}$, and the dimension of the representation of $SU(3)$ with highest weight $\lambda (\lambda = m_1 + m_2\omega,\ m_2 > 0,\ m_2 > 0)$ is $\dfrac{\lambda^3 - \bar{\lambda}^3}{\varrho^3 - \bar{\varrho}^3}$ (ϱ is the highest weight for the trivial representation). The fundamental domain B_n is the set $\{(m_1, m_2), m_1 > 0, m_2 > 0, m_1 + m_2 < n\}$. Recall that the level k is such that $n = k+3$.

Representations of $SU(3)$ have a triality $\lambda \to t(\lambda) \in M^*/M \equiv F_3$, such that if $\lambda = m_1 + \omega m_2$, $t(\lambda) \equiv m_1 - m_2 \bmod 3$. Furthermore as a set, B_n is invariant under a

group of rotations of order three generated by

$$\lambda \to \sigma(\lambda) = \omega^2 \lambda + n \bmod n\varrho$$

arising from the outer automorphism group of $A_2^{(1)}$.

To motivate the following discussion it is perhaps illuminating to rephrase the construction of $SU(2)$ invariants [2] using the formalism introduced at the end of the preceding section. In the $SU(2)$ case we also have a principal ring structure for M^*/nM isomorphic to $\mathbb{Z}_{2n}$ with usual product as scalar product, and here all subgroups are also ideals.

Let $\tilde{\delta}$ divide $2n$ ($2n = \tilde{\delta}\delta'$), set $K = \tilde{\delta}\mathbb{Z}_{2n}$ then $\hat{K} = \frac{2n}{\tilde{\delta}}\mathbb{Z}_{2n}$. The only homomorphisms from K to $\mathbb{Z}_{2n}/\hat{K}$ are of the form $r : \tilde{\delta}x \to r(x + \hat{K})$, where r is an integer. The homomorphism r has to verify $2ar(a) \equiv a^2 \bmod 4n$ for a in $\tilde{\delta}\mathbb{Z}_{2n}$. This is equivalent to $\tilde{\delta} = 2\delta$ and $r \equiv \delta \bmod \delta'$. This gives an element Ω_δ of the commutant, with $\langle x|\Omega_\delta|x'\rangle = \delta_{x-x' \equiv 0(2\delta)}\delta_{x+x' \equiv 0(2\delta')}$. We set $\alpha = [\delta, \delta']$ and choose $u, v \in \mathbb{Z}$ such that $\delta u + \delta' v = \alpha$. Then $\delta u - \delta' v$ is well defined mod $\frac{2n}{\alpha}$. But $x - x' \equiv 0(2\delta) x + x' \equiv 0(2\delta')$ implies that $x \equiv x' \equiv 0(\alpha)$, hence $\frac{\delta' v - \delta u}{\alpha} x$ is well defined mod $\frac{2n}{\alpha}$ and $x' - \frac{\delta' v - \delta u}{\alpha} x = \frac{\alpha x' - (\delta' v - \delta u)x}{\alpha} = \frac{u\delta(x+x') + v\delta'(x'-x)}{\alpha}$, and this is zero mod $\frac{2n}{\alpha}$. Conversely we have

$$x - \frac{\delta' v - \delta u}{\alpha} x = 2\delta u \frac{x}{\alpha} \equiv 0(2\delta)$$

and

$$x + \frac{\delta' v - \delta u}{\alpha} x \equiv 2\delta' v \frac{x}{\alpha} \equiv 0(2\delta') \ ,$$

hence if we set $b = \frac{\delta v - \delta u}{\alpha}$, we have $\left(\text{note that } b^2 \equiv 1 \left(\frac{2n}{\alpha^2}\right)\right)$

$$\langle x|\Omega_\delta|x'\rangle = \begin{cases} 1 & \text{if} \quad x \equiv x' \equiv 0 \bmod \alpha \quad \text{and} \quad x' \equiv bx \bmod \frac{2n}{\alpha} \\ 0 & \text{else} \ . \end{cases}$$

In this form it is easy to extend this discussion to the $SU(3)$ case. We had α such that α^2 divided n and b such that $b^2 \equiv 1 \left(\frac{2n}{\alpha^2}\right)$. We replace this by an element α up to a unit such that $\alpha\bar{\alpha}$ divides n and μ such that $\mu\bar{\mu} \equiv 1 \left(\frac{3n}{\alpha\bar{\alpha}}\right)$ and define $\Omega_\mu^{(\alpha)}$,

$$\langle \lambda|\Omega_\mu^{(\alpha)}|\lambda'\rangle = \begin{cases} 1 & \text{if} \quad \lambda' \equiv \lambda' \equiv 0 \bmod \alpha \quad \text{and} \quad \lambda' \equiv \mu\lambda \bmod \frac{\varrho n}{\bar{\alpha}} \\ 0 & \text{else} \ . \end{cases}$$

First we note that $\bar{\varrho}$ and ϱ differ by a unit and that if δ divides ϱn the dual of δG_n is $\frac{\varrho n}{\delta} G_n$. We now compute $\mathrm{Tr}\, \Omega_\mu^{(\alpha)} Q_{-\lambda'} P_{-\lambda}$, i.e.

$$\sum_\nu \langle \nu | \Omega_\mu^{(\alpha)} | \nu - \lambda \rangle e\left(\frac{-2\,\mathrm{Re}\,\lambda'(\overline{\nu-\lambda})}{3n}\right) .$$

This sum is non-zero if and only if we can write λ in the form (we define $\mathcal{N} \equiv n\varrho$) : $(1-\mu)\alpha z + \frac{\mathcal{N}}{\bar{\alpha}} u$, i.e. λ belongs to the ideal

$$\left[(1-\mu)\alpha, \frac{\mathcal{N}}{\bar{\alpha}}\right] = \alpha\left[1-\mu, \frac{\mathcal{N}}{\alpha\bar{\alpha}}\right] .$$

If λ is in this ideal which we denote by K, the possible z's differ by multiples of $\frac{\mathcal{N}}{\bar{\alpha}\left[(1-\mu)\alpha, \frac{\mathcal{N}}{\bar{\alpha}}\right]}$. Hence αz is defined modulo the ideal generated by $\frac{\mathcal{N}}{\bar{\alpha}\left[1-\mu, \frac{\mathcal{N}}{\alpha\bar{\alpha}}\right]}$ which is the dual of $\alpha\left[1-\mu, \frac{\mathcal{N}}{\alpha\bar{\alpha}}\right]$ since $1-\mu = -\mu(1-\bar{\mu}) \bmod \frac{\mathcal{N}}{\alpha\bar{\alpha}}$ and $\left[\mu, \frac{\mathcal{N}}{\alpha\bar{\alpha}}\right] = 1$. Hence we retrieve the general structure presented at the end of Sect. 4, and all that remains to shown is that if to $\lambda \in K$ we associate αz such that $\lambda - (1-\mu)\alpha z \equiv 0 \bmod \frac{\mathcal{N}}{\bar{\alpha}}$ then $2\,\mathrm{Re}\,\bar{\lambda}\alpha z \equiv \lambda\bar{\lambda} \bmod 3n$. To do so, we write $\lambda = (1-\mu)\alpha z + \frac{\mathcal{N}}{\bar{\alpha}} t$. The dual of αG_n is generated by $\frac{\mathcal{N}}{\bar{\alpha}}$, hence

$$\begin{aligned}\lambda\bar{\lambda} &= (1-\mu)(1-\bar{\mu}) z\bar{z}\alpha\bar{\alpha} + \frac{\mathcal{N}\bar{\mathcal{N}}}{\alpha\bar{\alpha}} t\bar{t} + 2\,\mathrm{Re}\,(1-\mu) z \mathcal{N} \bar{t} \\ &\equiv (2-\mu-\bar{\mu}) z\bar{z}\alpha\bar{\alpha} \bmod 3n\end{aligned}$$

using $\mu\bar{\mu} \equiv 1 \left(\frac{3n}{\alpha\bar{\alpha}}\right)$. On the other hand

$$\begin{aligned}2\,\mathrm{Re}\,\lambda\bar{\alpha}\bar{z} &\equiv 2\,\mathrm{Re}\,(1-\mu)\alpha z\bar{\alpha}\bar{z} \bmod 3n \\ &\equiv \alpha\bar{\alpha} z\bar{z}(2-\mu-\bar{\mu}) \bmod 3n .\end{aligned}$$

Hence the property is satisfied and $\Omega_\mu^{(\alpha)}$ belongs to the integral commutant.

In the $SU(3)$ case G_n is isomorphic as an additive group to $\mathbb{Z}_{3n} \times \mathbb{Z}_n$, and we have an explicit formula for the dimension of the commutant. For small values of n this dimension is listed in Table 1.

Table 1. Dimension of the commutant for small values of n in the $SU(3)$ case

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
$\dim_3$	2	10	12	32	22	60	30	88	54	110	46	192	54	150	132	224	70	270	78	352	180	230	94	528	170	270	216

For instance for $n=5$ this dimension is 22, but it is possible to verify that the number of distinct $\Omega_\mu^{(\alpha)}$ in this case is 12. In general we expect that the $\Omega_\mu^{(\alpha)}$ represent only a small fraction of the commutant.

However all known invariants up to now can be expressed using only the Ω's. The significance of this property is not clear to us.

Table 2. List of known $SU(3)$ invariants. Conjugate partners are omitted, $t(\lambda)$ is the triality and $\sigma(\tau)$ is the Z_3 action on representations labeled $\lambda = m_1 + \omega m_2$, i.e. $\chi_\lambda \equiv \chi_{m_1, m_2}$

Height n	Invariant $\sum \bar{\chi}_\lambda \mathcal{N}_{\lambda\lambda'} \chi_{\lambda'}$	$\mathcal{N}_{\lambda\lambda'}$
$n \geqq 3$	$A_n = \sum_\lambda \lvert\chi_\lambda\rvert^2$	$\Omega_1^{(1)}$
$n \geqq 6$	$D_n = \sum_{\lambda, \sigma \mid \lambda} \bar{\chi}_\lambda \chi_\lambda + \bar{\chi}_\lambda \chi_{\sigma(\lambda)} + \bar{\chi}_\lambda \chi_{\sigma^2(\lambda)}$	$\Omega_1^{(q)}$
$n \equiv 0 \bmod 3$		
$n > 6$	$D_n = \sum_\lambda \bar{\chi}_\lambda \chi_{\sigma^{nt(\lambda)}(\lambda)}$	$\Omega_{n+1}^{(1)} \quad n \equiv 1 \bmod 3$
$n \not\equiv 0 \bmod 3$		$\Omega_{n+\omega}^{(1)} \quad n \equiv -1 \bmod 3$
8	$E_8 = \lvert\chi_{1,1} + \chi_{3,3}\rvert^2 + \lvert\chi_{3,1} + \chi_{3,4}\rvert^2 + \lvert\chi_{1,3} + \chi_{4,3}\rvert^2 + \lvert\chi_{4,1} + \chi_{1,4}\rvert^2 + \lvert\chi_{2,3} + \chi_{6,1}\rvert^2 + \lvert\chi_{3,2} + \chi_{1,6}\rvert^2$	$\Omega_1^{(1)} + \Omega_{5\omega}^{(1)}$
12	$E_{12} = \lvert\chi_{1,1} + \chi_{10,1} + \chi_{1,10} + \chi_{5,2} + \chi_{2,5} + \chi_{5,5}\rvert^2 + 2\lvert\chi_{3,3} + \chi_{3,6} + \chi_{6,3}\rvert^2$	$\Omega_1^{(q)} + \Omega_5^{(q)}$
	$F_{12} = \lvert\chi_{1,1} + \chi_{1,10} + \chi_{10,1}\rvert^2 + \lvert\chi_{3,3} + \chi_{3,6} + \chi_{6,3}\rvert^2 + \lvert\chi_{5,2} + \chi_{2,5} + \chi_{5,5}\rvert^2 + \lvert\chi_{4,1} + \chi_{7,4} + \chi_{1,7}\rvert^2 + \lvert\chi_{1,4} + \chi_{4,7} + \chi_{7,1}\rvert^2 + 2\lvert\chi_{4,4}\rvert^2 + \bar{\chi}_{4,4}(\chi_{2,2} + \chi_{8,2} + \chi_{2,8}) + (\bar{\chi}_{2,2} + \bar{\chi}_{8,2} + \bar{\chi}_{2,8})\chi_{4,4}$	$\Omega_1^{(q)} - \frac{1}{3}\Omega_1^{(2q)}$
24	$E_{24} = \lvert\chi_{1,1} + \chi_{22,1} + \chi_{1,22} + \chi_{5,5} + \chi_{14,5} + \chi_{5,14} + \chi_{11,11} + \chi_{11,5} + \chi_{5,11} + \chi_{11,8} + \chi_{8,11}\rvert^2 + \lvert\chi_{7,1} + \chi_{1,7} + \chi_{16,1} + \chi_{1,16} + \chi_{16,7} + \chi_{7,16} + \chi_{8,5} + \chi_{5,8} + \chi_{11,2} + \chi_{2,11} + \chi_{7,7} + \chi_{10,7} + \chi_{7,10}\rvert^2$	$\Omega_1^{(q)} + \Omega_5^{(q)} + \Omega_7^{(q)} + \Omega_{11}^{(q)}$

We list the expressions of the known invariants for $SU(3)$ [4, 5] in Table 2 omitting possible "charge conjugate" partners. (Given a positive normalized invariant $Z = \sum_{\lambda, \lambda'} \overline{\chi_\lambda(\tau)} \mathcal{N}_{\lambda\lambda'} \chi_{\lambda'}(\tau)$, we can always associate a "conjugate" one Z' obtained from the preceding by changing $\mathcal{N}_{\lambda\lambda'} \to \mathcal{N}'_{\lambda, \lambda'} = \mathcal{N}_{\lambda, \omega\bar{\lambda}'}$, which may or may not coincide with Z.)

References

1. Kac, V.G.: Infinite dimensional Lie algebras, 2nd edn., Cambridge: Cambridge University Press 1985
2. Cappelli, A., Itzykson, C., Zuber, J.-B.: The A-D-E classification of minimal and $A_1^{(1)}$ conformal invariant theories. Commun. Math. Phys. **113**, 1, 26 (1987)
3. Curtis, C.W., Rainer, I.: Representation theory of finite groups and associative algebras, Chap. 1. New York: Wiley 1988
4. Christe, P., Ravanini, F.: $G_N \otimes G_L / G_{L+N}$ conformal field theories and their modular invariant partition functions. Int. J. Mod. Phys. A**4**, 897–920 (1989)
5. Moore, G., Seiberg, N.: Naturality in conformal field theory. Nucl. Phys. B**313**, 16–40 (1989)

Communicated by K. Gawedzki

Received Juli 31, 1989