Commun. Math. Phys. 160, 475–492 (1994)

Communications in
Mathematical
Physics

Automorphisms of the Affine $SU(3)$ Fusion Rules

Philippe Ruelle
Dublin Institute for Advanced Studies, 10 Burlington Road, Dublin 4, Ireland

Received: 25 February 1993

Abstract: We classify the automorphisms of the (chiral) level-k affine $SU(3)$ fusion rules, for any value of k, by looking for all permutations that commute with the modular matrices S and T. This can be done by using the arithmetic of the cyclotomic extensions where the problem is naturally posed. When k is divisible by 3, the automorphism group ($\sim Z_2$) is generated by the charge conjugation C. If k is not divisible by 3, the automorphism group ($\sim Z_2 \times Z_2$) is generated by C and the Altschüler–Lacki–Zaugg automorphism. Although the combinatorial analysis can become more involved, the techniques used here for $SU(3)$ can be applied to other algebras.

1. Introduction

Modular invariance has received much attention over the past six years, as it proved to play a key role in the classification of 2d conformal field theories [1]. For a left-right symmetric theory, the basic problem is to classify the modular invariant partition functions of the form

$$Z(\tau^*, \tau) = \sum_{i,j} \chi_i^*(\tau) N_{ij} \chi_j(\tau) , \tag{1.1}$$

where the $\chi_i(\tau)$, possibly in infinite number, are the irreducible characters of the chiral symmetry algebra occurring in that theory. The matrix N in (1.1) must have non-negative integer entries and must be normalized by requiring $N_{00} = 1$, where χ_0 denotes the character of the representation which contains the (chiral) vacuum. The characters carry a representation of the modular group:

$$\chi_i(\tau + 1) = \sum_j T_{ij} \chi_j(\tau), \quad \text{and } \chi_i\left(\frac{-1}{\tau}\right) = \sum_j S_{ij} \chi_j(\tau) . \tag{1.2}$$

That $Z(\tau^*, \tau)$ is modular invariant forces N to satisfy

$$T^\dagger N T = N \quad \text{and} \quad S^\dagger N S = N . \tag{1.3}$$

When the modular matrices S and T are unitary, the conditions (1.3) are equivalent to N being in their commutant: $[T, N] = [S, N] = 0$.

The above conditions on the matrix N prove to be extremely restrictive. A general analysis was carried out by Moore and Seiberg [2]. Their result is that, for a given theory, the matrices N which satisfy all the conditions must be permutation matrices, or else they are such once the symmetry has been adequately extended. Moreover, as follows from the Verlinde's formula [3], these permutations are automorphisms of the fusion coefficients of the original or the extended theory respectively.

For only a small class of theories has the classification been completed. Examples (almost all related to each other) include theories with an affine $SU(2)$ symmetry [4], the (unitary and non-unitary) Virasoro minimal models [4], supersymmetric minimal models [5] and parafermionic theories [6]. As to non-rational theories, only for those with $c = 1$ has a classification been (almost) established [7].

Among the rational theories, those with an affine Lie symmetry play a central role as they are thought to be the building blocks to construct all the others. At present, the complete classification is known only for theories with an $\widehat{SU(2)}$ symmetry [4], although partial results exist for $\widehat{SU(3)}$ [8, 9].

The purpose here is to study the modular invariant partition functions of theories possessing a symmetry not larger than an (untwisted) affine Lie symmetry. In other words, we will be looking for permutations N commuting with the matrices S and T describing the modular transformations of the characters of Kac–Moody algebras. Here we restrict ourselves to the $\widehat{SU(3)}$ algebra, which is the simplest case still open and yet, which offers generic features of other simple algebras.

The integrable representations of the $\widehat{SU(3)}_k$ Kac–Moody algebra are in correspondence with the $SU(3)$ strictly dominant weights p in the alcôve $B_n = \{p = (a, b)\colon a, b \geqq 1 \text{ and } a + b \leqq n - 1\}$, where we set the height $n = k + 3$ [10]. Their total number is $\frac{(n-1)(n-2)}{2}$. The representation labelled by $p = (1, 1)$ contains the vacuum of the Fock space where the algebra is being represented. We denote by $\chi_p(\tau)$ the corresponding (restricted) characters. As functions of τ, we have $\chi_p(\tau) = \chi_{p'}(\tau)$ if and only if $p' = Cp$, where C is the charge conjugation acting by $C(a, b) = (b, a)$.

The modular matrices, unitary in this case, have the following expressions. For $p = (a, b)$ and $p' = (c, d)$, the T matrix reads

$$T_{p,p'} = \exp\left[2i\pi\left(\frac{p^2}{2n} - \frac{1}{3}\right)\right]\delta_{p,p'} = \zeta_{3n}^{a^2+ab+b^2-n}\delta_{a,c}\delta_{b,d}\,, \tag{1.4a}$$

while the S matrix is more complicated

$$\begin{aligned} S_{p,p'} &= \frac{-i}{\sqrt{3n}}\sum_{w\in W}(\det w)\exp\left[2i\pi\frac{p\cdot w(p')}{n}\right], \\ &= \frac{-i}{\sqrt{3n}}\Big\{\zeta_{3n}^{(2a+b)c+(a+2b)d} + \zeta_{3n}^{-(a+2b)c+(a-b)d} + \zeta_{3n}^{-(a-b)c-(2a+b)d} \\ &\quad - \zeta_{3n}^{(2a+b)c+(a-b)d} - \zeta_{3n}^{-(a-b)c+(a+2b)d} - \zeta_{3n}^{-(a+2b)c-(2a+b)d}\Big\}\,. \end{aligned} \tag{1.4b}$$

Here $\zeta_{3n} = \exp\left(\frac{2i\pi}{3n}\right)$ and $W = S_3$ is the Weyl group of $SU(3)$.

In the following, we classify, for all heights n, the permutation matrices $N_{p,p'} = \delta_{p',\sigma(p)}$ which commute with the matrices S and T of (1.4), thereby classifying the partition functions of the form

$$Z(\tau, \tau^*) = \sum_{p \in B_n} [\chi_p(\tau)]^* [\chi_{\sigma(p)}(\tau)] . \tag{1.5}$$

Since the permutations σ are also automorphisms of the fusion rules, we could try to determine them directly from the fusion coefficients. This is indeed possible for $SU(3)$, by using their explicit expressions, obtained recently in [11]. It would however definitely confine us to $SU(3)$ since the fusion coefficients for higher rank algebras are not known. Instead, the approach we follow here, although applied to $SU(3)$, does not confine us to this particular case. We emphasize that we will not use any peculiar feature of $SU(3)$ that is not immediately available in other algebras. Our analysis can therefore be carried out in other cases as well. Another advantage of looking at the S matrix elements is that our proof can be useful to classify the automorphisms of the extensions defined by the complementary invariants of [12]. Indeed for those extensions, most of the extended S matrix is the same as the non-extended one, up to numerical factors.

Finally we should mention that modular invariants of the kind we are interested in here are already known. Whenever the KM algebra has outer automorphisms, Altschüler, Lacki and Zaugg have shown that one can construct a whole class of invariants (also called complementary) [13]. Whether these permutation invariants are exhaustive is generally an open problem, though the invariants found in [14] for G_2 and F_4 show that they are not exhaustive in those cases at least. For $\widehat{SU(3)}$, we will show that they are complete.

2. The Classification

The best part of this article will be devoted to the proof of the following necessary condition for σ to commute with S.

Theorem. *Let $p = (a, b)$ and $p' = \sigma(p) = (c, d)$ two weights in the alcôve B_n related by an automorphism σ. Then, modulo n, $(c, d, -c-d)$ is a permutation of $(a, b, -a-b)$.*

The theorem can be proved by only requiring that σ commutes with S, although for simplicity, we will make use of a stronger condition. Its proof is contained in Sects. 4 and 5. For the moment we show that the classification follows from it.

Since the weight $p' = \sigma(a, b)$ must belong to the alcôve, the six values quoted in the theorem are

$$\sigma(a, b) = \begin{cases} (a, b),\ (n-a-b, a),\ (b, n-a-b)\,, \\ (b, a),\ (a, n-a-b),\ (n-a-b, b)\,. \end{cases} \tag{2.1}$$

The last three values are the charge conjugated of the first three. We first ignore the action of the charge conjugation C, therefore focusing on the coset of the automorphism group by C.

The first three weights in (2.1) are the images of (a, b) under the outer automorphisms of $\widehat{SU(3)}$, generated by $\mu(a, b) = (n - a - b, a)$, $\mu^3 = 1$. One readily checks that for any pair of weights p, p' in the alcôve,

$$S_{\mu^k(p), p'} = e^{-\frac{2i\pi k t(p')}{3}} S_{p,p'} , \tag{2.2}$$

where $t(p') = c - d \bmod 3$ is the triality of the weight $p' = (c, d)$.

So the theorem says that the pointwise action of an automorphism of the fusion rules must be an outer automorphism of the KM algebra, up to the charge conjugation. The problem is to define σ on the whole of B_n in such a way that it still commutes with S. On the other hand, σ must also commute with T, which implies, from (1.4a), that the norms of p and $\sigma(p)$ must be equal modulo $2n$. From

$$(\mu^k(p))^2 = p^2 + \frac{2n}{3}[n - kt(p)] \bmod 2n \quad \text{for } k \neq 0 , \tag{2.3}$$

we obtain the following possibilities, depending on the residue of n modulo 3 and the triality of p:

$$\begin{aligned} n = 0 \bmod 3\colon\ & \sigma(p) = \mu^k(p) \quad \text{if } t(p) = 0 , \\ & \sigma(p) = p, \quad \text{if } t(p) \neq 0 , \\ n \neq 0 \bmod 3\colon\ & \sigma(p) = p \quad \text{or} \quad \mu^{nt(p)}(p) . \end{aligned} \tag{2.4}$$

We now impose the commutation of σ with S, which reads

$$S_{\sigma(p), p'} = S_{p, \sigma^{-1}(p')} \quad \text{for all } p, p' \in B_n . \tag{2.5}$$

If $n = 0 \bmod 3$, for any fixed root p of zero triality, we choose a weight p' of non-zero triality such that $S_{p,p'} \neq 0$. (This is always possible unless $p = (\frac{n}{3}, \frac{n}{3})$, but then $\mu(p) = p$ anyway.) We obtain from (2.2) and (2.4),

$$S_{\sigma(p), p'} = S_{\mu^k(p), p'} = e^{-\frac{2i\pi k t(p')}{3}} S_{p,p'} = S_{p, \sigma^{-1}(p')} = S_{p,p'} . \tag{2.6}$$

Equation (2.6) implies $k = 0$, so that none of the weights in B_n, whatever its triality, can undergo a non-trivial transformation σ (up to C).

For $n \neq 0 \bmod 3$, we take $p = (n-2, 1)$ and an arbitrary weight p', both of non-zero triality, and prove that if p undergoes a non-trivial transformation, then p' has to do the same. Suppose the contrary, namely $\sigma(p) = \mu^{nt(p)}(p)$ and $\sigma(p') = p'$. We have from (2.2)

$$S_{\sigma(p), p'} = S_{\mu^{nt(p)}(p), p'} = e^{-\frac{2i\pi n t(p) t(p')}{3}} S_{p,p'} = S_{p, \sigma^{-1}(p')} = S_{p,p'} . \tag{2.7}$$

The matrix element $S_{p,p'} = S_{(n-2,1), p'}$ is never zero for any p', so that (2.7) is a contradiction since $nt(p)t(p')$ is not zero modulo 3. Thus the transformation $\mu^{nt(\cdot)}(\cdot)$ acts on all the weights of B_n or on none of them.

We have proved that, up to the charge conjugation C, there is no non-trivial automorphism if $n = 0 \bmod 3$, and there is a single one if $n \neq 0 \bmod 3$, acting by $\sigma(p) = \mu^{nt(p)}(p)$. This automorphism is a permutation of order 2.

Finally we show that the charge conjugation must act in the same way on all the weights in B_n if it is to commute with S. From

$$S_{C(p),p'} = S^*_{p,p'}\,, \tag{2.8}$$

we obtain that, if p is transformed by C while p' is kept fixed, $S_{p,p'}$ must be real. However Eq. (2.2) implies

$$S_{\mu(1,1),p'} = S_{(n-2,1),p'} = e^{-\frac{2i\pi t(p')}{3}} S_{(1,1),p'}\,. \tag{2.9}$$

Since the matrix element $S_{(1,1),p'}$ is real and strictly positive for any p', it follows that $S_{(n-2,1),p'}$ has a non-zero imaginary part for every p' with a non-zero triality. Thus if a weight p' is conjugated, then $(n-2,1)$ must also be conjugated, and in turn that means that every weight has to be conjugated. Therefore, C acts on all the weights of non-zero triality or on none of them. To settle the question for the roots, we go back to the definition of σ as an automorphism of the fusion rules.

It is straightforward to compute the fusion rule of the fundamental representation of $SU(3)$ with any other representation. The result is (in terms of the shifted weights)

$$(2,1)*(a,b) = (a+1,b) + (a-1,b+1) + (a,b-1)\,, \tag{2.10}$$

where however, on the right-hand side, a representation must be omitted if one of its Dynkin label is zero or if the sum of its Dynkin labels is equal to n. If we take a root for (a,b), all the other representations entering (2.10) have a non-zero triality. This shows that if none of the weights undergoes the C transformation, none of the roots can either and conversely, if the fusion rules (2.10) are to be kept invariant. Therefore the charge conjugation C is an automorphism of the fusion rules if and only if it transforms uniformly all the weights and roots of the alcôve.

The proof is complete. We note that for $n=4$ and 5, the actions of $\mu^{nt(\cdot)}(\cdot)$ and C are identical. We have the

Proposition. *The automorphism group of the fusion rules of $\widehat{SU}(3)_k$ is generated by C if $n=k+3$ is divisible by 3 or if $n=4$ or 5, and is generated by C and $\mu^{nt(\cdot)}(\cdot)$ when $n \geqq 7$ is not divisible by 3. The group structure is Z_2 and $Z_2 \times Z_2$ respectively.*

As a direct consequence, there exist respectively two or four modular invariant partition functions originating from automorphisms of the fusion rules. They are the only ones if the $\widehat{SU}(3)$ symmetry is not extended.

3. Preliminaries

The proof of the theorem of Sect. 2 extensively uses the arithmetic of cyclotomic fields. A useful reference on this matter is the book by Washington [15].

Let ζ_n be a primitive n^{th} root of unity, for an arbitrary integer n, and let $Q(\zeta_n)$ denote the corresponding cyclotomic extension, of degree $\varphi(n)$ over the rationals. Its Galois group, noted $\mathrm{Gal}(Q(\zeta_n)/Q)$, is isomorphic to Z_n^* (the group of integers invertible modulo n) and transforms ζ_n into ζ_n^α for α coprime with n.

If p^l divides n, $Q(\zeta_n)$ is an algebraic extension of $Q(\zeta_{n/p^l})$, of relative degree p^l or $p^{l-1}(p-1)$ according to whether p does or does not divide $\frac{n}{p^l}$. In each case, the extension can be defined by the irreducible polynomial $X^{p^l} - \zeta_{n/p^l} = 0$ and $\Phi_{p^l}(X) = 0$ respectively, where $\Phi_m(X)$ denotes the m^{th} cyclotomic polynomial. If $k = \text{ord}_p n$ (i.e. p^k is the largest power of p dividing n), the Galois group of the relative extension is:

$$\text{Gal}(Q(\zeta_n)/Q(\zeta_{n/p^l})) = \left\{ \sigma_\alpha(\zeta_n) = \zeta_n^\alpha \colon \alpha = 1 \bmod \frac{n}{p^l} \text{ and } (\alpha, n) = 1 \right\}$$

$$\sim Z_{p^l}(l < k) \quad \text{or} \quad Z^*_{p^l}(l = k) \,. \tag{3.1}$$

For any z in $Q(\zeta_n)$, one defines its norm (over Q) by taking the product of all its Galois conjugates: $N_{Q(\zeta_n)/Q}(z) = \prod_{\sigma \in \text{Gal}(Q(\zeta_n)/Q)} \sigma(z)$. For d a divisor of n and x an integer coprime with $\frac{n}{d}$, one obtains

$$N_{Q(\zeta_n)/Q}(1 - \zeta_n^{dx}) = \begin{cases} 1 & \text{if two different primes divide } \dfrac{n}{d}\,, \\ p^{\frac{\varphi(n)}{\varphi(n/d)}} & \text{if } p \text{ is the only prime dividing } \dfrac{n}{d}\,. \end{cases} \tag{3.2}$$

We also note the useful polynomial identity

$$\prod_{j=1}^{m} (1 - X\zeta_m^j) = 1 - X^m \,. \tag{3.3}$$

In the maximal real sub-field $Q(\zeta_n + \zeta_n^{-1})$, the following subset of cyclotomic units will have some importance. Let $n = p^k$ be a prime power. These units are defined by

$$\xi_a = \zeta_n^{(1-a)/2} \frac{1 - \zeta_n^a}{1 - \zeta_n}\,, \quad 1 < a < \frac{n}{2}\,, (a, n) = 1 \,. \tag{3.4}$$

All the ξ_a are real and their number is equal to $r = \frac{1}{2}\varphi(n) - 1$, although the ξ_a can be defined for any $a \in Z_n^*$ and satisfy $\xi_a + \xi_{-a} = 0$. In particular, $\xi_1 = 1$ and $\xi_{-1} = -1$. The most useful property of the units ξ_a is that they are multiplicatively independent in $Q(\zeta_n + \zeta_n^{-1})$. It means that the existence of the relation

$$\xi_{a_1}^{t_1} \xi_{a_2}^{t_2} \ldots \xi_{a_r}^{t_r} = (-1)^{t_0}, \quad t_i \in Z \,, \tag{3.5}$$

requires $t_1 = t_2 = \ldots = t_r = 0$ and t_0 be even.

We will also need (additive) independence properties among the roots of unity. Let again $n = p^k$. A complete set of relations is given by

$$\zeta_n^r(1 + \zeta_n^{p^{k-1}} + \zeta_n^{2p^{k-1}} + \cdots + \zeta_n^{(p-1)p^{k-1}}) = 0, \quad 0 \leqq r \leqq p^{k-1} - 1 \,. \tag{3.6r}$$

Note that each of the n powers of ζ_n appears in one and only one relation. This implies that if a set of powers $\zeta_n^{a_i}$ is not linearly independent, Eq. (3.6r) for some r must hold among p of them. In particular, any set of $N < p$ different powers is linearly independent.

The related independence problem for n not a prime power can be reduced to the above case by using the fact that $Q(\zeta_{mn})$ is the product of $Q(\zeta_m)$ and $Q(\zeta_n)$ if m and n are coprime: one can choose a basis of $Q(\zeta_{mn})$ which is the product of bases of $Q(\zeta_m)$ and $Q(\zeta_n)$. This property implies that if a set of powers $\zeta_n^{a_i} \in Q(\zeta_n)$ are linearly independent over Q, they are also linearly independent over $Q(\zeta_m)$ provided $(n, m) = 1$.

Our starting point to prove the theorem of Sect. 2 is the expression (1.4b) for the matrix elements of S. When one of the indices is a "diagonal" root (l, l), the expression simplifies to become (from now on, we omit the prefactor $\frac{-i}{\sqrt{3}n}$)

$$S_{(l,l),(a,b)} = \zeta_n^{la+lb} + \zeta_n^{-la} + \zeta_n^{-lb} - \text{c.c.}\,. \tag{3.7}$$

This is an additive form of $S_{(l,l),(a,b)}$. In view of the independence property of the units (3.4), the following multiplicative form is equally useful. It is obtained by using the expression for the denominator of the Weyl character formula

$$S_{(l,l),(a,b)} = (1 - \zeta_n^{la})(1 - \zeta_n^{lb})(1 - \zeta_n^{-la-lb})\,. \tag{3.8}$$

Let us recall the generalization of (3.8) to any simple algebra $\hat{G}_k$. We set $n = k + h$ with h the dual Coxeter number of G. When $p = l\rho$ is a weight proportional to ρ, half the sum of the positive roots, the Weyl formula recasts the matrix element $S_{p,p'}$ into (up to an irrelevant prefactor)

$$S_{p,p'} = S_{(l,l,\ldots,l),p'} = \prod_{\text{positive roots } \alpha} \zeta_n^{l\alpha\cdot p'/2}(1 - \zeta_n^{-l\alpha\cdot p'})\,. \tag{3.9}$$

On account of the definition (3.4), $S_{l\rho,p'}$ can be expressed as a product of units ξ_a, up to an overall power of $(1 - \zeta_n)$ and ζ_n. This formula is the main tool of Sect. 4. (Note that if G is not simply-laced, the numbers $\alpha \cdot p'$ may not be integers.)

We also recall the arithmetical symmetry that the commutant of S and T was recently shown to possess [9]. Let N be a matrix commuting with S and T. (N can have complex entries). One defines on the pairs of $B_n \times B_n$ the following action of the group Z_{3n}^*. For any $\nu \in Z_{3n}^*$, it is defined by M_ν: $(p, p') \to (p_\nu, p'_\nu)$, where $p_\nu \in B_n$ is the image by an affine Weyl transformation w_ν of the weight νp. The symmetry was the statement that under this action, the coefficients $N_{p,p'}$ of N satisfy

$$N_{p,p'} = (\det w_\nu)(\det w'_\nu)\, N_{p_\nu,p'_\nu}\,. \tag{3.10}$$

In particular it was noted that $M_{-1}(p) = Cp$ is the charge conjugation, implying $N_{p,p'} = N_{Cp,Cp'}$ for any p, p'. As a consequence, if N is to be a permutation matrix, a diagonal root can only be permuted with another diagonal root: $p = Cp$ and $N_{p,p'} \neq 0$ imply $p' = Cp'$. In the following, we use this mild property in the only purpose to simplify the proofs. The theorem of Sect. 2 can be proved without using it. (In general, one finds $M_{-1}(p) = Cp$ for $G = SU(N)$, $SO(4N + 2)$ and E_6, while $M_{-1}(p) = p$ is the identity in all other cases, -1 being a Weyl transformation.)

The following two sections contain the proof itself of the theorem. We will exclusively use the matrix elements $S_{(l,l),p}$ in the form (3.7) and (3.8). Section 4 is essentially multiplicative while Sect. 5 is definitely additive.

4. A Local Version of the Theorem

Throughout this section and the next one, we let $n = \prod_1^s p_i^{k_i}$ be the prime decomposition of n, so that $k_i = \mathrm{ord}_{p_i} n$.

In this section, we prove that the theorem of Sect. 2 is (almost) true if we replace the congruence modulo n by a congruence modulo $p_i^{k_i}$, for any i (Corollary 1). We set $(c, d) = \sigma(a, b)$. They must satisfy $a, b, a+b, c, d, c+d \not\equiv 0 \bmod n$ to be in the alcôve B_n. The core of the analysis is contained in the following lemma, concerned with the solutions of the following two equations:

$$(1-\zeta_n^a)(1-\zeta_n^b)(1-\zeta_n^{-a-b}) = (1-\zeta_n^c)(1-\zeta_n^d)(1-\zeta_n^{-c-d}), \tag{4.1}$$

$$(1-\zeta_{p^k}^a)(1-\zeta_{p^k}^b)(1-\zeta_{p^k}^{-a-b}) = (1-\zeta_{p^k}^c)(1-\zeta_{p^k}^d)(1-\zeta_{p^k}^{-c-d}). \tag{4.2}$$

Equation (4.1) expresses the fact that $[S, \sigma]_{(1,1),(a,b)} = 0$, as follows from (2.5) and (3.8), and the invariance of (1, 1) under any automorphism. Likewise, (4.2) is $[S, \sigma]_{(\frac{n}{p^k}, \frac{n}{p^k}),(a,b)} = 0$ if $(\frac{n}{p^k}, \frac{n}{p^k})$ is known to be invariant under σ.

Let us define $l_x = \mathrm{ord}_p x$ for $x = a, b, a+b, c, d, c+d$. We note that within each triplet (l_a, l_b, l_{a+b}) or (l_c, l_d, l_{c+d}), two numbers must be equal and furthermore, these two are smaller or equal to the third one, on account of

$$l_{a+b} \geqq \min(l_a, l_b), \quad l_{c+d} \geqq \min(l_c, l_d), \tag{4.3}$$

where the equalities hold if $l_a \neq l_b$ or $l_c \neq l_d$.

Lemma 1. *Let a, b, c, d be integers such that $a, b, a+b, c, d, c+d \not\equiv 0 \bmod n$ satisfy Eqs.* (4.1) *and* (4.2), *where $k = \mathrm{ord}_p n$. Then either $(c, d, -c-d)$ is a permutation of $(a, b, -a-b) \bmod p^k$, or else we must have (up to permutations of $a, b, a+b$ or of $c, d, c+d$):*

$$p = 2, 3: \quad l_a = l_b = l_{a+b} = l_d = k \quad \text{and} \quad l_c = l_{c+d} = k-1, \tag{4.4a}$$

$$p = 2: \quad l_a = l_b = l_{a+b} = l_d = k \quad \text{and} \quad l_c = l_{c+d} = k-2, \tag{4.4b}$$

$$p = 2, 3: \quad l_c = l_d = l_{c+d} = l_b = k \quad \text{and} \quad l_a = l_{a+b} = k-1, \tag{4.4c}$$

$$p = 2: \quad l_c = l_d = l_{c+d} = l_b = k \quad \text{and} \quad l_a = l_{a+b} = k-2, \tag{4.4d}$$

$$p = 2: \quad l_a = l_{a+b} = k-1,\ l_b = k, \quad \text{and} \quad l_c = l_{c+d} = k-2,\ l_d = k, \tag{4.4e}$$

$$p = 2: \quad l_c = l_{c+d} = k-1,\ l_d = k, \quad \text{and} \quad l_a = l_{a+b} = k-2,\ l_b = k. \tag{4.4f}$$

Proof. Due to the symmetry of the problem, we need to consider only four cases: $l_a = l_b = l_{a+b} < k$ (case 1), $l_a = l_{a+b} < l_b < k$ (case 2), $l_a = l_b = l_{a+b} = k$ (case 3) and finally $l_a = l_{a+b} < l_b = k$ (case 4).

Case 1. $l_a = l_b = l_{a+b} < k$. Let $l = l_a$. Without loss of generality, we can assume $l_c = l_{c+d} \leqq l_d < k$. (None of l_c, l_d, l_{c+d} can be equal to k since the left-hand side of (4.2) is not zero.) Taking the norm $N_{Q(\zeta_{p^k})/Q}$ of (4.2), we obtain from (3.2),

$$3p^l = 2p^{l_c} + p^{l_d}. \tag{4.5}$$

If l_c and l_d are not both equal to l, one is smaller and the other is bigger than l, that is $l_c < l < l_d$. Then (4.5) yields $2p^{l_c} = 0 \bmod p^l$, a contradiction unless $p = 2$. However $p = 2$ is already excluded from the very start, because it is not compatible with $l_a = l_b = l_{a+b}$.

Hence $l_c = l_d = l_{c+d} = l$. For $a = \alpha p^l$, $b = \beta p^l$, $c = \gamma p^l$, $d = \delta p^l$ with $\alpha, \beta, \gamma, \delta, \alpha + \beta, \gamma + \delta$ coprime with p, (4.2) reads

$$(1 - \zeta^{\alpha})(1 - \zeta^{\beta})(1 - \zeta^{-\alpha-\beta}) = (1 - \zeta^{\gamma})(1 - \zeta^{\delta})(1 - \zeta^{-\gamma-\delta}),$$
$$\zeta = \zeta_{p^{k-l}}. \tag{4.6}$$

Dividing (4.6) by $(1 - \zeta)^3$, we get $\xi_\alpha \xi_\beta \xi_{-\alpha-\beta} \xi_\gamma^{-1} \xi_\delta^{-1} \xi_{-\gamma-\delta}^{-1} = 1$ from (3.4). The independence property of the ξ's implies that $(\alpha, \beta, -\alpha-\beta)$ is a permutation of $(\gamma, \delta, -\gamma-\delta) \bmod p^{k-l}$ and therefore $(a, b, -a-b)$ is a permutation of $(c, d, -c-d) \bmod p^k$, as required.

Case 2. $l_a = l_{a+b} < l_b < k$. Again we assume $l_c = l_{c+d} \leqq l_d < k$. Now the norm from $Q(\zeta_{p^k})$ to Q of (4.2) yields

$$2p^{l_a} + p^{l_b} = 2p^{l_c} + p^{l_d}. \tag{4.7}$$

We cannot have $l_c = l_d = l_{c+d} < k$ because, from the Case 1, it would imply $l_a = l_b = l_{a+b}$. So $l_c = l_{c+d} < l_d < k$.

Assume first $l_d > l_b$. We obtain from (4.7) $p^{l_c} = 0 \bmod p^{l_a}$ and $2^{l_c+1} = 0 \bmod 2^{l_a+1}$ for $p \neq 2$ and $p = 2$ respectively, implying $l_c \geqq l_a$. Since (4.7) has no solution for $l_d > l_b$ and $l_c > l_a$, we must have $l_c = l_a$, a contradiction since it implies $l_d = l_b$. We obtain the same contradiction if we assume $l_d < l_b$, by exchanging the two triplets $(a, b, a+b)$ and $(c, d, c+d)$. Therefore $l_d = l_b$ and $l_c = l_a$.

Setting $a = \alpha p^{l_a}$, $b = \beta p^{l_b}$, $c = \gamma p^{l_a}$, and $d = \delta p^{l_b}$ with $\alpha, \beta, \gamma, \delta$ coprime with p, (4.2) becomes for $\zeta = \zeta_{p^{k-l_a}}$,

$$(1 - \zeta^{\alpha})(1 - \zeta^{\beta p^{l_b - l_a}})(1 - \zeta^{-\alpha-\beta p^{l_b-l_a}}) = (1 - \zeta^{\gamma})(1 - \zeta^{\delta p^{l_b-l_a}})$$
$$\times (1 - \zeta^{-\gamma-\delta p^{l_b-l_a}}). \tag{4.8}$$

Using (3.3) twice with $X = \zeta^{\beta}$ or ζ^{δ} and $m = p^{l_b - l_a}$, (4.8) can be recast into

$$(1 - \zeta^{\alpha})(1 - \zeta^{-\alpha-\beta p^{l_b-l_a}}) \prod_{j=1}^{p^{l_b-l_a}} (1 - \zeta^{\beta + jp^{k-l_b}})$$
$$= (1 - \zeta^{\gamma})(1 - \zeta^{-\gamma-\delta p^{l_b-l_a}}) \prod_{j=1}^{p^{l_b-l_a}} (1 - \zeta^{\delta + jp^{k-l_b}}). \tag{4.9}$$

Dividing (4.9) by $(1 - \zeta)^{2 + p^{l_b - l_a}}$, we obtain

$$\xi_\alpha \xi_{-\alpha-\beta p^{l_b-l_a}} \prod_{j=1}^{p^{l_b-l_a}} \xi_{\beta + jp^{k-l_b}} = \xi_\gamma \xi_{-\gamma-\delta p^{l_b-l_a}} \prod_{j=1}^{p^{l_b-l_a}} \xi_{\delta + jp^{k-l_b}}. \tag{4.10}$$

The sub-indices of the ξ's are now all coprime with p^{k-l_a}, so we can use their independence to obtain $\gamma = \alpha$ or $-\alpha - \beta p^{l_b - l_a} \bmod p^{k-l_a}$ and $\delta = \beta \bmod p^{k-l_b}$, or equivalently $(c, d) = (a, b)$ or $(-a-b, b) \bmod p^k$. Restoring the symmetry, we have that $(c, d, -c-d)$ is a permutation of $(a, b, -a-b)$ modulo p^k.

Case 3. $l_a = l_b = l_{a+b} = k$. Equation (4.2) shows that one of $c, d, c + d$ must be zero mod p^k (since the left-hand side is zero). Suppose d is the one and $l_c = l_{c+d} \leqq l_d = k$. We want to prove $l_c = l_{c+d} = k$ as well.

If $l_c < k$, i.e. $c \neq 0 \bmod p^k$, every $\sigma_\alpha \neq 1$ in $\mathrm{Gal}(\zeta_n/\zeta_{n/p^k})/\mathrm{Gal}(\zeta_n/\zeta_{n/p^{l_c}}) \sim Z^*_{p^{k-l_c}}$ is such that $\sigma_\alpha(\zeta_n^c) \neq \zeta_n^c$. In other words, σ_α leaves ζ_n^a, ζ_n^b and ζ_n^d invariant, but not ζ_n^c. Acting with σ_α on (4.1) and comparing back with (4.1) yields

$$\zeta_n^c - \zeta_n^{\alpha c} = -\zeta_n^{-d}(\zeta_n^{-c} - \zeta_n^{-\alpha c}) = \zeta_n^{-d-(\alpha+1)c}(\zeta_n^c - \zeta_n^{\alpha c}) . \tag{4.11}$$

Equation (4.11) implies $d + (\alpha + 1)c = 0 \bmod n$. If we write $c = c_1 p^k + \gamma p^{l_c} \frac{n}{p^k}$, then $\alpha c = c_1 p^k + j\gamma p^{l_c} \frac{n}{p^k}$ for $j \neq 1$ in $Z^*_{p^{k-l_c}}$ (see (3.1)). The condition $d + (\alpha + 1)c = 0 \bmod n$ implies $(1 + \alpha)c = 0 \bmod p^k$, or

$$1 + j = 0 \bmod p^{k-l_c} . \tag{4.12}$$

However, we are free to take $j \neq \pm 1$, in $Z^*_{p^{k-l_c}}$, therefore obtaining a contradiction, except if $Z^*_{p^{k-l_c}} = \{1\}$ or $\{+1, -1\}$, that is if $p = 3$ and $l_c = k - 1$, if $p = 2$ and $l_c = k - 2$ or $k - 1$. These are the cases recorded in Eqs. (4.4a – b).

Except in the above special cases for $p = 2$ or 3, we obtain $l_c = l_{c+d} = k$ and so $(c, d, -c-d)$ is a permutation of $(a, b, -a-b) \bmod p^k$ since these six numbers are all zero.

Case 4. $l_a = l_{a+b} < l_b = k$. As in Case 3, Eq. (4.2) shows that one of $c, d, c + d$ must be zero mod p^k. Again we assume $l_c = l_{c+d} \leqq l_d = k$. The equalities $l_c = l_{c+d} = l_d = k$, according to Case 3, are consistent with $l_a = l_{a+b} < l_b = k$ only in the exceptional cases, i.e. $l_a = k - 2$ $(p = 2)$ or $l_a = k - 1$ $(p = 2, 3)$, as shown in (4.4c–d).

We are left with $l_c = l_{c+d} < l_d = k$, so that the situation is now symmetric with respect to the exchange of the triplets $(a, b, -a-b)$ and $(c, d, -c-d)$. As a first step, we show that $l_c \geqq l_a$.

If $l_c < l_a$, we take $\sigma_\alpha \neq 1$ in $\mathrm{Gal}(\zeta_n/\zeta_{n/p^{l_a}})/\mathrm{Gal}(\zeta_n/\zeta_{n/p^{l_c}}) \sim Z_{p^{l_a-l_c}}$ and obtain Eq. (4.11) as before. So we have $d + (\alpha + 1)c = 0 \bmod n$, but here $\alpha c = c_1 p^k + (1 + jp^{k-l_a})\gamma p^{l_c} \frac{n}{p^k}$ with $j \neq 0$ in $Z_{p^{l_a-l_c}}$. It implies $(1 + \alpha)c = 0 \bmod p^k$ or

$$2 + jp^{k-l_a} = 0 \bmod p^{k-l_c}, \quad \text{for all } j \neq 0 \text{ in } Z_{p^{l_a-l_c}} . \tag{4.13}$$

One obtains from (4.13) that $2 = 0 \bmod p^{k-l_a}$, or $p^{k-l_a} = 2$. From this, Eq. (4.13) implies $j = -1 \bmod p^{k-l_c-1}$ for all $j \neq 0$ in $Z_{p^{l_a-l_c}} = Z_{p^{k-l_c-1}}$. This is a contradiction unless $p^{k-l_c-1} = 2$. Thus $p = 2$, $l_a = k - 1$, $l_c = k - 2$ is the only case that escapes the conclusion $l_c \geqq l_a$.

We can repeat the above argument in which we exchange the two triplets $(a, b, a + b)$ and $(c, d, c + d)$. Doing so, we get $l_a \geqq l_c$ unless $p = 2$, $l_a = k - 2$ and $l_c = k - 1$.

Combining the two parts, we conclude that $l_a = l_{a+b} = l_c = l_{c+d}$, except if $p = 2$, $l_a = k - 1$, $l_c = k - 2$ or the other way round, which are the cases listed in (4.4e–f). For the rest, we ignore them and set $l = l_a = l_{a+b} = l_c = l_{c+d} < k$. To complete the proof, we still have to show that $(a, -a-b)$ is a permutation of $(c, -c-d) \bmod p^k$, or equivalently, that $a = \pm c \bmod p^k$.

Set $a = \alpha_1 p^l \frac{n}{p^k} + \alpha_2 p^k$, $b = \beta_2 p^k$, $c = \gamma_1 p^l \frac{n}{p^k} + \gamma_2 p^k$ and $d = \delta_2 p^k$ with α_1 and γ_1 coprime with p. Equation (4.1) in the "additive" form (3.7) yields

$$\zeta_{p^{k-l}}^{\alpha_1}(\zeta_{n/p^k}^{\alpha_2} - \zeta_{n/p^k}^{\alpha_2+\beta_2}) - \zeta_{p^{k-l}}^{-\alpha_1}(\zeta_{n/p^k}^{-\alpha_2} - \zeta_{n/p^k}^{-\alpha_2-\beta_2}) - \zeta_{p^{k-l}}^{\gamma_1}(\zeta_{n/p^k}^{\gamma_2} - \zeta_{n/p^k}^{\gamma_2+\delta_2})$$
$$+ \zeta_{p^{k-l}}^{-\gamma_1}(\zeta_{n/p^k}^{-\gamma_2} - \zeta_{n/p^k}^{-\gamma_2-\delta_2}) + (\zeta_{n/p^k}^{\beta_2} - \zeta_{n/p^k}^{\delta_2} - \zeta_{n/p^k}^{-\beta_2} + \zeta_{n/p^k}^{-\delta_2}) = 0\,. \quad (4.14)$$

Note that, because α_1 and γ_1 are coprime with p, we have $\alpha_1 \neq -\alpha_1 \bmod p^{k-l}$ and $\gamma_1 \neq -\gamma_1 \bmod p^{k-l}$ unless $p^{k-l} = 2$, but in this case $\alpha_1 = \gamma_1 = 1$ from which the claim follows since $a = c \bmod p^k$. We must show that $\alpha_1 = \pm\gamma_1 \bmod p^{k-l}$. Suppose the contrary, $\alpha_1 \neq \gamma_1$ *and* $\alpha_1 \neq -\gamma_1$. It implies that the five powers $\zeta_{p^{k-l}}^{\pm\alpha_1}$, $\zeta_{p^{k-l}}^{\pm\gamma_1}$ and 1 are all distinct. We prove that this leads to a contradiction.

If the five powers of $\zeta_{p^{k-l}}$ entering (4.14) are linearly independent over Q, and therefore also over $Q(\zeta_{n/p^k})$, the corresponding five coefficients must vanish. Setting the coefficient of $\zeta_{p^{k-l}}^{\alpha_1}$ equal to zero leads to $\beta_2 = 0 \bmod \frac{n}{p^k}$, which implies $b = 0 \bmod n$, contrary to the assumption stated in the lemma.

On the other hand, if the five powers of $\zeta_{p^{k-l}}$ are not independent, one of the relations (3.6r) must hold among them. Since each such relation involves p terms, this is impossible for $p \geqq 7$. We consider the other values of p separately.

If $p = 5$, the relation must be the one corresponding to $r = 0$ because it is the only one that contains 1. But then the numbers $\{\pm\alpha_1, \pm\gamma_1\}$ must be identified with $\{5^{k-l-1}, 2.5^{k-l-1}, 3.5^{k-l-1}, 4.5^{k-l-1}\}$, which is impossible since α_1 and γ_1 are coprime with 5, unless $k - l = 1$. If $k - l = 1$, the five powers satisfy the relation $1 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0$. Eliminating one of them in terms of the other (independent) ones, Eq. (4.14) implies that the five coefficients must be equal. Making the coefficients of $\zeta_{p^{k-l}}^{\alpha_1}$ and $\zeta_{p^{k-l}}^{-\alpha_1}$ equal, we obtain $\alpha_2 = \pm(\alpha_2 + \beta_2) \bmod \frac{n}{p^k}$. The solution with the $+$ sign must be rejected as it implies $\beta_2 = 0 \bmod \frac{n}{p^k}$ and $b = 0 \bmod n$. Hence $2\alpha_2 + \beta_2 = 0$. Repeating the argument for the coefficients of $\zeta_{p^{k-l}}^{\gamma_1}$ and $\zeta_{p^{k-l}}^{-\gamma_1}$, we have $2\gamma_2 + \delta_2 = 0$ as well. Equating now the coefficients of $\zeta_{p^{k-l}}^{\alpha_1}$ and $\zeta_{p^{k-l}}^{\gamma_1}$, we obtain $2\alpha_2 = -2\gamma_2 \bmod \frac{n}{p^k}$. Finally the last condition comes from making the coefficients of $\zeta_{p^{k-l}}^{\alpha_1}$ and 1 equal, which, using the relations between β_2, γ_2, δ_2 and α_2, reads

$$\sin\frac{2\pi\alpha_2}{n/p^k} = -4\sin\frac{2\pi\alpha_2}{n/p^k}\cos\frac{2\pi\alpha_2}{n/p^k}\,. \quad (4.15)$$

The factor $\sin\frac{2\pi\alpha_2}{n/p^k}$ cannot be zero, because if it was, $2\alpha_2$ would be zero, implying $\beta_2 = 0$ and $b = 0 \bmod n$. Therefore Eq. (4.15) reduces to $\cos\frac{2\pi\alpha_2}{n/p^k} = -\frac{1}{4}$. The solutions of this quadratic equation read $\zeta_{n/p^k}^{\alpha_2} = -\frac{1}{4}(1 \pm \sqrt{-15})$, which is impossible because $\sqrt{-15}$ does not belong to $Q(\zeta_{n/p^k})$ when $\frac{n}{p^k}$ is coprime with 5. More simply, $\cos\frac{2\pi\alpha_2}{n/p^k} = -\frac{1}{4}$ can be recast into $\zeta_{n/p^k}^{\alpha_2} + \zeta_{n/p^k}^{-\alpha_2} = -\frac{1}{2}$, expressing a cyclotomic integer as a rational non-integer number, a plain contradiction.

Take $p = 3$. There can be a 3-term cyclotomic relation among the five powers $\zeta_{p^{k-l}}^{\pm\alpha_1}$, $\zeta_{p^{k-l}}^{\pm\gamma_1}$ and 1, but two powers will be left over. Their coefficient must vanish, implying either $\beta_2 = 0$ or $\delta_2 = 0$, i.e. $b = 0$ or $d = 0$ modulo n, a contradiction to the assumptions.

The last case is $p = 2$. We assume $p^{k-l} \geqq 16$ (to have five different powers). In order to escape the conclusion $\beta_2 = 0$ or $\delta_2 = 0$ as for $p = 3$, there must be two cyclotomic relations among the four powers $\zeta_{p^{k-l}}^{\pm\alpha_1}$, $\zeta_{p^{k-l}}^{\pm\gamma_1}$. The coefficient of the left-over power 1 must vanish, yielding $\beta_2 = \delta_2$. The 2-term relation involving $\zeta_{p^{k-l}}^{\alpha_1}$ can be $\zeta_{p^{k-l}}^{\alpha_1} + \zeta_{p^{k-l}}^{-\alpha_1} = 0$, $\zeta_{p^{k-l}}^{\alpha_1} + \zeta_{p^{k-l}}^{\gamma_1} = 0$, or $\zeta_{p^{k-l}}^{\alpha_1} + \zeta_{p^{k-l}}^{-\gamma_1} = 0$. It is easy to see that none of them is tenable. This finishes the proof of the lemma. ■

The first lemma is very restrictive and allows us to prove the announced local version of the theorem.

Corollary 1. *Let* $(c, d) = \sigma(a, b)$ *the image of* $(a, b) \in B_n$ *by an automorphism. Then* $(c, d, -c-d)$ *is a permutation* π_i *of* $(a, b, -a-b) \bmod p_i^{k_i}$, *for any* $p_i^{k_i}$ *dividing* n, *or else* $p = 2$, *and we have, up to permutations,* $a = b = c = 0 \bmod 2^k$ *and* $d = 0 \bmod 2^{k-1}$.

Proof. Define $m_i = \frac{n}{p_i^{k_i}}$ for $i = 1, \ldots, s$. We first show that all the $(m_i, m_i) \in B_n$ must be left invariant by the automorphism σ. Let $(c, c) = \sigma(m_i, m_i)$ (necessarily a diagonal root from the discussion below Eq. (3.10)). Equation (4.1) reads

$$(1 - \zeta_{p^k})^2 (1 - \zeta_{p^k}^{-2}) = (1 - \zeta_n^c)^2 (1 - \zeta_n^{-2c}) , \tag{4.16}$$

where, for simplicity, we dropped the index i from p_i, k_i and m_i. From (3.2), the norm $N_{Q(\zeta_n)/Q}$ of the left-hand side of (4.16) is a (strictly positive) power of p. (The norm could be zero if $p^k = 2$, but in that case $(m, m) = (\frac{n}{2}, \frac{n}{2})$ is not in B_n.) If the same is to be true of the right-hand side, c must be a multiple of $\frac{m}{2}$, or of m if m is odd, since otherwise the norm of the right-hand side of (4.16) is either equal to 1 or equal to the power of a prime different from p. In case $c = \frac{m}{2} \bmod m$ or equivalently $c = \gamma m + \frac{n}{2}$ (hence m is even and p is odd), the norm from $Q(\zeta_n)$ to Q of $1 - \zeta_n^c = 1 + \zeta_{p^k}^{\gamma}$ is equal to 1. Thus the norm of (4.16) requires (remember p is odd)

$$N_{Q(\zeta_n)/Q}(1 - \zeta_n^{-2c}) = N_{Q(\zeta_n)/Q}[(1 - \zeta_{p^k})^2 (1 - \zeta_{p^k}^{-2})] = p^{3\varphi(m)} . \tag{4.17}$$

Equation (4.17) has no solution for c unless $p = 3$, $p^k \geqq 9$ and $\operatorname{ord}_3 \gamma = 1$, in which case Eq. (4.16) can be recast into

$$(1 - \zeta_{3^k})^2 (1 - \zeta_{3^k}^{-2})(1 - \zeta_{3^k}^{\gamma})^2 = (1 - \zeta_{3^k}^{2\gamma})^2 (1 - \zeta_{3^k}^{-2\gamma}) . \tag{4.18}$$

Then using an argument similar to that of Case 2 in Lemma 1 shows that (4.18) has no solution for γ. We conclude that the assumption that c is not a multiple of m leads to a contradiction.

Setting $c = \gamma m$, Eq. (4.16) becomes

$$(1 - \zeta_{p^k})^2 (1 - \zeta_{p^k}^{-2}) = (1 - \zeta_{p^k}^{\gamma})^2 (1 - \zeta_{p^k}^{-2\gamma}) . \tag{4.19}$$

The first lemma with $n = p^k$ implies that $(\gamma, \gamma, -2\gamma)$ is a permutation of $(1, 1, -2)$, i.e. $\gamma = 1$ and $c = m$. We thus obtain $\sigma(m_i, m_i) = (m_i, m_i)$ for any $m_i = \frac{n}{p_i^{k_i}}$ except $m_i = \frac{n}{2}$. The first step of the proof, namely c must be a multiple of m, can alternatively be obtained by combining the arithmetical symmetry (3.10) (in which we take $v = 1 \bmod p^k$) with norm arguments. As to the second step, namely $c = \gamma m$ implies $\gamma = 1$, it also follows from the classification of simple currents [16].

Since the weights (m_i, m_i) are left invariant by the automorphisms, we obtain that, for any (a, b), the pairs (a, b) and $(c, d) = \sigma(a, b)$ must satisfy Eq. (4.1) and (4.2) with p^k replaced by any $p_i^{k_i} \neq 2$. Using again the first lemma with p being any p_i, we obtain that $(c, d, -c-d)$ is a permutation of $(a, b, -a-b) \bmod p_i^{k_i}$, except possibly if one of the equations (4.4) holds. (Note that although the value $p_i^{k_i} = 2$ is not allowed, the Lemma 1 in fact covers all the situations which could arise in this case.) Apart from Eq. (4.4a) and (4.4c) for $p = 2$, we now show that the others are not compatible with (4.1).

Let us first consider the case (4.4a) with $p = 3$. We suppose $a = b = c + d = 0 \bmod 3^k$ and $\mathrm{ord}_3 c = \mathrm{ord}_3 d = k - 1$. Setting $a = \alpha 3^k$, $b = \beta 3^k$, $c = \gamma 3^k + \frac{n}{3}$ and $d = \delta 3^k + \frac{2n}{3}$, one obtains from (4.1) with $\omega = \zeta_3$,

$$(1-\zeta^\alpha)(1-\zeta^\beta)(1-\zeta^{-\alpha-\beta}) = (1-\omega\zeta^\gamma)(1-\omega^2\zeta^\delta)(1-\zeta^{-\gamma-\delta}) \,,$$
$$\zeta = \zeta_{n/3^k} \,. \tag{4.20}$$

Expanding (4.20) in powers of ω and setting to zero the coefficients of ω and 1 (using $1 + \omega + \omega^2 = 0$ to eliminate ω^2) yield respectively $\gamma = \delta \bmod \frac{n}{3^k}$ and the condition

$$(1-\zeta^\alpha)(1-\zeta^\beta)(1-\zeta^{-\alpha-\beta}) = \zeta^\gamma + \zeta^{2\gamma} - \zeta^{-\gamma} - \zeta^{-2\gamma} \,. \tag{4.21}$$

If $\frac{n}{3^k}$ is a prime power, then $(\alpha, \beta, -\alpha-\beta)$ is a permutation of $(\gamma, \gamma, -2\gamma)$ from Lemma 1. Since the situation is still symmetric in $(\alpha, \beta, -\alpha-\beta)$, we may take $\alpha = \beta = \gamma$, in which case (4.21) reduces to $\zeta^\gamma = \zeta^{-\gamma}$, contradicting $(c, d) \in B_n$.

If on the other hand, $\frac{n}{3^k}$ is not a prime power, then there exists a prime power $q^l \mid \frac{n}{3^k}$ such that $(\alpha, \beta, -\alpha-\beta)$ is a permutation of $(\gamma, \gamma, -2\gamma)$ modulo q^l, that is $q \neq 2$. Furthermore we can assume $\gamma \neq 0 \bmod q^l$. (If $\gamma = 0 \bmod q^l$ for every $q \neq 2$, then $\alpha = \beta = 0 \bmod q^l$ as well, and we are back to (4.21) with an effective $\zeta = \zeta_{2^{k_2}}$, a case already discussed.) Again we choose $\alpha = \beta = \gamma \bmod q^l$. Equation (4.21) reads

$$\zeta_{q^l}^{\gamma}(\xi^\alpha + \xi^\beta + \xi^\gamma) + \zeta_{q^l}^{2\gamma}(\xi^{2\gamma} - \xi^{\alpha+\beta}) - \text{c.c.} = 0, \quad \xi = \zeta_{n/3^k q^l} \,. \tag{4.22}$$

Since $q \geqq 5$ and $\gamma \neq 0 \bmod q^l$, the four powers of ζ_{q^l} in (4.22) are linearly independent. The corresponding coefficients must vanish, implying in particular $\xi^\alpha + \xi^\beta + \xi^\gamma = 0$. This last equation has no solution since 3 does not divide $\frac{n}{3^k q^l}$.

Thus the exceptions (4.4a) and (4.4c) for $p = 3$ are ruled out. Cases (4.4b, d − f) must be similarly excluded. ∎

Note that if n is a prime power, Corollary 1 is the same as the theorem. For composite n, apart from the exception for $p = 2$, all that is yet to be proved is that the permutations π_i in Corollary 1 cannot depend on i.

5. Proof of the Theorem

In order to prove that the permutation π_i of Corollary 1 cannot depend on i, we first note the following

Corollary 2. *The diagonal roots of B_n are left invariant by the automorphisms,* i.e. $\sigma(a,a)=(a,a)$.

Proof. Since the image by σ of (a,a) must be a diagonal root, we have $c=d$ in Corollary 1. If $(c,c,-2c)=\pi_i(a,a,-2a) \bmod p_i^{k_i}$ for all i, the permutations π_i can only be the identity. So the only case to worry about is when $(c,c,-2c)=\pi_i(a,a,-2a) \bmod p_i^{k_i}$ for $p_i \neq 2$, yielding $c=a \bmod \frac{n}{2^{k_2}}$, and $a=0 \bmod 2^{k_2}$, $c=2^{k_2-1} \bmod 2^{k_2}$ (or a and c interchanged). In this case, Eq. (4.1) requires $1-\zeta^a_{n/2^{k_2}} = \pm(1+\zeta^a_{n/2^{k_2}})$, which has no solution. ■

Define $m_{ij}=\frac{n}{p_i^{k_i}p_j^{k_j}}$ for $1 \leqq i \neq j \leqq s$. Since $\sigma(m_{ij},m_{ij})=(m_{ij},m_{ij})$, the pairs $(c,d)=\sigma(a,b)$ must satisfy the new set of equations $[S,\sigma]_{(m_{ij},m_{ij}),(a,b)}=0$ for any $m_{ij}\in B_n$. If, to save the notation, one sets $m=\frac{n}{p^k q^l}$, with $p^k \neq q^l$ any prime powers $p_i^{k_i}$, $p_j^{k_j}$ dividing n, these equations read

$$(1-\zeta^a_{p^kq^l})(1-\zeta^b_{p^kq^l})(1-\zeta^{-a-b}_{p^kq^l})=(1-\zeta^c_{p^kq^l})(1-\zeta^d_{p^kq^l})(1-\zeta^{-c-d}_{p^kq^l})\,. \quad (5.1)$$

Lemma 2. *Let p and q be two different primes and $(c,d)=\sigma(a,b)$ two weights of B_n. If $a, b, a+b \neq 0 \bmod p^kq^l$, then $(c,d,-c-d)$ is a permutation of $(a,b,-a-b)$ $\bmod p^kq^l$.*

Proof. We may assume $p>q$, so that $p \geqq 3$. We also note that $a, b, a+b \neq 0 \bmod p^kq^l$ implies $c, d, c+d \neq 0 \bmod p^kq^l$ (neither side of (5.1) vanishes). Let us define

$$a=\alpha_p q^l+\alpha_q p^k \bmod p^kq^l,\quad b=\beta_p q^l+\beta_q p^k \bmod p^kq^l\,,$$
$$c=\gamma_p q^l+\gamma_q p^k \bmod p^kq^l,\quad d=\delta_p q^l+\delta_q p^k \bmod p^kq^l\,. \quad (5.2)$$

From Corollary 1, we have

$$(\gamma_p,\delta_p,-\gamma_p-\delta_p)=\pi_p(\alpha_p,\beta_p,-\alpha_p-\beta_p) \bmod p^k,\quad \pi_p\in S_3\,. \quad (5.3)$$

The problem being completely symmetric under a permutation of c, d and $-c-d$, we fix that freedom by requiring $\pi_p=1$, so that $\gamma_p=\alpha_p$ and $\delta_p=\beta_p$. We aim at proving $\pi_q=1$ as well, i.e. $\gamma_q=\alpha_q$ and $\delta_q=\beta_q$.

With $\pi_p=1$, Eq. (5.1) reads

$$\zeta^{\alpha_p}_{p^k}(\zeta^{\alpha_q}_{q^l}-\zeta^{\gamma_q}_{q^l})-\zeta^{-\alpha_p}_{p^k}(\zeta^{-\alpha_q}_{q^l}-\zeta^{-\gamma_q}_{q^l})+\zeta^{\beta_p}_{p^k}(\zeta^{\beta_q}_{q^l}-\zeta^{\delta_q}_{q^l})-\zeta^{-\beta_p}_{p^k}(\zeta^{-\beta_q}_{q^l}-\zeta^{-\delta_q}_{q^l})$$
$$-\zeta^{\alpha_p+\beta_p}_{p^k}(\zeta^{\alpha_q+\beta_q}_{q^l}-\zeta^{\gamma_q+\delta_q}_{q^l})+\zeta^{-\alpha_p-\beta_p}_{p^k}(\zeta^{-\alpha_q-\beta_q}_{q^l}-\zeta^{-\gamma_q-\delta_q}_{q^l})=0\,. \quad (5.4)$$

As often with additive equations, different cases must be distinguished. First, there is the question as to how many among the numbers α_p, β_p, $\alpha_p+\beta_p$ are zero modulo p^k. There can be zero, one or three. The easy case is when all three are zero, because there is nothing much to prove. From Corollary 1, we have $(\gamma_q,\delta_q,-\gamma_q-\delta_q)=\pi_q(\alpha_q,\beta_q,-\alpha_q-\beta_q)$ (the exception for $q=2$ plays no role because of the assumption $a, b, a+b \neq 0 \bmod p^kq^l$). Setting $\pi_p=1$ does not fix anything (any π_p has the same effect) and we can harmlessly choose $\pi_p=\pi_q$ whatever π_q is.

Suppose now that one of α_p, β_p, $\alpha_p+\beta_p$ is zero, $\beta_p=0$ say. Then the powers 1 and $\zeta^{\pm\alpha_p}_{p^k}$ are all different (remember $p \geqq 3$). If $p \geqq 5$ they are linearly independent, so that the corresponding three coefficients must vanish. The coefficient of 1 being zero implies $\delta_q = \beta_q$ or $\delta_q = \frac{q^l}{2} - \beta_q$, while the coefficient of $\zeta_{p^k}^{\alpha_p}$ set to zero yields

$$\zeta_{q^l}^{\alpha_q} - \zeta_{q^l}^{\gamma_q} = \zeta_{q^l}^{\alpha_q+\beta_q} - \zeta_{q^l}^{\gamma_q+\delta_q}\,. \tag{5.5}$$

If $\delta_q = \beta_q$, (5.5) obviously gives $\gamma_q = \alpha_q$. If $\delta_q = \frac{q^l}{2} - \beta_q$, Eq. (5.5) becomes $\zeta_{q^l}^{\alpha_q}(1 - \zeta_{q^l}^{\beta_q}) = \zeta_{q^l}^{\gamma_q - \beta_q}(1 + \zeta_{q^l}^{\beta_q})$, so that $(1 - \zeta_{q^l}^{\beta_q})/(1 + \zeta_{q^l}^{\beta_q}) = \pm i$ is a purely imaginary root of unity. In turn this means $\zeta_{q^l}^{\beta_q} = \mp i$, and again $\gamma_q = \alpha_q$, $\delta_q = \frac{q^l}{2} - \beta_q = \beta_q$.

If $p = 3$ $(q = 2)$, the powers 1 and $\zeta_{p^k}^{\pm\alpha_p}$ are either independent, in which case we reach the conclusion $\gamma_q = \alpha_q$, $\delta_q = \beta_q$, or else $\alpha_p = \pm p^{k-1}$. In the latter case, Eq. (5.4) (with $\beta_p = 0$) implies the equality of the three coefficients,

$$\zeta_{q^l}^{\alpha_q} - \zeta_{q^l}^{\gamma_q} - \zeta_{q^l}^{\alpha_q+\beta_q} + \zeta_{q^l}^{\gamma_q+\delta_q} = -\zeta_{q^l}^{-\alpha_q} + \zeta_{q^l}^{-\gamma_q} + \zeta_{q^l}^{-\alpha_q-\beta_q} - \zeta_{q^l}^{-\gamma_q-\delta_q}\,, \tag{5.6a}$$

$$\zeta_{q^l}^{\alpha_q} - \zeta_{q^l}^{\gamma_q} - \zeta_{q^l}^{\alpha_q+\beta_q} + \zeta_{q^l}^{\gamma_q+\delta_q} = \zeta_{q^l}^{\beta_q} - \zeta_{q^l}^{\delta_q} - \zeta_{q^l}^{-\beta_q} + \zeta_{q^l}^{-\delta_q}\,. \tag{5.6b}$$

From Corollary 1, $(\gamma_q, \delta_q, -\gamma_q - \delta_q)$ must be a permutation π_q of $(\alpha_q, \beta_q, -\alpha_q - \beta_q)$. Trying each of the five $\pi_q \neq 1$, we end up with impossible equations or contradictions to $a, b, a + b \neq 0 \bmod p^k q^l$, or else α_q and β_q are related in such a way that $\gamma_q = \alpha_q$ and $\beta_q = \delta_q$ still hold. Thus $\pi_q = 1$.

We turn to the last case: none of α_p, β_p, $\alpha_p + \beta_p$ is zero. We distinguish the cases $p \geqq 5$ from $p = 3$.

For $p \geqq 5$, there can be no cyclotomic relation among the six powers of ζ_{p^k} entering (5.4). (For $p \geqq 7$, it is obvious, while for $p = 5$, the would-be relation has to be (3.6r) with $r = 0$ because it must contain one of the powers along with its complex conjugate. But then one of the powers must be 1.) Therefore those which are different are linearly independent and their coefficient must vanish. This still leaves two possibilities: the six powers are different or only four of them are different. The first case clearly yields $\gamma_q = \alpha_q$ and $\delta_q = \beta_q$. The second possibility arises if $\alpha_p = \beta_p$ or $\alpha_p = -\alpha_p - \beta_p$. (Any other identification contradicts $\alpha_p, \beta_p, \alpha_p + \beta_p \neq 0 \bmod p^k$.) If $\alpha_p = \beta_p$, one obtains from (5.4) either $(\gamma_q, \delta_q, -\gamma_q - \delta_q) = (\alpha_q, \beta_q, -\alpha_q - \beta_q)$ (i.e. $\pi_q = 1$) or $(\gamma_q, \delta_q, -\gamma_q - \delta_q) = (\beta_q, \alpha_q, -\alpha_q - \beta_q)$, that is π_q exchanges the first two objects, $\pi_q(1, 2, 3) = (2, 1, 3)$. But since $\alpha_p = \beta_p$, we could as well have fixed π_p by requiring $\pi_p(1, 2, 3) = (2, 1, 3)$, in which case we have $\pi_p = \pi_q$. (The permutation π_q is only defined relative to π_p.) The other case with four different powers of ζ_{p^k}, namely $\alpha_p = -\alpha_p - \beta_p$, is treated similarly.

Finally we set $p = 3$ and make the same kind of discussion. First there cannot be a cyclotomic relation $\zeta_{p^k}^x + \zeta_{p^k}^y + \zeta_{p^k}^z = 0$, with x, y, z chosen from $\pm\alpha_p$, $\pm\beta_p$, $\pm(\alpha_p + \beta_p)$. Because if there is, the triplet (x, y, z) must be equal to $(r, r + p^{k-1}, r + 2 \cdot p^{k-1})$ for some r. However, every choice of x, y, z contradicts α_p, β_p, $\alpha_q + \beta_p \neq 0$. Thus those powers of ζ_{p^k} in (5.4) which are different must have a vanishing coefficient. If the six powers are all different, (5.4) gives $\gamma_q = \alpha_q$ and $\delta_q = \beta_q$. If they are not all different, there are only two possibilities as in the previous case $p \geqq 5$: $\alpha_p = \beta_p$ or $\alpha_p = -\alpha_p - \beta_p$. (Here however both equalities may hold at the same time.) We only consider the first case, $\alpha_p = \beta_p$, the other being similar.

If $\alpha_p = \beta_p$ but $\alpha_p \neq -\alpha_p - \beta_p$, the four powers $\zeta_{p^k}^{\pm\alpha_p}$ and $\zeta_{p^k}^{\pm(\alpha_p+\beta_p)}$ are different and we obtain $\pi_p = \pi_q$ as in the $p \geqq 5$ case. If $\alpha_p = \beta_p = -\alpha_p - \beta_p$, the two left-over powers $\zeta_{p^k}^{\pm\alpha_p}$ are different. Their coefficient must vanish, yielding the following condition:

$$\zeta_{q^l}^{\alpha_q} + \zeta_{q^l}^{\beta_q} + \zeta_{q^l}^{-\alpha_q-\beta_q} = \zeta_{q^l}^{\gamma_q} + \zeta_{q^l}^{\delta_q} + \zeta_{q^l}^{-\gamma_q-\delta_q} . \tag{5.7}$$

If $(\gamma_q, \delta_q, -\gamma_q-\delta_q) = \pi_q(\alpha_q, \beta_q, -\alpha_q-\beta_q)$ is a permutation, we can choose $\pi_p = \pi_q$ whatever π_q is (since $\alpha_p = \beta_p = -\alpha_p - \beta_p$). If, on the other hand, $\alpha_q, \beta_q, \gamma_q, \delta_q$ appear as the exception of Corollary 1, we readily check that (5.7) is not satisfied. ■

We can now complete the proof. If n is composed of only two primes, Lemma 2 proves the final result: $(c, d, -c-d)$ is a permutation of $(a, b, -a-b) \bmod n$. Therefore we may assume that at least three different primes divide n. Let $(c, d) = \sigma(a, b)$.

Let us split the set of primes dividing n into two subsets, B and G. B will contain those primes p_i such $a, b, a+b$ are all $0 \bmod p_i^{k_i}$, while G receives the primes which are not in B. Note that if p_i is in G, then at most one among $a, b, a+b$ can be zero modulo $p_i^{k_i}$, and we accordingly split G into four subsets:

$$\begin{aligned} G_0 &= \{p_i \in G : a, b, a+b \neq 0 \bmod p_i^{k_i}\} , \\ G_1 &= \{p_i \in G : (a, b, -a-b) = (0, b, -b) \bmod p_i^{k_i}\} , \\ G_2 &= \{p_i \in G : (a, b, -a-b) = (a, 0, -a) \bmod p_i^{k_i}\} , \\ G_3 &= \{p_i \in G : (a, b, -a-b) = (a, -a, 0) \bmod p_i^{k_i}\} . \end{aligned} \tag{5.8}$$

We first prove that $(c, d, -c-d)$ is a permutation of $(a, b, -a-b)$ modulo G, and by this we mean modulo $\prod_{p_i \in G} p_i^{k_i}$.

If $G_0 \neq \emptyset$, it contains a prime p_1 such that $a, b, a+b \neq 0 \bmod p_1^{k_1} p_i^{k_i}$ for every $p_i \neq p_1$. Then Lemma 2 implies that $(c, d, -c-d)$ is a permutation of $(a, b, -a-b) \bmod p_1^{k_1} p_i^{k_i}$ for all $i \geqq 2$, from which the stronger claim clearly follows: $(c, d, -c-d)$ is a permutation of $(a, b, -a-b)$ modulo n, since $\pi_i = \pi_1$ for all $i \geqq 2$.

If $G_0 = \emptyset$, at least two of the subsets G_1, G_2, G_3 are non-empty, since otherwise it would contradict $a, b, a+b \neq 0 \bmod n$. From the definitions (5.8), it follows that if p_i and p_j belong to two different subsets G_k, then a, b, $a+b \neq 0 \bmod p_i^{k_i} p_j^{k_j}$ and $(c, d, -c-d)$ is a permutation of $(a, b, -a-b) \bmod p_i^{k_i} p_j^{k_j}$. By making i and j vary over the three subsets (but keeping p_i and p_j in different G_k), we obtain the same result for any pair p_i, p_j of primes in G, whether in different subsets or not. Again the statement follows: $(c, d, -c-d)$ is a permutation of $(a, b, -a-b) \bmod G$.

We now consider the primes in B. For the primes p_i in B different from 2, we know that $(c, d, -c-d)$ is permutation of $(a, b, -a-b) = (0, 0, 0) \bmod p_i^{k_i}$. Which permutation it is becomes irrelevant since the three objects are identical anyway. We can therefore choose the same permutation as the one relating $(c, d, -c-d)$ to $(a, b, -a-b) \bmod G$, and doing so we obtain

$$(c, d, -c-d) = \pi(a, b, -a-b) \bmod \frac{n}{2^{k_2}} . \tag{5.9}$$

The only remaining case is when 2 is in B, that is when a and b are both multiples of 2^{k_2}. In this case, Corollary 1 does not guarantee that c and d are also multiples of

2^{k_2}. If they are, then of course the statement (5.9) is also true mod n. Thus it remains to rule out the single exception of Corollary 1, namely $a = b = 0 \bmod 2^{k_2}$, and say $c = 0 \bmod 2^{k_2}$, $d = 2^{k_2 - 1} \bmod 2^{k_2}$. We can do so by repeating the above argument in which we exchange $(a, b, -a-b)$ with $(c, d, -c-d)$. We define two new sets B' and G' as above but relative to $(c, d, -c-d)$. From $d = 2^{k_2-1} \bmod 2^{k_2}$, we find that $p_i = 2$ belongs to G', and since Corollary 1 and Lemma 2 are symmetric under the interchange of $(a, b, -a-b)$ and $(c, d, -c-d)$, we conclude that (5.9) holds modulo n. The proof of the theorem is complete.

6. Perspectives

The proof we gave for $SU(3)$ in Sects. 4 and 5 has clearly a multiplicative and an additive part. They both can be applied to any other algebra, since in most instances, the problem is to assess independence properties of cyclotomic numbers. As this usually involves discussing different cases separately, it can become rather painful when the number of terms increases. This is especially true when additive relations must be examined. So for practical feasability, solving the problem for large algebras requires a more systematic way of dealing with the additive part. Another possibility is to keep the whole discussion at the multiplicative level, which is more satisfactory and easier to handle, even when the number of terms gets large. Essentially, this means changing the arguments of Lemma 2 so as to keep the multiplicative character of Eq. (5.1). It would not yield a simpler proof for $SU(3)$, but it looks more promising for larger algebras.

Acknowledgements. I would like to thank E. Thiran and J. Weyers for discussions during the early stage of this work. While this manuscript was being completed, I received the preliminary version of a preprint by T. Gannon which contains the full classification of $SU(3)$ modular invariant partition functions [17]. In particular, it also contains for $SU(3)$, by using the results of [11], the classification of automorphisms shown here.

References

1. Cardy, J.: Operator content of two-dimensional conformally invariant theories. Nucl. Phys. **B270** [FS16], 186–204 (1986)
2. Moore, G., Seiberg, N.: Naturality in conformal field theory. Nucl. Phys. **B313**, 16–40 (1989)
3. Verlinde, E.: Fusion rules and modular transformations in 2D conformal field theory. Nucl. Phys. **B300** [FS22], 360–376 (1988)
4. Capelli, 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)
5. Capelli, A.: Modular invariant partition functions of superconformal theories. Phys. Lett. **185B**, 82–88 (1987)
6. Gepner, D., Qiu, Z.: Modular invariant partition functions for parafermionic theories. Nucl. Phys. **B285** [FS19], 423–453 (1987)
7. Ginsparg, P.: Curiosities at $c = 1$. Nucl. Phys. **B295** [FS21], 153–170 (1988); Kiritsis, E.: Proof of the completeness of the classification of rational conformal theories with $c = 1$. Phys. Lett. **217B**, 427–430 (1989)
8. Ruelle, P., Thiran, E., Weyers, J.: Modular Invariant Partition Functions for Affine $\widehat{SU(3)}$ Theories at Prime Heights. Commun. Math. Phys. **133**, 305–322 (1990)
9. Ruelle, P., Thiran, E., Weyers, J.: Implications of an arithmetical symmetry of the commutant for modular invariants. Nucl. Phys. **B402**, 693–708 (1993)

10. Kac, V.: Infinite Dimensional Lie Algebras. Boston, Basel, Stuttgart: Birkhäuser 1983
11. Bégin, L., Mathieu, P., Walton, M.: $\widehat{su(3)}_k$ fusion coefficients. Mod. Phys. Lett. **A7**, 3255–3266 (1992)
12. Bernard, D.: String characters from Kac–Moody automorphisms. Nucl. Phys. **B288**, 628–648 (1987)
13. Altschüler, D., Lacki, J., Zaugg, P.: The affine Weyl group and modular invariant partition functions. Phys. Lett. **205B**, 281–284 (1988)
14. Verstegen, D.: New exceptional modular invariant partition functions for simple Kac–Moody algebras. Nucl. Phys. **B346**, 349–386 (1990)
15. Washington, L.: Introduction to Cyclotomic Fields. Graduate Texts in Mathematics, Vol. **83**. Berlin, Heidelberg, New York: Springer 1982
16. Fuchs, J.: Simple WZW Currents. Commun. Math. Phys. **136**, 345–356 (1991)
17. Gannon, T.: The Classification of Affine $SU(3)$ Modular Invariant Partition Functions. 1992

Communicated by G. Felder