ELSEVIER

Journal of Geometry and Physics 22 (1997) 134–189

JOURNAL OF GEOMETRY AND PHYSICS

Comments on the links between $su(3)$ modular invariants, simple factors in the Jacobian of Fermat curves, and rational triangular billiards

M. Bauer [a], A. Coste [b,1], C. Itzykson [a], P. Ruelle [c,2],

[a] *Service de Physique Théorique de Saclay, F-91191, Gif-sur-Yvette, France*
[b] *Centre de Physique Théorique, UPR 7061, CNRS Luminy case 907, F-13288, Marseille cedex 09, France*
[c] *Institut de Physique Théorique, Université Catholique de Louvain, B-1348, Louvain-La-Neuve, Belgium*

Received 24 April 1996

Abstract

We examine the proposal made recently that the $su(3)$ modular invariant partition functions could be related to the geometry of the complex Fermat curves. Although a number of coincidences and similarities emerge between them and certain algebraic curves related to triangular billiards, their meaning remains obscure. In an attempt to go beyond the $su(3)$ case, we show that any rational conformal field theory determines canonically a Riemann surface.

1991 MSC: 81T40; 14H40; 14K22
Keywords: Affine Lie algebras; Modular invariance; Abelian varieties

1. Introduction

The partition function of a rational conformal field theory (RCFT) on a torus is subjected to modular invariance constraints. These constraints turn out to be very strong, and have led to the classification of families of models. The most celebrated achievement is the ADE classification of $su(2)$ Wess–Zumino–Novikov–Witten models [1]. Its relationship with the classification of simply laced Lie algebras, a one-to-one correspondence, is an a posteriori observation. Two very different problems lead to the same classification pattern, but the

[1] Member of the CNRS.
[2] Chercheur qualifié FNRS.

PII S0393-0440(96)00027-7

proofs have very little in common. This remarkable coincidence sustained the hope that RCFTs, combined with the requirement of modular invariance, could perhaps be organized by known mathematical structures, thereby bringing order in the so-called conformal zoo, and possibly much deeper connections with seemingly unrelated problems. At the moment, however, such general connections remain very uncertain. Even in the case of the $su(2)$ models, the reason behind the ADE correspondence has remained elusive. The few other families of theories classified up to now are either closely related to ADE, or clearly related to arithmetical peculiarities, which look like mere facts, and for that reason, are not understood.

The classification of $su(3)$ modular invariants, due to Gannon [2], belongs to this second class. But even if a clear interpretation of the result is lacking, the work on $su(3)$ has led to fundamental progress in our understanding of general methods to address the problem of modular invariance. In particular a very powerful (but weaker than the full modular invariance) selection rule, called the parity rule, has emerged. First defined in a restricted context [3,4], it has now been shown to hold in any rational conformal field theory as an application of Galois theory [5]. A few years ago, Thiran, Weyers and one of the authors [4] observed that the parity rule for $su(3)$ appears in a totally different context, as an isomorphism criterion for Abelian varieties that build up the decomposition of the Jacobian of Fermat curves in simple factors. In this case, existing mathematical results about Fermat curves apply directly to the problem of modular invariance, and the work of Koblitz and Rohrlich [6] was used to classify the modular invariants when the height (to be defined in Section 2) is prime to 6 [4]. Our first aim in this paper is to explore this connection in more detail. In particular, we shall show that $su(3)$ conformal field theories and Fermat curves have striking similarities that might go beyond the above observation, but they have important differences as well. Also, quite unexpectedly, the problem of rational triangular billiards [7] is naturally related to the parity rule and to modular invariants.

We will present a certain number of "strange coincidences", relating in a curious way the three topics we discuss in this article, namely the $su(3)$ models, the complex Fermat curves and the triangular billiards. These observations take place at various levels, but as intriguing as they may be, they remain obscure. In fact the obvious observation that conformal field theories are often organized in families (indexed by the level for Wess–Zumino–Novikov–Witten models, or the degree of Fermat curves for instance) is the starting point for other puzzling remarks. The paper is organized as follows.

Section 2 is a general reminder of conformal theories with an affine Lie algebra, which we take to be $su(3)$ for definiteness. The material is not new, but presented in such a way as to emphasize the links with Fermat curves. This section contains a short review on the modular group and the modular invariance problem, and recalls the parity selection rule. We also prove some character identities related to lattice summations.

Section 3 is an introduction for non-experts to the geometry of complex Fermat curves and their Jacobians. Complex multiplication in Abelian varieties is briefly discussed. Again there is no claim to originality. We present the criterion of Shimura–Taniyama to study the isogeny classes of Abelian varieties and we show its equivalence with the parity rule for $su(3)$.

In Section 4, we start with a short introduction to the notion of "dessins d'enfants" (see for instance the collective contribution [8]). They give a convenient framework to discuss combinatorial and analytic aspects of certain (special, but ubiquitous for the objects we study) ramified coverings between Riemann surfaces. This general discussion puts on the same footing Fermat curves and their holomorphic differentials, rational triangular billiards and some aspects of their trajectories. We then attempt to make a list of similarities between $su(3)$ affine characters and holomorphic differentials on Fermat curves. In particular we show that the identity block of the exceptional modular invariants for $su(3)$ is encoded in a sequence of rational maps between the degree 24 Fermat curve and algebraic curves associated with rational triangular billiards. We also show that holomorphic differentials on Fermat curves can be reinterpreted, via uniformization theory, as modular forms that share some of the properties of the $su(3)$ characters, and for which we solve the modular problem.

Finally we explore in Section 5 the algebraic consequences of the fact that the genus one characters of an arbitrary rational conformal field theory are automorphic functions for a finite index subgroup of the modular group. We prove that the characters are all algebraic over $\mathbb{Q}(j)$, a property that allows to associate a well-defined Riemann surface with any rational conformal field theory (or with any chiral algebra). We study some general features of the Riemann surfaces arising in this way, and show how they can be computed in actual cases. This is illustrated by determining the surface associated to the $su(3)$, level 1 ($su(3)$, level 2, is relegated to a separate appendix).

There are two appendices containing technicalities and computational details.

Claude Itzykson's premature death is a tragedy for his friends and collaborators. This article tries to address questions that were raised more than three years ago and Claude participated very actively in the early stages of this work. He not only did actual computations (the link between billiards and blocks of modular invariants is only one of those), but he also pointed out some possible hidden facets of the problem. We tried to put his ideas in a form as close as possible to Claude's standards. Anyway, it is fair to say that he should be credited for most of the ideas while the other authors should be blamed for the inaccuracies. We miss him very much.

2. Modular invariance for $su(3)$ theories

We review in this section the basic features of affine Lie algebras and the problem of modular invariance. We will mainly consider the so-called untwisted $su(3)$ affine Lie algebra, but most of the material presented here has straightforward generalizations to other algebras [9–11].

2.1. *Affine representations*

The Wess–Zumino–Novikov–Witten (WZNW) models are rational conformal theories which describe two-dimensional massless physical systems possessing an affine Lie algebra as dynamical current symmetry [10,12,13]. The building block for the chiral algebra pertaining to the $su(3)$-based models is the current algebra known as $\widehat{su(3)}_k$

$$[x_l, y_m] = [x, y]_{l+m} + kl\,\delta_{l+m,0}\,\langle x, y\rangle, \quad x, y \in su(3), \quad l, m \in \mathbb{Z}. \tag{2.1}$$

k is a central element, $[k, x_l] = 0$, called the level, and $\langle\cdot,\cdot\rangle$ is the Killing form on the finite-dimensional algebra $su(3)$. The full symmetry algebra $\mathcal{A}$ is built on the direct product $\widehat{su(3)}_k \otimes_I \widehat{su(3)}_k$, where $\otimes_I$ means that the central extensions are identified. An appropriate completion of the enveloping algebra of (2.1) contains a central extension of the conformal algebra with central charge $c_k = k \dim su(3)/(k+g) \equiv 8 - (24/n)$, where $g = 3$ is the dual Coxeter number of $su(3)$ and $n \equiv k + 3$ is called the height. If we write $x(z) = \sum_m x_m z^{-1-m}$, the Virasoro algebra is generated by the density $L(z) = \sum_m L_m z^{-m-2} = \alpha\colon\langle x(z), x(z)\rangle\colon$ for a suitable choice of the constant α. One traditionally denotes the generators of the symmetry algebra $\mathcal{A}$ by $x_l \otimes \overline{x}_m$, and those of the Virasoro algebra by $L_l \otimes \overline{L}_m$.

The Hilbert space $\mathcal{H}$ of the theory is the direct sum of highest weight $\mathcal{A}$-modules:

$$\mathcal{H} = \bigoplus_{p,p'} N_{p,p'}\,\mathcal{R}_p \otimes \mathcal{R}_{p'} \tag{2.2}$$

with $N_{p,p'} \in \mathbb{N}$ giving the multiplicities. If one requires that the representations $\mathcal{R}_p$ be unitary, as appropriate in the case of WZNW models which are unitary field theories, the level hence the height must be a positive integer (implying $c_k \geq 0$), and only a finite number of representations are possible. They are labeled by strictly (i.e. shifted) dominant $su(3)$ weights $p = (r, s)$ whose Dynkin labels satisfy $r + s < n$. For what follows, it is convenient to introduce a third label $t = n - r - s$, which can be interpreted as the zeroth label corresponding to the extra affine fundamental weight [9], and define the alcôve as the set of triplets (or affine weights)

$$B_n = \{p = (r, s, t) : r, s, t \geq 1 \text{ and } r + s + t = n\}. \tag{2.3}$$

B_n consists of the portion of the $su(3)$ weight lattice that lies in the interior of the region delimited by the three lines (affine walls) $\alpha_1 \cdot p = \alpha_2 \cdot p = \psi \cdot p - n = 0$ (α_i's are the two simple roots and ψ is the highest root). Equivalently, B_n is a fundamental domain for the action of the affine Weyl group $\widehat{W}_n$ on elements of the weight lattice with a trivial little group. Its cardinality is $\frac{1}{2}(n-1)(n-2)$.

In addition to being graded by a Cartan subalgebra of $su(3)$, which is the reason why we could label the affine representations (and all their states) by weights, all modules $\mathcal{R}_p$ are graded by L_0. On $\mathcal{R}_p$, the spectrum of L_0 is equal to $h_p + \mathbb{N}$, with h_p given by ($\rho = \frac{1}{2}\sum_{\alpha>0}\alpha$)

$$h_p = h_{(r,s)} = \frac{p^2}{2n} - \frac{\rho^2}{2n} = \frac{r^2 + rs + s^2}{3n} - \frac{1}{n}. \tag{2.4}$$

It follows that $h_p > 0$ for all p except $p = (1, 1)$ for which $h_{(1,1)} = 0$. The vacuum of the theory, which is annihilated by L_0 due to the global conformal symmetry, necessarily belongs to the $\mathcal{A}$-module $\mathcal{R}_{(1,1)} \otimes \mathcal{R}_{(1,1)}$. Its uniqueness then implies that we should impose $N_{(1,1),(1,1)} = 1$.

In complete analogy with the finite-dimensional Lie algebras, one defines the character χ_p of the representation $\mathcal{R}_p$ as the function

$$\chi_p(q, M) = \mathrm{Tr}_{\mathcal{R}_p}(q^{L_0 - c_k/24} M) = q^{h_p - c_k/24} \sum_{m=0}^{\infty} \mathrm{Tr}_m(M) q^m, \quad |q| < 1. \tag{2.5}$$

The notation Tr_m means that one traces over the subspace of $\mathcal{R}_p$ where $L_0 = h_p + m$. In (2.5), M is a function which takes its values in the Cartan subalgebra. A traditional choice is $M = \exp(\mathrm{i} \sum_j z_j H_j)$, in which case one can show that, as functions of q and z_j, the χ_p are linearly independent as p runs over B_n.

We will exclusively use the specialized (or restricted) characters $\chi_p(q) \equiv \chi_p(q, I)$. They can be very explicitly computed from the Weyl–Kac formula [9]. If we denote the coroot lattice by $\tilde{R}$, the formula yields in the case of $su(3)$:

$$\chi_{(r,s,t)}(q) = [\eta(q)]^{-8} \sum_{(a,b)=(r,s)+n\tilde{R}} \tfrac{1}{2} ab(a+b)\, q^{(a^2+ab+b^2)/3n}, \tag{2.6}$$

where $\eta(q) = q^{1/24} \prod_{m \geq 1}(1 - q^m)$ is the Dedekind function. Note that the charge conjugation $C(r, s) = (s, r)$ stabilizes B_n, and also leaves the specialized characters invariant: $\chi_p = \chi_{Cp}$. In the case of $su(3)$ and for fixed n, there is no other linear relation among the specialized characters, but, as we will show in Section 5, any two of them are algebraically related (they satisfy a polynomial equation with coefficients in $\mathbb{Q}$). However there are linear relations among characters corresponding to different values of n, as we now show.

Let us define the functions $\mathcal{F}^{[n]}_{(r,s,t)}(q) \equiv [\eta(q)]^8 \chi_{(r,s,t)}$ as the numerators of the characters. We added an extra superscript n to stress the height dependence. Let $\widehat{W}_n$ be the affine Weyl group corresponding to height n, that is, $\widehat{W}_n$ is the semi-direct product of the finite Weyl group (the symmetric group S_3 for $su(3)$) by the group $n\tilde{R}$ of translations by n-multiples of coroots. Let $\varepsilon(w)$ be the parity of a Weyl transformation. Then for all integers j in $\mathbb{N}^*$ and all p in B_n, we claim that the following relations hold:

$$\mathcal{F}^{[n]}_p(q) = \sum_{\substack{w \in \widehat{W}_n \\ w(p) \in B_{jn}}} \varepsilon(w)\, \mathcal{F}^{[jn]}_{w(p)}(q^j). \tag{2.7}$$

The proof is easy. First of all, formula (2.6) allows to extend the functions χ_p to the whole weight lattice, but one may check that $\chi_{p+n\tilde{R}} = \chi_p$ and $\chi_{w(p)} = \varepsilon(w)\chi_p$ for any (finite) Weyl transformation. In particular, if p lies on a boundary of B_n, one has $\chi_p(q) = 0$ identically. Obviously, the functions $\mathcal{F}^{[n]}_p$ have the same properties. The sum over $(a, b) - (r, s) \in n\tilde{R}$ can be split into a sum over the classes $\{n\tilde{r} + nj\tilde{R}\}$ for $\tilde{r} \in \tilde{R}/j\tilde{R}$, from which it follows that

$$\mathcal{F}^{[n]}_p(q) = \sum_{\tilde{r} \in \tilde{R}/j\tilde{R}} \mathcal{F}^{[jn]}_{p+n\tilde{r}}(q^j) = \sum_{\tilde{r} \in \tilde{R}/j\tilde{R}} \varepsilon(w_{\tilde{r}})\, \mathcal{F}^{[jn]}_{w_{\tilde{r}}(p+n\tilde{r})}(q^j). \tag{2.8}$$

The last equality is proved by observing that, although $p + n\tilde{r}$ is not in B_{jn}, there exists a Weyl transformation $w_{\tilde{r}}$ in $\widehat{W}_{jn}$ such that $w_{\tilde{r}}(p + n\tilde{r})$ is in B_{jn}. Since $\widehat{W}_{jn} \subset \widehat{W}_n$, the j^2 weights $w_{\tilde{r}}(p + n\tilde{r})$ are images of p under affine Weyl transformations of $\widehat{W}_n$. Conversely, the intersection $\widehat{W}_n(p) \cap B_{jn}$ is precisely equal to these weights, and formula (2.7) follows.

Another straightforward consequence of (2.6) is the identity

$$\mathcal{F}_{jp}^{[jn]}(q) = j^3\, \mathcal{F}_p^{[n]}(q^j). \tag{2.9}$$

Combined with (2.7), it leads to an identity for the characters

$$\chi_p^{[n]}(q) = \frac{1}{j^3} \sum_{\substack{w\in\widehat{W}_n \\ w(p)\in B_{jn}}} \varepsilon(w)\chi_{jw(p)}^{[j^2n]}(q) \quad \forall j \in \mathbb{N}^*. \tag{2.10}$$

These formulas, written here for $su(3)$, have a strict analog in more general algebras, and constitute the generalization of relations that have appeared in [1] in the case of $su(2)$.

As illustration, we write the relations for $j = 2$ and $j = 3$ in the case of $su(3)$:

$$8\chi_{(r,s)}^{[n]} = \chi_{(2r,2s)}^{[4n]} + \chi_{(2s+2n,2t)}^{[4n]} + \chi_{(2t,2r+2n)}^{[4n]} - \chi_{(2n-2s,2n-2r)}^{[4n]}, \tag{2.11}$$

$$\begin{aligned} 27\chi_{(r,s)}^{[n]} = {}& \chi_{(3r,3s)}^{[9n]} + \chi_{(3s+3n,3t)}^{[9n]} + \chi_{(3t,3r+3n)}^{[9n]} + \chi_{(3r+3n,3s+3n)}^{[9n]} + \chi_{(3s,3t+6n)}^{[9n]} \\ & + \chi_{(3t+6n,3r)}^{[9n]} - \chi_{(3n-3s,3n-3r)}^{[9n]} - \chi_{(3n-3r,6n-3t)}^{[9n]} - \chi_{(6n-3t,3n-3s)}^{[9n]}. \end{aligned} \tag{2.12}$$

Setting $n = 3$ and using $\chi_{(1,1)}^{[3]} = 1$, one obtains linear relations between affine characters and the constant function. It is amusing to note that the above relation for $j = 2$ and $n = 3$ is precisely the one Moore and Seiberg used to discover the exceptional $su(3)$ modular invariant at height $k + 3 = 12$ [14], namely

$$\chi_{(2,2,8)} + \chi_{(2,8,2)} + \chi_{(8,2,2)} - \chi_{(4,4,4)} = 8. \tag{2.13}$$

2.2. *Modular invariance*

Besides their group theoretical importance, the characters are intimately related to the partition function of physical models on Riemann surfaces. The simplest and by now classical case, namely tori, has been first considered in [15]. There it was shown that the partition function of a rational conformal field theory put on a torus $\mathbb{C}/\mathbb{Z} + \tau\mathbb{Z}$ of modulus τ, has the general form

$$Z(\tau) = \mathrm{Tr}_{\mathcal{H}}(q^{L_0-c/24} \otimes \overline{q}^{\overline{L}_0-c/24}), \tag{2.14}$$

where the complex number q is related to the modulus of the torus by $q = \mathrm{e}^{2\mathrm{i}\pi\tau}$. The trace is taken over the Hilbert space of the model, and $\overline{q}$ is the complex conjugate of q. In virtue of the decomposition (2.2) – it is completely general, just insert the representations of whatever the symmetry algebra $\mathcal{A}$ is – one obtains

$$Z(\tau) = \sum_{p,p'} N_{p,p'}\, \chi_p(q)\, \chi_{p'}(\overline{q}). \tag{2.15}$$

The problem of modular invariance stems from the fact that the same torus may be given in terms of a whole class of moduli, namely all τ related by $PSL_2(\mathbb{Z})$ transformations, also known as modular transformations, in fact specify a single torus. Which representative one chooses in this class should not affect the physical partition function, and as a consequence, it must be modular invariant, $Z(\tau) = Z((a\tau+b)/(c\tau+d))$. It is actually sufficient to check the invariance of the partition function under $S : \tau \to -1/\tau$ and $T : \tau \to \tau+1$, since together they generate the whole of $PSL_2(\mathbb{Z}) = \langle S, T \mid S^2, (ST)^3\rangle$. This is what the modular invariance (on the torus) requires: to check that the partition function satisfies

$$Z(\tau) = Z(\tau+1) = Z\left(\frac{-1}{\tau}\right). \tag{2.16}$$

But in fact this argument can be turned around. Since the partition function must have the general form (2.15), the modular invariance constrains the choice of the integers $N_{p,p'}$, and hence the model itself. This is how the criterion of modular invariance led to the possibility of classifying the consistent (candidates of) conformal theories. It turns out that the modular invariance is a fantastically strong constraint, as very few choices of integers $N_{p,p'}$ lead to modular invariant partition functions. In the first case for which the classification has been carried out, namely $\mathcal{A} = \widehat{su(2)}_k \otimes_I \widehat{su(2)}_k$, unexpected connections emerged with other mathematical areas. Indeed the results showed that the list of $su(2)$ modular invariants is isomorphic to the list of simply laced simple complex Lie algebras ADE (or equivalently to the list of finite subgroups of $SO(3)$) [1]. This surprising correspondence has remained largely mysterious (see [16] however), but prompted further investigations. As far as affine Lie algebras are concerned, the next case is $\widehat{su(3)}$. Here too the complete list is known for all levels [2], but it shows no obvious pattern. An attempt to link the structure of modular invariants (for $su(3)$ and more general cases) to graphs has been made in [17]. Based on technical similarities, another connection was suggested in [4], which relates the affine $su(3)$ modular problem to the geometry of the complex Fermat curves. This connection is precisely the problem we want to address in this article.

It would probably be inspiring to see the solution to the modular problem for higher rank affine simple Lie algebras, but no complete list is known beyond rank 2. Partial results for affine algebras include: all simple algebras at level 1 [3], all $su(N)$ algebras at level 2 and 3 [18], products of $su(2)$ factors with the restriction $\gcd(k_i+2, k_j+2) \le 3$ (except for a product of two factors for which the classification is complete) [19]. Other approaches to the classification problem have produced complete lists of modular invariants of specific types [19–21].

One may check the modular invariance of $Z(\tau)$ by looking at the way the affine characters transform [9]. From the general form (2.5) of the characters, the transformation under T is easy to compute, while that under S can be obtained from the Poisson formula. The results show that the characters χ_p, for $p \in B_n$, transform linearly under a modular transformation, $\chi_p(X\tau) = \sum_{p'} X_{p',p}\, \chi_{p'}(\tau)$ for X in $PSL_2(\mathbb{Z})$. For $su(3)$ the explicit matrices representing T and S read

$$T_{p',p} = \mathrm{e}^{2i\pi(h_p - c_k/24)}\, \delta_{p,p'} = \xi^{r^2+s^2+rs-n}\, \delta_{p,p'}, \tag{2.17}$$

$$S_{p',p} = \frac{-\mathrm{i}}{n\sqrt{3}} \sum_{w\in W} \varepsilon(w) \mathrm{e}^{-2\mathrm{i}\pi p\cdot w(p')/n}$$
$$= \frac{-\mathrm{i}}{n\sqrt{3}} \xi^{-(2rr'+2ss'+rs'+r's)}(1+\zeta^{tt'-rs'}+\zeta^{tt'-r's}-\zeta^{rr'}-\zeta^{ss'}-\zeta^{tt'}) \tag{2.18}$$

with $\xi = \mathrm{e}^{2\mathrm{i}\pi/3n}$ and $\zeta = \xi^3$. The two matrices are symmetric and unitary, and satisfy $S^2 = (ST)^3 = C$ with C the charge conjugation, so that S and T generate a representation of $SL_2(\mathbb{Z})$ rather than $PSL_2(\mathbb{Z})$. It has been proved in [9,22] that the kernel of this representation is of finite index in $SL_2(\mathbb{Z})$, for any value of n, and is even contained in some principal congruence subgroup, but a precise description of these kernels is still lacking. An obvious relation is $T^{3n} = 1$, and it is not difficult to see that no smaller power of T equals 1 (except for $n = 3$). One can also show that for $n \geq 5$, no power T^a for $a < 3n$ has all its eigenvalues equal because this would mean that $a(3-n)$, $a(7-n)$, $a(12-n)$ are equal modulo $3n$, which implies that $3n$ divides a. On the other hand, T^3 is central for $n = 4$.

Inserting the modular transformations of the characters into the partition function, one finds that $Z(\tau)$ is modular invariant iff the matrix $N_{p,p'}$ satisfies $TNT^\dagger = SNS^\dagger = N$, or, by using the unitarity of S and T, iff N is in the commutant of the representation of $PSL_2(\mathbb{Z})$ carried by the characters [3]

$$Z(\tau) \text{ modular invariant} \iff [N,T] = [N,S] = 0. \tag{2.19}$$

The commutant of S and T, without imposing the positivity condition $N_{p,p'} \geq 0$, has been worked out in full generality for the affine Lie algebras of the $su(N)$ series [22], but the results extend trivially to all algebras. It was found that the commutant over $\mathbb{C}$ actually has a basis of matrices with coefficients in $\mathbb{Q}$, and also that this commutant is rather big. Its dimension is an arithmetic function, growing roughly like $n^{2N-5}/N!$ for $su(N)$ at level $k = n - N$ [23]. In view of the fact that very few modular invariant partition functions satisfy it, it shows that the positivity condition is really the crucial one, and also the most difficult to handle. Recent developments have shown that the most efficient way of dealing simultaneously with the commutation and with the positivity conditions is to use Galois theory techniques, which beautifully combine the algebraic nature of S with the rational character of $N_{p,p'}$. Before we review these aspects in the next section, we mention another feature of the modular matrices S and T.

When n is coprime with 3, S and T have a property which is useful in actual calculations, namely they can be written as tensor products. From the above formulas, one may check that under the cyclic rotation $\mu(r,s,t) = (t,r,s)$, an automorphism of the extended Dynkin diagram of $su(3)$, one has, for $\omega = \mathrm{e}^{2\mathrm{i}\pi/3}$

$$T_{\mu(p),\mu(p)} = \omega^{n-r-2s}\, T_{p,p}, \qquad S_{p,\mu(p')} = \omega^{r+2s}\, S_{p,p'}. \tag{2.20}$$

[3] The partition function is given in terms of the specialized characters, on which the charge conjugation C is trivial.

The quantity $r + 2s$ taken modulo 3 is the triality of p. When n and 3 are coprime, μ acts on the weights of B_n without fixed points. Thus if one splits B_n into orbits under the action of μ by writing $p = \mu^k(r)$ for $k = 0, 1, 2$ and $r \in B_n/\langle\mu\rangle$ of zero triality, one obtains

$$T_{\mu^k(r),\mu^{k'}(r')} = (\omega^{k^2 n}\delta_{k,k'})\, T_{r,r'}, \qquad S_{\mu^k(r),\mu^{k'}(r')} = \omega^{nkk'}\, S_{r,r'}. \tag{2.21}$$

The same property holds in $su(N)$, level k, whenever N and $n = N + k$ are coprime.

2.3. Galois and parity selection rules

Perhaps the most remarkable property of the modular matrices S and T is that they are rational combinations of roots of unity, in this case $3n$-roots of unity [24]. Even more remarkable is the fact that this situation is completely general: any RCFT has matrices S and T that have their coefficients in cyclotomic extensions of finite degree over $\mathbb{Q}$. For T, it follows from the fact that in a RCFT, the Virasoro central charge c and all conformal weights are rational numbers [25]. The corresponding result for S has been proved in [5], whose authors built on results from [26].

Let us first fix our notations concerning cyclotomic extensions. For $\zeta_m = e^{2i\pi/m}$, we will denote by $\mathbb{Q}(\zeta_m)$ the cyclotomic extension of the rationals by m-roots of unity, of degree $\varphi(m)$, the Euler totient function, over $\mathbb{Q}$. Its Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ consists of the automorphisms $\sigma_h(\zeta_m) = \zeta_m^h$ for all integers h between 1 and m, coprime with m. The Galois group is Abelian, isomorphic to $\mathbb{Z}_m^* = (\mathbb{Z}/m\mathbb{Z})^*$, the group of invertible integers modulo m.

The Galois automorphisms of the algebraic extension where the coefficients of S lie, have important consequences for the modular problem, which we now summarize. Each element of the Abelian Galois group of the relevant extension induces the unique permutation of the weights of the alcôve $\sigma : p \to \sigma(p)$ (we keep the same name for the element of the Galois group and for the induced permutation), such that

$$\sigma(S_{p,p'}) = \varepsilon_\sigma(p) S_{\sigma(p),p'} = \varepsilon_\sigma(p') S_{p,\sigma(p')}, \tag{2.22}$$

where $\varepsilon_\sigma(p) = \pm 1$ is a cocycle satisfying $\varepsilon_{\sigma\sigma'}(p) = \varepsilon_\sigma(p)\varepsilon_{\sigma'}(\sigma(p))$. Acting with σ on the commutation relation $[N, S] = 0$ and using the fact that the coefficients $N_{p,p'}$ are rational numbers, one obtains that N must satisfy [5]:

$$N_{\sigma(p),\sigma(p')} = \varepsilon_\sigma(p)\varepsilon_\sigma(p')\, N_{p,p'}, \quad \text{for all } \sigma. \tag{2.23}$$

This equation is a necessary condition for N to commute with S. Its importance for the modular problem is obvious. Since the entries of N are to be non-negative integers, it leads to the selection rule:

$$N_{p,p'} = 0 \text{ as soon as there is a } \sigma \text{ for which } \varepsilon_\sigma(p)\varepsilon_\sigma(p') = -1. \tag{2.24}$$

Its utility is two-fold. First, it turns out to be extremely restrictive, forcing most of the coefficients to vanish. Even though in actual cases, it may not be easy to determine which coefficients may or may not vanish, it still remains much easier than the commutation problem. Second, it facilitates enormously computer searches, because in the examples we know, which include all affine algebras, to check the sign of $\varepsilon_\sigma(p)\varepsilon_\sigma(p')$ is computationally trivial. The first use of (2.24) was made in the restricted context of $su(3)$, n prime [27], where, however, neither its generality nor its Galoisian origin were recognized. They were later generalized to all affine algebras in [3,4], and eventually to all RCFT in [5] where the Galoisian nature of the result was transparently brought out.

From formula (2.18) for the matrix S, in which one may neglect the prefactor $-\mathrm{i}/n\sqrt{3}$ since one is interested in commuting N with S, the action of the Galois automorphism σ_h amounts formally to multiply the weight p (or p') by h: $\sigma_h(S_{p,p'}) = S_{hp,p'}$. This action of σ_h is only formal since in general hp is not in the alcôve B_n. However one can show that h being invertible modulo n ensures there is a unique affine Weyl transformation which maps hp on some weight $\sigma_h(p)$ of B_n, so we can write

$$\sigma_h(p) = w_{h,p}(hp) + n\alpha, \quad w \in W, \ \alpha \in \tilde{R}. \tag{2.25}$$

One then obtains from (2.18)

$$\sigma_h(n\sqrt{-3}S_{p,p'}) = \sum_{w\in W} \varepsilon(w)\mathrm{e}^{-2\mathrm{i}\pi\sigma_h(p)\cdot(w_{h,p}\circ w)(p')/n} = \varepsilon(w_{h,p})\,(n\sqrt{-3}S_{\sigma_h(p),p'}). \tag{2.26}$$

Therefore the permutation of B_n induced by an element of the Galois group is given in (2.25), and the cocycle is just the parity of the Weyl transformation defining the permutation, $\varepsilon_{\sigma_h}(p) = \varepsilon(w_{h,p})$, up to the sign $\sigma_h(\sqrt{-3})/\sqrt{-3}$, that only depends on h. The same is true of any affine algebra. For that reason, the cocycles have been termed "parities" in the literature.

We finish this section by showing how the parities can be computed in the case of $su(3)$. The general algorithm for computing both $\sigma_h(p)$ and $\varepsilon_{\sigma_h}(p)$ in the $su(N)$ series has been given in [4]. The sign $\varepsilon_{\sigma_h}(p) = \pm 1$ is the signature of the Weyl transformation which maps the weight hp back in the alcôve. By extension, one can assign all weights a parity $\varepsilon(p)$, which is just the signature of the Weyl transformation which maps p back in the alcôve. It is well defined only for those weights which do not lie on the affine walls, since they would be fixed points of odd Weyl transformations. For $su(3)$ it means that the parity of $p = (r, s, t)$ is well defined iff $r, s, t \neq 0 \bmod n$. If p is in a wall, we set $\varepsilon(p) = 0$. We have $\varepsilon(p) = +1$ for all p in B_n. A translation by $n\alpha$, α a coroot, being even, the parity does not change under such translations, $\varepsilon(p + n\alpha) = \varepsilon(p)$, so that we may restrict our attention to the six triangles obtained from B_n by the action of the finite Weyl group. Up to translations by elements of $n\tilde{R}$, the even Weyl transformations map B_n onto

$$B_n = \{(r, s): r, s \geq 1,\ r + s \leq n - 1\}, \tag{2.27}$$

$$w_1 w_2(B_n) + n(\alpha_1 + \alpha_2) = \{(n + s, n - r - s)\}, \tag{2.28}$$

$$w_2 w_1(B_n) + n(\alpha_1 + \alpha_2) = \{(n - r - s, n + r)\}. \tag{2.29}$$

We note that if p is in B_n, then $p + (n, 0)$ and $p + (0, n)$ are, respectively, in the second and third triangle, so we conclude that the parity of $p = (r, s)$ depends only on the residue

$(\langle r\rangle, \langle s\rangle)$ modulo n of p. From the above discussion, $\langle r\rangle$, $\langle s\rangle$ and $\langle r+s\rangle$ are all different from zero modulo n for any weight which is not in an affine wall. If we take the residues $\langle\cdot\rangle$ in $[0, n-1]$, two possibilities remain. Either $\langle r\rangle + \langle s\rangle < n$, in which case the parity $\varepsilon(p) = +1$ since the weights in B_n satisfy this inequality, or else $\langle r\rangle + \langle s\rangle > n$ and $\varepsilon(p) = -1$. In the first case, $\langle t\rangle = \langle n-r-s\rangle = n - \langle r\rangle - \langle s\rangle$, while in the second case, $\langle t\rangle = 2n - \langle r\rangle - \langle s\rangle$. Putting all together, one obtains the parity function

$$\varepsilon(p) = \varepsilon(r,s,t) = \begin{cases} 0 & \text{if } \langle r\rangle = 0 \text{ or } \langle s\rangle = 0 \text{ or } \langle t\rangle = 0, \\ +1 & \text{if } \langle r\rangle + \langle s\rangle + \langle t\rangle = n, \\ -1 & \text{if } \langle r\rangle + \langle s\rangle + \langle t\rangle = 2n. \end{cases} \tag{2.30}$$

Let us summarize the $su(3)$ parity selection rules. With each Galois automorphism σ_h is associated an integer h, coprime with $3n$. Given a weight p in the alcôve B_n, we compute for each h the parity $\varepsilon(hp)$ from formula (2.30). The parity depends only on the residue of hp modulo n, so we may take h between 1 and n. In this way, we obtain a finite sequence $\{\varepsilon(hp) = \pm 1\}_h$. The parity selection rules then say that the coefficient $N_{p,p'}$ in the modular invariant partition function may be non-zero only if the two sequences $\{\varepsilon(hp)\}_h$ and $\{\varepsilon(hp')\}_h$ are equal, componentwise. Equivalently, if we collect the h's for which $\varepsilon(hp) = +1$ by defining

$$H_p = H_{r,s,t} = \{h \in \mathbb{Z}_n^*: \langle hr\rangle + \langle hs\rangle + \langle ht\rangle = n\}, \tag{2.31}$$

the selection rules imply

$$H_p \neq H_{p'} \quad \Longrightarrow \quad N_{p,p'} = 0. \tag{2.32}$$

In this form, the parity condition appears in a completely different context, namely the study of the complex Fermat curves, of which it governs the decomposition.

3. Fermat curves

The parity rule is extremely powerful for the problem of modular invariance. It is a sufficient condition for N, the matrix specifying a modular invariant, to commute with S, and is not concerned at all with the commutation with T. Hence fulfilling the parity rule does not involve the full complexity of finding the commutant of S (let alone of S and T), but at the same time is constraining enough to encapsulate much of the structure of the commutant. On the practical side, this makes it a prime tool, as witnessed by the latest developments [18,28,29], while conceptually, its Galoisian origin and its universality [5] also yielded a renewed viewpoint.

As noted in [4], the parity rule for $\widehat{su(3)}$ is very peculiar as it has also a key role in the understanding of the geometry of the Fermat curves, and more specifically, in the decomposition of the Jacobian of the Fermat curves into simple factors [6]. There is no apparent reason for this, and whether this relationship is deep or accidental was the original motivation for our investigations. There is no indication a priori why the Fermat curves should have anything to do with the partition functions of $\widehat{su(3)}$ CFTs on tori (other curves have, as we shall see in the Section 5). It is the purpose of this section to merely describe the connection. We follow the original or standard material available in the mathematics literature with a presentation which has no claim to rigor and is directed towards the application at hand. We refer to the original articles for further (and perhaps more accurate) details.

3.1. Abelian varieties

A complex Abelian variety of dimension g is a complex torus $\mathbb{C}^g/L$ equipped with a Riemann form [30]. L is a lattice (a discrete free Abelian group of rank $2g$ over $\mathbb{Z}$), and the existence of a Riemann form means that there is a positive definite Hermitian form on $\mathbb{C}^g$, of which the imaginary part takes integral values on L. A prime example, though not generic, of an Abelian variety is the Jacobian of a Riemann surface. As this example is most relevant to us, we will describe it in more detail.

If Σ is a compact Riemann surface of genus g, it is well known that the homology group of Σ has $2g$ independent cycles γ_i, and that the vector space of holomorphic 1-forms has dimension equal to g. A period of Σ is the g-tuple $(\oint_\gamma \omega_1, \ldots, \oint_\gamma \omega_g)$ for some cycle γ, where the ω_i form a basis for the holomorphic differentials. The period lattice is the collection of all periods

$$L(\Sigma) = \left\{ \left(\oint_\gamma \omega_1, \oint_\gamma \omega_2, \ldots, \oint_\gamma \omega_g \right) : \gamma = \sum_i n_i \gamma_i \in H_1(\Sigma, \mathbb{Z}) \right\} \subset \mathbb{C}^g. \tag{3.1}$$

For any fixed point P_0 on the surface, it follows that the map (called the Abel–Jacobi map)

$$P \in \Sigma \quad \longmapsto \quad J(P) = \left(\int_{P_0}^{P} \omega_1, \int_{P_0}^{P} \omega_2, \ldots, \int_{P_0}^{P} \omega_g \right) \tag{3.2}$$

is well defined modulo the periods (i.e. does not depend on the path from P_0 to P), and provides an embedding of the surface into the factor group $\mathrm{Jac}(\Sigma) = \mathbb{C}^g/L(\Sigma)$, the Jacobian of Σ. Clearly, for $g > 1$, the map $J(P)$ is only an embedding, but if we extend the map J to J_g by setting

$$\boldsymbol{P} = (P_1, P_2, \ldots, P_g) \quad \longmapsto \quad J_g(\boldsymbol{P}) = J(P_1) + J(P_2) + \cdots + J(P_g) \in \mathrm{Jac}(\Sigma), \tag{3.3}$$

then a fundamental result of Riemann, anticipated and proved in specific cases by Jacobi, asserts that the map J_g is invertible for "generic" points $\boldsymbol{P}$ in the gth symmetric power of Σ, $\mathrm{Sym}_g\, \Sigma = \Sigma^g/S_g$ (S_g is the permutation group on g letters). Torelli theorem then shows that the isomorphism class of the Jacobian in fact determines that of the Riemann surface. Thus the Jacobian captures the essential features of the surface, and, being an affine space, provides a kind of linearization of it. Taking advantage of that, attention is sometimes focussed on the Jacobians rather than on the surfaces themselves. For elliptic curves ($g = 1$), this is what one is used to, as the curve is isomorphic to its Jacobian, usually described as a parallelogram with sides 1 and τ.

An important notion in the study of Abelian varieties is that of isogeny [31,32]. A map $\phi : A \to B$ is an isogeny if it is a surjective homomorphism with finite kernel. Isogenies go both ways: if ϕ is an isogeny from A to B, there exists another one $\hat{\phi}$ from B to A. When there are isogenies between them, we say that A and B are isogenous and write $A \sim B$ (if A and B are Jacobians of algebraic curves, we say by extension that the two curves are isogenous). Being isogenous is an equivalence relation. For what follows, it may be convenient to rephrase these properties in terms of lattices. If we view Abelian varieties as complex tori, say $A = \mathbb{C}^g/L_A$ and $B = \mathbb{C}^g/L_B$, an equivalent definition is that A is isogenous to B if and only if there is a complex linear map ψ such that $\psi(L_A) \subset L_B$ with finite index, say m. If this is the case, one has $mL_B \subset L_A$, which explicitly displays an isogeny from B to A, and shows that isogenies define an equivalence relation (reflexivity and transitivity are trivial). We then say that the lattices are isogenous, $L_A \sim L_B$. For instance, in the elliptic case for which the complex lattice L can be written $L(\tau) = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\}$ with $\tau = \omega_2/\omega_1 \notin \mathbb{R}$, two lattices $L(\tau) \sim L(\tau')$ are isogenous if and only if

$$\tau' = \frac{a\tau + b}{c\tau + d} \quad \text{for some} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ in } GL_2(\mathbb{Q}).$$

The following results show the importance of isogenies. It may happen that an Abelian variety A contains a non-trivial Abelian subvariety A_1. If $A = \mathbb{C}^g/L_A$, it means that there is a complex vector space $V_1 = \mathbb{C}^h \subset \mathbb{C}^g$ such that $V_1 \cap L_A \equiv L_{A_1}$ is a lattice in V_1 (of rank $2h$). Then the orthocomplement of V_1 with respect to the Riemann form, call it V_2, has the same property: $V_2 \cap L_A \equiv L_{A_2}$ is a lattice in V_2 (of rank $2g - 2h$). Hence $L_{A_1} \oplus L_{A_2}$ is of finite index in L_A, and A is isogenous to $V_1/L_{A_1} \times V_2/L_{A_2} \equiv A_1 \times A_2$. Moreover, the Riemann form on A induces by restriction a Riemann form on A_1 and A_2, so that they are themselves Abelian varieties. (Note that A being a Jacobian does not imply that A_1 and A_2 are Jacobians.) Repeating this decomposition process as many times as possible, one eventually finds that an Abelian variety is isogenous to the product of simple Abelian varieties, where simple means that they contain no proper complex torus. This is the complete reducibility theorem [31,32], due to Poincaré. Moreover this decomposition is unique up to isogenies.

Decomposing into simple factors the Jacobians of the Fermat curves, defined in affine coordinates by

$$F_n : x^n + y^n = 1, \quad n \text{ integer} \tag{3.4}$$

was precisely the purpose of, first, Koblitz and Rohrlich [6], who partially resolved it, and then of Aoki [33]. We are now in a position to detail their work, and the relation to the problem of modular invariance for $su(3)$.

3.2. Jacobians

The periods of the Fermat curves have been computed by Rohrlich [34]. A basis for the holomorphic differentials on F_n is obtained by taking $\omega_{r,s,t} = \alpha_{r,s,t}\, x^{r-1} y^{s-n}\, dx$, for all admissible triplets (r, s, t), i.e. those such that $0 < r, s, t < n$ and $r + s + t = n$ (see also Section 4.2). Its dimension equals the genus of F_n, namely $\frac{1}{2}(n-1)(n-2)$. This is also the cardinality of the fundamental alcôve for $\widehat{su(3)}$, height n. A suitable choice for the normalization constants $\alpha_{r,s,t}$ yields the following result for the integration of the differentials along closed curves:

$$\oint_{\gamma_{i,j}} \omega_{r,s,t} = \zeta_n^{ri+sj}, \qquad 1 \le i, j \le n, \tag{3.5}$$

where $\{\gamma_{i,j}\}_{1\le i,j\le n}$ is a generating set of closed loops [34]. Every cycle in $H_1(F_n, \mathbb{Z})$ can be written $\gamma = \sum_{i,j} m_{i,j}\,\gamma_{i,j}$, so the period lattice of the nth Fermat curve is

$$L(F_n) = \left\{ \left(\ldots, \sum_{i,j} m_{i,j}\, \zeta_n^{ri+sj}, \ldots \right)_{0<r,s,t<n} : m_{i,j} \in \mathbb{Z} \right\}. \tag{3.6}$$

When all $m_{i,j}$ are varied over $\mathbb{Z}$, it is clear that the (r,s,t)th component of the period lattice covers the whole of $\mathbb{Z}(\zeta_{n_0})$, for n_0 defined by $\gcd(r,s,t) = n/n_0$. If however two triplets are related by $(r',s',t') = (\langle hr\rangle, \langle hs\rangle, \langle ht\rangle)$ for some $h \in \mathbb{Z}^*_{n_0}$, the (r',s',t')th component of $L(F_n)$ is just the Galois transform by σ_h of the (r,s,t)th component, so that the two are not independent. The triplet $(\langle hr\rangle, \langle hs\rangle, \langle ht\rangle)$ is admissible if h is in the set [4]

$$H_{r,s,t} = \{h \in \mathbb{Z}^*_{n_0} : \langle hr\rangle + \langle hs\rangle + \langle ht\rangle = n\}. \tag{3.7}$$

We saw in Section 2 that $H_{r,s,t}$ was crucial for the $su(3)$ parity rule, and in fact we shall see that it also governs the decomposition of the Jacobian of the Fermat curves. For the moment we note that $h \in H_{r,s,t}$ is equivalent to $-h \notin H_{r,s,t}$, so $H_{r,s,t}$ is a set of representatives of $\mathbb{Z}^*_{n_0}/\{\pm 1\}$.

If $\{e_{r,s,t}: \text{admiss.}\ (r,s,t)\}$ is the canonical basis of $\mathbb{C}^g$, a simple reordering leads to the following writing:

$$\mathbb{C}^g = \bigoplus_{\text{admiss.}\,(r,s,t)} \mathbb{C}\, e_{r,s,t} = \bigoplus_{[r,s,t]} \bigoplus_{h\in H_{r,s,t}} \mathbb{C}\, e_{\langle hr\rangle,\langle hs\rangle,\langle ht\rangle}, \tag{3.8}$$

where $[r,s,t]$ is the class $\{(\langle hr\rangle, \langle hs\rangle, \langle ht\rangle) : h \in H_{r,s,t}\}$. Using the same reordering on the period lattice, one easily sees that

$$L(F_n) \subset \bigoplus_{[r,s,t]} L_{r,s,t}, \tag{3.9}$$

where

$$L_{r,s,t} = \{(\ldots, \sigma_h(z), \ldots)_{h\in H_{r,s,t}} : z \in \mathbb{Z}(\zeta_{n_0})\}. \tag{3.10}$$

Note that the right-hand side of (3.9) is well defined because $L_{r,s,t} = L_{r',s',t'}$ if the two triplets belong to the same class $[r,s,t]$ (a consequence of $H_{\langle hr\rangle,\langle hs\rangle,\langle ht\rangle} = h^{-1} H_{r,s,t}$). The inclusion (3.9) holds with finite index, since both lattices have the same rank over $\mathbb{Z}$,

$$(n-1)(n-2) = \sum_{[r,s,t]\in B_n} \varphi(n_0). \tag{3.11}$$

[4] If $n_0 < n$, the set defined in (2.31) is the trivial extension modulo n of the set defined here.

Consequently the period lattice $L(F_n)$ is isogenous to the direct sum $\oplus L_{r,s,t}$, and from this follows the isogeny [34]:

$$\mathrm{Jac}(F_n) = \mathbb{C}^g/L(F_n) \sim \prod_{[r,s,t]} (\mathbb{C}^{\varphi(n_0)/2}/L_{r,s,t}). \tag{3.12}$$

This shows that the (Jacobian of the) curve F_n is far from being simple, but has a number of factors increasing (at least) linearly with n. It is not difficult to compute the number of factors in (3.12). For $n = \prod p^k$, one finds

$$\#\,\text{classes}\ [r,s,t] = \prod_p [\sigma_1(p^k) + \sigma_1(p^{k-1})] - 3\sigma_0(n) + 2, \tag{3.13}$$

where $\sigma_k(n)$ is the sum of the kth powers of all divisors of n (including 1 and n). If n is prime, there are $(n-2)$ classes, which can be chosen as $[1, s, n-1-s]$ for $s = 1, 2, \ldots, n-2$. Other particular values for the number of classes are 1, 3, 10, 12, 34, 88 for $n = 3,\ 4,\ 6,\ 8,\ 12,\ 24$, respectively.

Let us mention that in case n is a prime number, Weil has shown that $L_{r,s,t}$ is in fact the period lattice of the following curve [35]:

$$C_{r,s,t}(n) : v^n = u^r(1-u)^s. \tag{3.14}$$

This is not true in general as the genus of (the irreducible part of) $C_{r,s,t}(n)$, equal to

$$g(C_{r,s,t}(n)) = \tfrac{1}{2}(n_0 - 1) - \tfrac{1}{2}[\gcd(n_0, r) + \gcd(n_0, s) + \gcd(n_0, t) - 3], \tag{3.15}$$

is generically different from $\frac{1}{2}\varphi(n_0)$. What is true for general n is that $C_{r,s,t}(n)$ is the image of F_n under the rational map $(x, y) \mapsto (u, v) = (x^n, x^r y^s)$, so that the Jacobian of $C_{r,s,t}(n)$ is contained in that of F_n [34]. There is also a rational map from F_n to F_d for every divisor d of n (namely the n/dth power map), – implying in particular $\mathrm{Jac}(F_d) \subset \mathrm{Jac}(F_n)$, see e.g. (3.36) below – so altogether there is a sequence of rational maps

$$F_n \longrightarrow \{F_d\} \longrightarrow \{C_{r,s,t}(d)\} \quad \text{for any}\ d|n. \tag{3.16}$$

The curves $C_{r,s,t}(n)$ have been extensively discussed in [7] in the context of rational billiards. There $C_{r,s,t}(n)$ was associated (through a Schwarz transformation) with the rational triangle of angles $r\pi/n, s\pi/n, t\pi/n$. For that reason, we call them triangular curves. We will come back to them in Section 4.3, where we will show that some of the triangular curves which are rational images of F_{24} are intimately related to the exceptional modular invariants of $su(3)$, occurring at $n = 8$, 12 and 24.

3.3. Complex multiplication

The main result of the previous section was the decomposition (3.12) of the Jacobian of F_n. The question that remains is whether this decomposition is complete.

Let $A = \mathbb{C}^n/L$ be an Abelian variety. The endomorphisms of A, denoted by $\mathrm{End}(A)$, are the complex endomorphisms of $\mathbb{C}^n$ fixing the lattice L, and have a ring structure. It is clear that $\mathrm{End}(A)$ contains $\mathbb{Z}$, realized as the multiplication of the elements of A by integers, and that $\mathbb{Z}$ is central in End(A). One may broaden the class of transformations and consider endomorphisms of A up to isogenies, or equivalently endomorphisms of the isogeny class of A, therefore allowing for arbitrary rational factors in the transformations of A into A. This one can do by defining $\mathrm{End}_{\mathbb{Q}}(A) = \mathrm{End}(A) \otimes \mathbb{Q}$, which is then isogeny invariant. One has now that $\mathbb{Q}$ is in the center of $\mathrm{End}_{\mathbb{Q}}(A)$, but it may happen that the center be larger than $\mathbb{Q}$. If this is the case, one can show that it is necessarily a number field F, which is either totally real (all its embeddings in $\mathbb{C}$ lie in $\mathbb{R}$), or else is a totally imaginary quadratic extension of a totally real number field (F has no embedding in $\mathbb{R}$). In the second case, F is called a CM field and A is said to have complex multiplication by F. [5]

If F is a CM field of degree $2n$ over $\mathbb{Q}$, let us denote by σ_i, $1 \le i \le 2n$, the distinct embeddings of F in $\mathbb{C}$. (If F is Galois, the embeddings are related to each other by Galois transformations.) Among the σ_i, let us choose a subset $P_+ = \{\sigma_1, \dots, \sigma_n\}$ such that no two embeddings in P_+ are complex conjugates of each other. Given the pair (F, P_+), called a CM-type, one may define the lattice

$$L(F, P_+) = \{(\sigma_1(z), \dots, \sigma_n(z)) \colon z \in \mathcal{O}_F\} \subset \mathbb{C}^n, \tag{3.17}$$

with $\mathcal{O}_F$ the ring of integers of F, and then consider the complex torus $\mathbb{C}^n/L(F, P_+)$. Its special structure allows to put a Riemann form on it (see [36] for the explicit construction), and so to promote it to an Abelian variety, which, by construction, has complex multiplication by F. Note that P_+ and $P_+\sigma$ lead to the same torus for any embedding σ. Conversely, if A is an Abelian variety of dimension n, such that $\mathrm{End}_{\mathbb{Q}}(A)$ contains F, a CM field of degree $2n$, then A is isogenous to $\mathbb{C}^n/L(F, P_+)$ for some P_+. This shows that the complex multiplication is a very restrictive property, fixing much of the variety.

Complex multiplication also yields a criterion of simplicity for an Abelian variety, known as the Shimura–Taniyama (ST) theorem [37]. Let us assume that $A = \mathbb{C}^n/L(F, P_+)$ is an Abelian variety of CM-type (F, P_+), and that F is Galois over $\mathbb{Q}$ (is a splitting field for any of its defining polynomials). Set

$$W(P_+) = \{\sigma \in \mathrm{Gal}\,(F/\mathbb{Q}) \colon P_+\sigma = P_+\}. \tag{3.18}$$

The ST theorem then states that A is simple if and only if $W(P_+) = \{1\}$ [36,37]. One can moreover prove that if $W(P_+) \neq \{1\}$, A is isogenous to the product of $|W(P_+)|$ isomorphic simple factors, each one having complex multiplication by the subfield of F fixed by $W(P_+)$ (see below).

All these notions and results have a straight application to the case at hand. In the decomposition (3.12) of Jac(F_n), all factors have complex multiplication by $\mathbb{Q}(\zeta_{n_0})$, since the lattice $L_{r,s,t}$ is stabilized by the multiplication by arbitrary elements of $\mathbb{Z}(\zeta_{n_0})$ (note that the cyclotomic extension $\mathbb{Q}(\zeta_{n_0})$ is the imaginary quadratic extension of the totally real field $\mathbb{Q}(\zeta_{n_0} + \bar{\zeta}_{n_0}) = \mathbb{Q}(\cos(2\pi/n_0))$, and is thus a CM field). Observe also that $L_{r,s,t}$ is precisely a lattice arising from a CM-type, namely $(\mathbb{Q}(\zeta_{n_0}), H_{r,s,t})$. Indeed $\mathbb{Q}(\zeta_{n_0})$ has an Abelian Galois group over $\mathbb{Q}$, consisting of the transformations $\sigma_h \colon \zeta \mapsto \zeta^h$ for all $h \in \mathbb{Z}^*_{n_0}$,

[5] Sometimes a more restrictive definition is used, which requires in addition that the degree of F be twice the dimension of A.

and from a previous remark, $H_{r,s,t}$ is a coset of the Galois group by $\{\pm 1\}$, and therefore contains no two h, h' such that $\sigma_h = \overline{\sigma}_{h'} = \sigma_{-h'}$.

Following Koblitz and Rohrlich, one would like to answer two questions:
(i) Are the factors $\mathbb{C}^{\varphi(n_0)/2}/L_{r,s,t}$ simple?
(ii) Are there isogenies between some of them?
We have just observed that the factors $\mathbb{C}^{\varphi(n_0)/2}/L_{r,s,t}$ are Abelian varieties with CM-type $(\mathbb{Q}(\zeta_{n_0}), H_{r,s,t})$, so we can use the ST criterion to solve both problems. Set

$$W_{r,s,t} = \{w \in \mathbb{Z}_{n_0}^*: wH_{r,s,t} = H_{r,s,t}\}. \tag{3.19}$$

From the above general discussion, two factors related to (r, s, t) and (r', s', t') will be isogenous if and only if they have the same CM-type up to a Galois automorphism, i.e.

$$L_{r,s,t} \sim L_{r',s',t'} \quad \Longleftrightarrow \quad \begin{cases} \mathbb{Z}_{n_0}^* \sim \mathbb{Z}_{n_0'}^*, \\ H_{r,s,t} = H_{\langle xr'\rangle,\langle xs'\rangle,\langle xt'\rangle} \text{ for some } x \in \mathbb{Z}_n^*. \end{cases} \tag{3.20}$$

The first condition is needed to ensure that $\mathbb{Q}(\zeta_{n_0}) = \mathbb{Q}(\zeta_{n_0'})$, and implies $n_0 = n_0'$, or $n_0 = 2n_0'$ with n_0' odd, or $n_0' = 2n_0$ with n_0 odd. That answers problem (ii). For the problem (i), one should look at $W_{r,s,t}$ and see whether it is reduced to the identity or not. If $W_{r,s,t} = \{1\}$, then $L_{r,s,t}$ is simple, otherwise $L_{r,s,t}$ splits up into $|W_{r,s,t}|$ simple factors. Since $wH_{r,s,t} = H_{\langle w^{-1}r\rangle,\langle w^{-1}s\rangle,\langle w^{-1}t\rangle}$, the determination of $W_{r,s,t}$ requires to compare the sets $H_{r,s,t}$. Therefore problems (i) and (ii), eventually leading to the complete decomposition of the Jacobian of F_n, boil down to the same question: when are two sets $H_{r,s,t}$ and $H_{r',s',t'}$ equal? This is precisely what the $su(3)$ parity rule requires to know.

This very concrete problem is easily solvable on a case-by-case basis, but remains difficult to work out for general n. Koblitz and Rohrlich solved it when n is coprime with 6, and when it is a power of 2 or 3. Recently the decomposition for general n was completed by Aoki, except for 33 values of n between 2 and 180. [6]

We now summarize their results, leaving out the 33 special values of n. We first define an equivalence relation on the admissible triplets: we will say that $(r, s, t) \sim (r', s', t')$ iff $(r', s', t') = (\langle hr\rangle, \langle hs\rangle, \langle ht\rangle)$ up to a permutation, that is, (r', s', t') belongs to the class $[r, s, t]$, up to a permutation.

Concerning problem (i), it has been shown that the only non-simple $L_{r,s,t}$ are those with (r, s, t) being equivalent to one of the following triplets [6,33]:

$$\frac{n}{n_0}(1, w, n_0 - 1 - w) \;\; \text{with } w^2 = 1 \bmod n_0,\ w \neq \pm 1,\ w \neq \tfrac{1}{2}n_0 + 1 \;\; \text{if } 8|n_0, \tag{3.21}$$

$$\frac{n}{n_0}(1, 1, n_0 - 2) \quad \text{if } 4|n_0, \tag{3.22}$$

$$\frac{n}{n_0}(1, w, w^2) \quad \text{with } 1 + w + w^2 = 0 \bmod n_0, \tag{3.23}$$

[6] The actual list of excluded integers is $\mathcal{E} = \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 18, 20, 21, 22, 24, 26, 28, 30, 36, 39, 40, 42, 48, 54, 60, 66, 72, 78, 84, 90, 120, 156, 180\}$.

$$\frac{n}{n_0}(1, \tfrac{1}{2}n_0 + 1, \tfrac{1}{2}n_0 - 2), \quad \text{if } 8|n_0. \tag{3.24}$$

Corresponding to these four cases, $L_{r,s,t}$ factorizes in, respectively, 2,2,3 and 4 isomorphic simple lattices. For instance, one may check that for $n = 7$,

$$L_{1,2,4} \sim [\mathbb{Z}(\tfrac{1}{2}(1 + \sqrt{-7}))]^3 \tag{3.25}$$

so that the factor $\mathbb{C}^3/L_{1,2,4}$ is isogenous to the cube of the elliptic curve of modulus $\tau = \frac{1}{2}(1 + \sqrt{-7})$.

As to problem (ii), obviously we have $L_{r,s,t} = L_{r',s',t'}$ if $(r', s', t') \in [r, s, t]$ (as noted after (3.9)), or if (r', s', t') is a permutation of (r, s, t). These are trivial isogenies (in fact isomorphisms), and they are the only ones if n is coprime with 6 [6]. When 2 or 3 divides n, there is a non-trivial isogeny between $L_{r,s,t}$ and $L_{r',s',t'}$ if and only if (r, s, t) and (r', s', t') are equivalent to elements in one of the following three sets [33]:

$$\{(a, a, n - 2a), (a, \tfrac{1}{2}n - a, \tfrac{1}{2}n), (\tfrac{1}{2}n - a, \tfrac{1}{2}n - a, 2a),$$
$$(\tfrac{1}{2}a, \tfrac{1}{2}(n + a), \tfrac{1}{2}n - a), (\tfrac{1}{4}(n - 2a), \tfrac{1}{4}(3n - 2a), 2a)\}, \tag{3.26}$$
$$\{(a, 3a, n - 4a), (\tfrac{1}{2}n - a, \tfrac{1}{2}n - 2a, 3a)\}, \tag{3.27}$$
$$\{(a, 2a, n - 3a), (\tfrac{1}{3}n - a, \tfrac{1}{3}2n - a, 2a)\}, \tag{3.28}$$

where the integer a is subjected to two conditions: first, the components of the triplets should be integers, and second, after (r, s, t) and (r', s', t') have been identified with two triplets in one of the three groups, n_0 and n'_0 should be related as in (3.20), namely $\mathbb{Z}^*_{n_0}$ and $\mathbb{Z}^*_{n'_0}$ should be isomorphic. On the other hand, a need not be coprime with n. This list, remarkably simple, is an easy consequence of the corresponding one for the pairs of triplets satisfying $H_{r,s,t} = H_{r',s',t'}$, as established in [33]. In the $su(3)$ interpretation, it completely solves the parity criterion by giving all pairs of affine weights whose characters can be coupled in a modular invariant, that is, those weights such that the matrix element $N_{p,p'}$ may be non-zero. This list could of course be used to rederive the classification of the $su(3)$ modular invariant partition functions proved in [2] (except at the 33 values of n excluded by Aoki, which can be handled by hand).

It is instructive to compute the decomposition of $\mathrm{Jac}(F_n)$ in specific cases. In order to do this, we first come back to the ST theorem and show how to compute the splitting of $L_{r,s,t}$.

Assume $W_{r,s,t} \neq \{1\}$. We start with two trivial observations: $W_{r,s,t} \subset H_{r,s,t}$ because 1 always belongs to $H_{r,s,t}$, and $W_{r,s,t} \subset \mathbb{Z}^*_{n_0}$ is a group. Recall the definition of $L_{r,s,t}$ as

$$L_{r,s,t} = \{(\dots, \sigma_h(z), \dots)_{h \in H_{r,s,t}} : z \in \mathbb{Z}(\zeta_{n_0})\}. \tag{3.29}$$

$W_{r,s,t}$ acts freely on $H_{r,s,t}$, so we can write a class decomposition as $H_{r,s,t} = A_{r,s,t} \cdot W_{r,s,t}$, with $|A_{r,s,t}| = |H_{r,s,t}|/|W_{r,s,t}|$. Reordering the entries in $L_{r,s,t}$ according to this decomposition, we have

$$L_{r,s,t} = \{(\dots, (\dots, \sigma_a \sigma_w(z), \dots)_{w \in W_{r,s,t}}, \dots)_{a \in A_{r,s,t}} : z \in \mathbb{Z}(\zeta_{n_0})\}. \tag{3.30}$$

Thus an element of $L_{r,s,t}$ is of the form $(\dots, \sigma_a(\lambda), \dots)_{a\in A_{r,s,t}}$ where λ is itself a vector of the type $(\dots, \sigma_w(z), \dots)_{w\in W_{r,s,t}}$.

Let K be the subfield of $\mathbb{Q}(\zeta_{n_0})$ fixed by $W_{r,s,t}$, and $\mathcal{O}_K$ be the ring of integers of K. Then $\mathbb{Q}(\zeta_{n_0})$ is an algebraic extension of K, with Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{n_0})/K) = W_{r,s,t}$. We also let θ_i be the elements of a K-integral basis of $\mathbb{Z}(\zeta_{n_0})$, that is, any element $z \in \mathbb{Z}(\zeta_{n_0})$ can be uniquely written as $z = \sum_i x_i\theta_i$ with all x_i in $\mathcal{O}_K$. Obviously the number of θ_i is equal to $|W_{r,s,t}|$.

Let $\Lambda = (\dots, \sigma_w(z), \dots)_{w\in W_{r,s,t}}$ for z running over $\mathbb{Z}(\zeta_{n_0})$. We define a linear complex map ψ on Λ by

$$x_i(z) \equiv (\psi(\lambda))_i = \sum_{w\in W_{r,s,t}} \sigma_w(\theta_i z) = \sum_{w} \sigma_w(\theta_i)\,\sigma_w(z), \quad 1 \le i \le |W_{r,s,t}|. \tag{3.31}$$

Clearly all x_i belong to $\mathcal{O}_K$, and we obtain the inclusion

$$\psi(\Lambda) \subset [\mathcal{O}_K]^{|W_{r,s,t}|}, \quad \text{with finite index.} \tag{3.32}$$

The index is proved to be finite by noticing that ψ is invertible since $\det \psi_{i,w} = \det \sigma_w(\theta_i)$ is the relative discriminant of $\mathbb{Q}(\zeta_{n_0})$ over K. Since $L_{r,s,t}$ is equal to $(\sigma_a(\Lambda))_{a\in A_{r,s,t}}$, we obtain that it is contained with finite index in a product of $|W_{r,s,t}|$ isomorphic factors through the linear map ψ, from which the isogeny follows:

$$L_{r,s,t} \sim \{(\dots, \sigma(x), \dots)_{\sigma\in H_{r,s,t}/W_{r,s,t}} : x \in \mathcal{O}_K\}^{|W_{r,s,t}|}. \tag{3.33}$$

The lattice within the curly brackets has complex multiplication by K, has CM-type $(K, H_{r,s,t}/W_{r,s,t})$, and is simple by the ST theorem.

For $n = 7$, the previous equation implies the decomposition (3.25). Indeed one checks that $W_{1,2,4} = H_{1,2,4} = \{1, 2, 4\}$, and that the subfield of $\mathbb{Q}(\zeta_7)$ fixed by σ_2 and σ_4 is $K = \mathbb{Q}(\sqrt{-7})$ with $\mathcal{O}_K = \mathbb{Z}(\frac{1}{2}(1 + \sqrt{-7}))$.

3.4. Elliptic curves

Being one-dimensional, an elliptic curve is the simplest Abelian variety of all. It is thus a natural question to see if a Fermat curve can decompose in a maximal way, as a product of elliptic curves. It turns out that this question has a positive answer, but also that it is far from being generic. We will show that a necessary condition to have a maximal splitting is that n be a divisor of 24. Koblitz has solved the more difficult question to list all lattices $L_{r,s,t}$ that have a maximal splitting in elliptic curves. Setting $\gcd(r, s, t) = n/n_0$ as above, he finds that no $L_{r,s,t}$ is isogenous to a product of elliptic factors unless n_0 belongs to the following set $\{3, 4, 6, 7, 8, 12, 15, 16, 18, 20, 21, 22, 24, 30, 39, 40, 48, 60\}$ [38].

The argument is in fact extremely simple. We know that the period lattice of F_n splits into a product of lattices $L_{r,s,t}$. If F_n is to be isogenous to a product of elliptic curves, each $L_{r,s,t}$ must be isogenous to a product of one-dimensional lattices. Since $L_{r,s,t} \subset \mathbb{C}^{\varphi(n_0)/2}$, the ST theorem (see Section 3.3) says that this can only happen if $|W_{r,s,t}| = |H_{r,s,t}| = \frac{1}{2}\varphi(n_0)$.

But $W_{r,s,t} \subset H_{r,s,t}$ implies $W_{r,s,t} = H_{r,s,t}$, so that $H_{r,s,t}$ is a group. Thus F_n is isogenous to a product of elliptic curves iff $H_{r,s,t}$ is a group for all admissible triplets (r, s, t). Note that because of $H_{r,s,t} = hH_{\langle hr\rangle,\langle hs\rangle,\langle ht\rangle}$ for h in $H_{r,s,t}$, the set $H_{r,s,t}$ in general depends on which representative of the class $[r, s, t]$ we choose, except if precisely $H_{r,s,t}$ is a group. Let $n = 2^m q$ with q odd.

First take $r = s = 2^m$. Then $H_{2^m,2^m,n-2^{m+1}} = \{1, 2, \ldots, \frac{1}{2}(q-1)\} \cap \mathbb{Z}_q^*$. Since q is odd, 2 and $\frac{1}{2}(q-1)$ belong to $H_{2^m,2^m,n-2^{m+1}}$, but $2 \cdot \frac{1}{2}(q-1) = q-1$ does not. Thus $H_{2^m,2^m,n-2^{m+1}}$ is not a group unless $q \leq 3$.

Now take $r = s = q$. Then $H_{q,q,n-2q} = \{1, 3, 5, \ldots, 2^{m-1}-1\} \subset \mathbb{Z}_{2^m}^*$. But if $2^m \geq 16$, then modulo 2^m, $(2^{m-2}+1)^2 = 2^{m-1}+1 \notin H_{q,q,n-2q}$. Thus $H_{q,q,n-2q}$ is not a group if $2^m \geq 16$.

Therefore a necessary condition for $H_{r,s,t}$ to be a group for all (r, s, t) is that $n = 2^m q$ with $2^m \leq 8$ and $q \leq 3$, or in other words, that n divides 24. This is a sufficient condition for $n \leq 12$ only. If n divides 24 and is smaller or equal to 12, $H_{r,s,t}$ is at most of order 2 since $\varphi(12) = 4$. Being a subset of $\mathbb{Z}_{24}^*$, $H_{r,s,t}$ is automatically a group because every element of $\mathbb{Z}_{24}^*$ has a square equal to 1 modulo 24 (24 is the largest integer to have this property). On the other hand, for $n = 24$, $H_{r,s,t}$ can be of order 4 and it is no longer guaranteed to be a group. An explicit calculation shows that indeed it is not always a group (see below), so we conclude that the Fermat curve F_n is isogenous to a product of elliptic curves if and only if $n \leq 12$ divides 24.

It is straightforward to compute the decomposition of F_n for $n \mid 24$. For $n = 3, 4$ and 6, all $L_{r,s,t}$ are already one-dimensional, isogenous to $\mathbb{Z}(\omega = \exp\frac{2}{3}i\pi)$ for $n = 3$ and 6, and to $\mathbb{Z}(i)$ for $n = 4$. For $n = 8$, $H_{r,s,t}$ can only be $\{1, 3\}$ or $\{1, 5\}$ if it is of order 2. One finds $K = \mathbb{Q}(\sqrt{-2})$ if $H_{r,s,t} = \{1, 3\}$ and $K = \mathbb{Q}(i)$ if $H_{r,s,t} = \{1, 5\}$. Apart from $(r, s, t) = (2, 2, 4)$, $(2, 4, 2)$ and $(4, 2, 2)$ which have their $H_{r,s,t}$ equal to $\{1\}$ and their $L_{r,s,t}$ isogenous to $\mathbb{Z}(i)$, the complete decomposition of F_8 follows by merely counting how many triplets have a $H_{r,s,t}$ equal to $\{1, 3\}$ or to $\{1, 5\}$. Similarly for $n = 12$, a set $H_{r,s,t}$ of order 2 can only be $\{1, 5\}$ or $\{1, 7\}$, yielding, respectively, $L_{r,s,t} \sim [\mathbb{Z}(i)]^2$ or $L_{r,s,t} \sim [\mathbb{Z}(\omega)]^2$. Finally for $n = 24$, there are 24 triplets (r, s, t) such that their $H_{r,s,t}$ is not a group, for instance $H_{1,3,20} = \{1, 5, 11, 17\}$. The corresponding $L_{r,s,t}$ are all equal and their product is $[L_{1,3,20}]^{24}$, with $L_{1,3,20} \subset \mathbb{C}^4$ simple because $W_{1,3,20} = \{1\}$. Putting everything together, one obtains

$$F_3 \sim \mathbb{Z}(\omega), \quad F_4 \sim [\mathbb{Z}(i)]^3, \quad F_6 \sim [\mathbb{Z}(\omega)]^{10}, \tag{3.34}$$

$$F_8 \sim [\mathbb{Z}(\sqrt{-2})]^{12} \oplus [\mathbb{Z}(i)]^9, \quad F_{12} \sim [\mathbb{Z}(\omega)]^{28} \oplus [\mathbb{Z}(i)]^{27}, \tag{3.35}$$

$$F_{24} \sim [\mathbb{C}^4/L_{1,3,20}]^{24} \oplus [\text{product of 157 elliptic curves}]. \tag{3.36}$$

Let us finally observe that the weights involved in the exceptional $su(3)$ modular invariants at height $n = 8$, 12 and 24, correspond to lattices which have all a maximal decomposition in elliptic curves. Moreover, those pertaining to a given type I modular invariant have complex multiplication by the same CM field, namely $\mathbb{Q}(\sqrt{-2})$ for $n = 8$ and 24, and $\mathbb{Q}(i)$ for $n = 12$. This is obvious for triplets that label characters coupled to each other since the very fact that they can be coupled means they have the same CM-type, but it is not for characters appearing in different blocks. The Moore–Seiberg exceptional invariant at $n = 12$ has not this property, and involves different CM-types.

4. Combinatorial groups for triangulated surfaces

We gather in this section some constructions that appear naturally in the context of Fermat curves, triangular billiards and rational conformal field theories. They lie at the heart of a deep interplay between combinatorial, complex and arithmetical structures on closed surfaces. A nice reference about them is [39], and [8] contains elementary reviews. It is a good exercise to read this section and the next in parallel, with the explicit case of the cubic Fermat curve in mind.

4.1. Cartography

Our starting point is a compact Riemann surface Σ together with a holomorphic map h from Σ to the Riemann sphere ramified over three points only, say 0, 1 and ∞.[7] The Riemann sphere has a "standard" triangulation consisting of 0, 1 and ∞ as vertices, the real segments $[\infty, 0]$, $[0, 1]$ and $[1, \infty]$ as edges, and the upper- and lower-half planes as faces. This triangulation has the obvious but remarkable property that:

- the vertices can be assigned labels 0, 1 and ∞ in such a way that edges do not link vertices with the same label (we say that vertices are three-colorable);
- the faces can be assigned labels black (corresponding to the lower-half plane) and white (corresponding to the upper-half plane) in such a way that faces of the same color have no common edge (faces are two-colorable).

Taking the inverse image of this triangulation by h, Σ can be equipped with a triangulation which inherits the same coloring properties.

The combinatorial data of the triangulation are conveniently encoded in the so-called cartographic group. Its definition uses the orientation of the triangulation (of course the orientation of Σ as a Riemann surface induces an orientation on the triangulation). The cartographic group permutes the flags of the triangulation. A flag is an ordered triple (v, e, f) where v is a vertex, e an edge containing v and f a face containing e in such a way that with respect to the orientation of the boundary of f, e starts from v. The number of flags is twice the number of edges (or thrice the number of faces for a triangulation). By orientability, there is a cyclic ordering of the flags $(v, ., .)$ (resp. $(., e, .)$, $(., ., f)$) that contain a fixed vertex v (resp. an edge e, a face f). Hence every flag (v, e, f) has a unique vertex successor $(v, e, f)^{\sigma}$ (of the form (v, e', f')), a unique edge successor $(v, e, f)^{\alpha}$ (of the form (v', e, f')) and a unique face successor $(v, e, f)^{\varphi}$ (of the form (v', e', f)). The flag permutations σ, α and φ generate the cartographic group $\widehat{C}$, which encodes all the

[7] The compact surfaces Σ for which such an h exists have the following characterization: they are defined over number fields (Belyi's theorem).

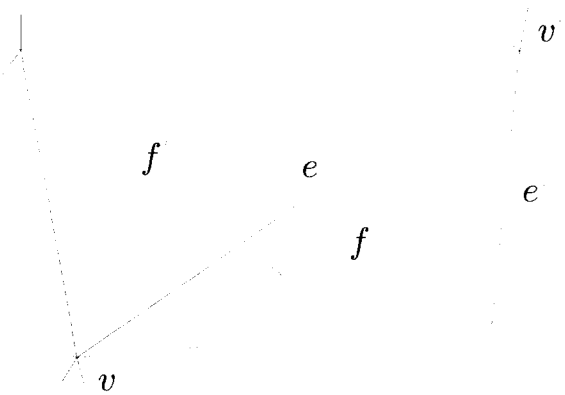

Fig. 1. The action of the generators of the cartographic group on the flags is defined in the text. One finds that $(v, e, f)^{\varphi} = (v', e', f)$, $(v', e', f)^{\sigma} = (v', e, f')$ and $(v', e, f')^{\alpha} = (v, e, f)$, confirming the relation $\alpha\sigma\varphi = 1$. The arrow indicates the orientation.

combinatorial data of the triangulation. In fact, the cycle decompositions of σ, α and φ are in one-to-one correspondence with the vertices, edges and faces of the triangulation. For instance, the cartographic group of the standard triangulation of the Riemann sphere is isomorphic to S_3 (the permutation group on three letters).

This definition of the cartographic group works for any polygonal decomposition of an oriented surface without boundary. In general one has $\alpha^2 = 1$ (an edge is common to only two faces), but particular to a triangulation is the relation $\varphi^3 = 1$. The order of σ is equal to $\mathrm{lcm}_v(n_v)$, where n_v is the number of triangles that meet at the vertex v. Perhaps less obvious is the relation $\alpha\sigma\varphi = 1$, valid for general polygonal decompositions. It can be easily verified with the help of Fig. 1.

The cartographic group of a triangulation is always a quotient group of the modular group via the homomorphism $S \to \alpha$, $T \to \sigma$. Indeed as noted above, one has $S^2 = 1$ and $(ST)^3 = (\alpha\sigma)^3 = \varphi^{-3} = 1$. This implies that there is a universal cartographic group, which is the modular group, and a universal triangulation, of which the flags can be parametrized by the elements of the modular group. The corresponding triangulation is familiar. The quotient of the upper-half plane $\mathfrak{H}$ by Γ_2, the principal congruence subgroup of level 2 in $PSL_2(\mathbb{Z})$ is known to be a sphere with three punctures. So there is a unique holomorphic map from $\mathfrak{H}$ to $\mathbb{CP}_1 - \{0, 1, \infty\}$ invariant under Γ_2. For $\tau \in \mathfrak{H}$, we set $q = \mathrm{e}^{2\mathrm{i}\pi\tau}$ and define

$$U(\tau) = \left[\frac{q^{1/24}\theta_4(0,\tau)}{\eta(q)}\right]^4 = \prod_{m=1}^{\infty}(1 - q^{m-\frac{1}{2}})^8, \tag{4.1}$$

$$V(\tau) = -\left[\frac{q^{1/24}\theta_3(0,\tau)}{\eta(q)}\right]^4 = -\prod_{m=1}^{\infty}(1 + q^{m-\frac{1}{2}})^8, \tag{4.2}$$

$$W(\tau) = \left[\frac{q^{1/24}\theta_2(0,\tau)}{\eta(q)}\right]^4 = 16\sqrt{q}\prod_{m=1}^{\infty}(1 + q^{m})^8. \tag{4.3}$$

It is a standard identity that $U(\tau) + V(\tau) + W(\tau) = 0$. Then the inverse image of the standard triangulation of the sphere by the map $\lambda(\tau) = -U(\tau)/W(\tau)$ (invariant under Γ_2) gives the appropriate triangulation of $\mathfrak{H}$. More precisely, one can check that

$$\lambda\left(\frac{-1}{\tau}\right) = \frac{1}{\lambda(\tau)}, \qquad \lambda(\tau+1) = 1 - \lambda(\tau), \tag{4.4}$$

from which the invariance under Γ_2 follows, and that $256(1-\lambda+\lambda^2)^3/(\lambda(1-\lambda))^2$ (a rational function of degree 6 in λ) is the standard modular invariant function j. Moreover it is easy to see that λ maps 0 to 0, 1 to 1 and ∞ to ∞. Thus λ defines a homeomorphism of $\overline{\mathfrak{H}/\Gamma_2}$ with the Riemann sphere. From the above product formulas, one checks that $\lambda(\tau)$ is real negative on the imaginary axis, ranges between 0 and 1 on the big semi-circles going from ± 1 to 0 (they are to be identified in $\mathfrak{H}/\Gamma_2$), and takes all positive values from 1 to ∞ on the line $\operatorname{Re}\tau = 1$. Thus the standard triangulation of the λ-sphere consists of the two faces (see Fig. 2)

$$\mathrm{B} = \{\tau \in \mathfrak{H}: -1 \le \operatorname{Re}\tau \le 0,\ |\tau + \tfrac{1}{2}|^2 \ge \tfrac{1}{4})\}, \tag{4.5}$$

$$\mathrm{W} = \{\tau \in \mathfrak{H}: 0 \le \operatorname{Re}\tau \le 1,\ |\tau - \tfrac{1}{2}|^2 \ge \tfrac{1}{4})\}. \tag{4.6}$$

The action of Γ_2 on this triangulation yields the universal triangulation of $\mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$ shown in Fig. 2. For later use, we record the following remarkable product formula:

$$\frac{\mathrm{d}\lambda}{\mathrm{d}\tau} = \frac{\mathrm{i}\pi}{16\sqrt{q}} \prod_{m=1}^{\infty} \frac{(1-q^m)^4}{(1+q^m)^{16}}. \tag{4.7}$$

In this interpretation, the cartographic group of the standard triangulation of the Riemann sphere, isomorphic to S_3, is represented as $PSL_2(\mathbb{Z})/\Gamma_2$. Let C be the kernel of the homomorphism from $PSL_2(\mathbb{Z})$ to $\widehat{C}$. Because of the intertwining property of h, an element of the modular group whose image is trivial in $\widehat{C}$ must be trivial in $S_3 = PSL_2(\mathbb{Z})/\Gamma_2$. This means that C is a subgroup of Γ_2. Let us also define $\widehat{D} = \Gamma_2/C$. It is well known that Γ_2 is the subgroup of $PSL_2(\mathbb{Z})$ generated by $R_\infty = T^2$, $R_0 = ST^2S^{-1}$ and $R_1 = (TS)T^2(TS)^{-1}$. They satisfy a single relation, namely $R_0R_1R_\infty = 1$. This implies that $\widehat{D}$ is generated by $\mu_\infty = \sigma^2$, $\mu_0 = \alpha\sigma^2\alpha^{-1}$ and $\mu_1 = (\sigma\alpha)\sigma^2(\sigma\alpha)^{-1}$. The order of $\widehat{C} = PSL_2(\mathbb{Z})/C$ is six times that of $\widehat{D}$.

The connectedness of Σ implies that $\widehat{C}$ acts transitively on flags. Hence, the set of flags is a homogeneous space for $\widehat{C}$. The isotropy subgroup of a flag, well defined up to conjugacy in $\widehat{C}$, has the following properties:

- it does not contain any invariant subgroup of $\widehat{C}$ (such an invariant subgroup would act trivially on all flags);
- its image in S_3 is trivial (because the cartographic group acts compatibly with the map h).

In summary, each pair (Σ, h) gives rise to a subgroup B of Γ_2, and an invariant subgroup G of $PSL_2(\mathbb{Z})$ (the intersection of all the conjugates of B in $PSL_2(\mathbb{Z})$ so G is a subgroup of B) such that: (i) the flags are parametrized by $B\backslash PSL_2(\mathbb{Z})$ (the set of left cosets Bg for $g \in PSL_2(\mathbb{Z})$), and, (ii) the cartographic group is isomorphic to $PSL_2(\mathbb{Z})/G$ acting on $B\backslash PSL_2(\mathbb{Z})$ on the right.

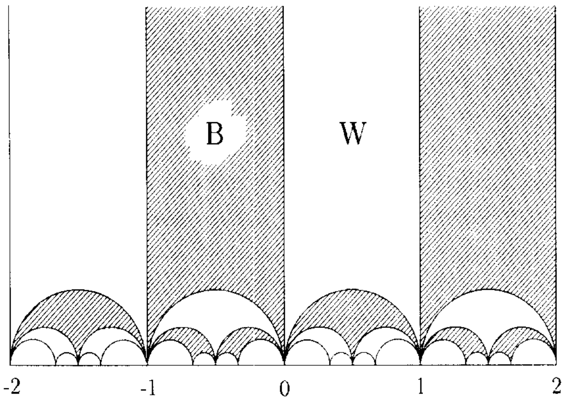

Fig. 2. Universal triangulation of $\mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}$ obtained by translating the standard triangulation of the λ-sphere (consisting of the two faces marked B(lack) and W(hite)) by the principal congruence group Γ_2. Any flag is obtained from a fixed one F^* by the action of a unique element of the modular group. The cartographic group acts by the standard multiplication: if c, c' are elements of the cartographic group, $(F^c)^{c'} = g_{c'} g_c(F^*)$ for some $g_c, g_{c'} \in PSL_2(\mathbb{Z})$. For instance the successors of the flag F containing the vertex 0 and the face W are $F^\sigma = ST^{-1}S(F)$, $F^\alpha = S(F)$ and $F^\varphi = TS(F)$ (orientation chosen clockwise).

But there is in fact a reciprocal. If B is any subgroup of Γ_2, let Σ' be the quotient $\mathfrak{H}/B$. It is a Riemann surface with punctures, and the projection from $\mathfrak{H}/B$ to $\mathfrak{H}/\Gamma_2 \cong \mathbb{CP}_1 - \{0, 1, \infty\}$ is holomorphic and unramified. This map has a holomorphic extension, say h', from the compactified surface $\overline{\Sigma}'$ (the surface obtained from Σ' by "filling" the punctures, see for example [40]) to $\mathbb{CP}_1$, ramified only above 0, 1 and ∞. Now if B comes from a compact Riemann surface Σ via a map h by the above construction, then Σ is isomorphic to $\overline{\Sigma}'$. Indeed Σ and $\overline{\Sigma}'$ can be cut into triangles with the same combinatorial arrangement. Let us consider pairs of triangles f and f' on Σ and $\overline{\Sigma}'$, that are mapped by h and h' onto the same triangle of the standard triangulation of $\mathbb{CP}_1$. Restricted to the interior of the triangles, these maps are holomorphic, so their composition defines maps from each triangle of Σ to the corresponding triangle of $\overline{\Sigma}'$, which are holomorphic on the interior of the triangles. Along the edges, they glue so as to yield a continuous one-to-one map from Σ to $\overline{\Sigma}'$. To check holomorphicity along the edges, consider a pair of faces f_1 and f_2 with a common edge e on Σ and the corresponding pair f_1' and f_2' with common edge e' on $\overline{\Sigma}'$. The maps h and h' send the domains made up of the interiors of the faces together with the interiors of the common edges holomorphically and one-to-one to the same open subset of the Riemann sphere. This ensures that the composite map is holomorphic, and in particular holomorphic along the interior of the common edge. So the continuous map we have constructed from Σ to $\overline{\Sigma}'$ is holomorphic except maybe at the marked points. But then its continuous extension has to be holomorphic everywhere (a holomorphic map in a pointed disk, bounded near the puncture has a unique holomorphic extension).

So the cartography of a Riemann surface (defined over $\overline{\mathbb{Q}}$) eventually leads to its uniformization by $\mathfrak{H}/B$ for some Fuchsian group B, in fact a subgroup of $PSL_2(\mathbb{Z})$. This will be extensively used in the next sections to uniformize the Fermat curves, and other related curves.

The symmetry group of a triangulation has a natural definition. It consists of the relabelings of the flags that do not change the combinatorial data, i.e. that commute with the action of the cartographic group. As the cartographic group acts transitively on flags, an element of the symmetry group that fixes one flag has to be the identity. For the same reason, the orbits of the symmetry group all have the same number of elements. So the order of the symmetry group divides the number of flags. If this order is the number of flags, we can choose a flag and then get any other flag by acting with a unique symmetry. So in that case, the flags can be parametrized by symmetries. But the cartographic group commutes with symmetries, so an element of the cartographic group can fix a flag only if it is the identity. In other words, there is no non-trivial isotropy, and the flags are also parametrized by elements of the cartographic group ($B = G = C$).

It is almost obvious (and can be checked along lines similar to the proof above that Σ and $\overline{\Sigma}'$ are the same Riemann surface) that the action of the symmetry group induces holomorphic automorphisms of the associated Riemann surface.

As mentioned above, the cartographic group can be used to encode the combinatorics of a polygonal decomposition of a closed oriented surface. For the triangulation of a Riemann surface given by the inverse image of the standard triangulation of the sphere by a map ramified only over 0, 1 and ∞, there is another convenient combinatorial description. Let us fix such a Riemann surface and such a map. This time, we use a group, which we call the triangular group, that permutes the faces of the triangulation. It is simpler to define than the cartographic group. It has three generators of order 2: σ_0, σ_1 and σ_∞. If f is a face of the triangulation, the edge of f opposite to the vertex 0 (i.e. joining the vertices 1 and ∞) is common to exactly one other face f', and we set $\sigma_0(f) = f'$. The other two generators are defined analogously. The triangular group specifies which triangle is glued to which other triangle and along which edge, so it gives all that is needed to reconstruct the surface. It contains an invariant subgroup of index 2 with generators

$$\rho_0 = \sigma_\infty\sigma_1, \qquad \rho_1 = \sigma_0\sigma_\infty, \qquad \rho_\infty = \sigma_1\sigma_0. \tag{4.8}$$

Geometrically, ρ_v is a rotation around the vertex v, mapping a triangle touching v to the next one of the same color. The order of ρ_v is half the number of triangles meeting at v. They clearly satisfy $\rho_\infty\rho_1\rho_0 = 1$, so this subgroup, called the oriented triangular group for obvious reasons, is a quotient group of Γ_2. Hence there is a unique epimorphism from Γ_2 to the oriented triangular group sending R_0^{-1} to ρ_0, R_1^{-1} to ρ_1 and R_∞^{-1} to ρ_∞. The oriented triangular group is important for two reasons. First it contains the same combinatorial information as the full triangular group. Indeed, since it maps white faces into white faces and black faces into black faces, it says how the vertices of faces of a given color are linked to each other, and thus specifies all the edge identifications needed to completely reconstruct the surface. Second, it is easier to compute than the cartographic group, and yet allows to describe the latter more easily than what was done before. The idea is simple, but requires first to find an appropriate parametrization of the flags. With the flag (v, e, f), we associate a permutation (jkl) of the symbol (01∞): the first element is the label of v, the second is the label of the other vertex of e and the third is the last label remaining. Then with the same flag (v, e, f), we associate the white triangle t that has e in common with f, and we write $(v, e, f) \cong [(jkl), t]$. Let $\varepsilon(jkl)$ be 0 if (jkl) is an even permutation and 1 if it is an odd permutation of (01∞). It is then easy to check that

$$\sigma[(jkl), t] = [(jlk), \rho_j^{\varepsilon(jkl)}(t)], \tag{4.9}$$

$$\alpha[(jkl), t] = [(kjl), t], \tag{4.10}$$

$$\varphi[(jkl), t] = [(klj), \rho_k^{-\varepsilon(klj)}(t)]. \tag{4.11}$$

From these, one computes the action of the $\widehat{D}$ group to be

$$\mu_0[(jkl), t] = [(jkl), \rho_k t], \tag{4.12}$$

$$\mu_1[(jkl), t] = [(jkl), \rho_j^{\varepsilon(jlk)} \rho_l \rho_j^{-\varepsilon(jlk)} t], \tag{4.13}$$

$$\mu_\infty[(jkl), t] = [(jkl), \rho_j t]. \tag{4.14}$$

The equation for μ_1 is a little bit surprising, but is needed to ensure the relation $\mu_\infty \mu_0 \mu_1 = 1$. This shows that although the group $\widehat{D}$ is closely related to the oriented triangular group, they do not coincide, the former being in general bigger. The three generators μ_0, μ_1 and μ_∞ all have the same order n, the least common multiple of the orders of ρ_0, ρ_1 and ρ_∞.

Because it is of particular importance for what follows, we will explore, for the rest of this section, the case where the oriented triangular group associated with (Σ, h) is Abelian. The above relations simplify to read

$$\mu_0[(jkl), t] = [(jkl), \rho_k t], \tag{4.15}$$

$$\mu_1[(jkl), t] = [(jkl), \rho_l t], \tag{4.16}$$

$$\mu_\infty[(jkl), t] = [(jkl), \rho_j t]. \tag{4.17}$$

Thus the group $\widehat{D}$ is also Abelian, and is isomorphic to a subgroup of $\mathbb{Z}_n \times \mathbb{Z}_n$ (or more invariantly of the quotient of $\mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$ by the diagonal $\mathbb{Z}_n$).

If $\widehat{D} \equiv \widehat{D}_n = \mathbb{Z}_n \times \mathbb{Z}_n$, one can even give a presentation of the cartographic group, which we denote by $\widehat{C}_n$, by generators and relations, i.e. one can determine the kernel C_n of the homomorphism from $PSL_2(\mathbb{Z})$ to $\widehat{C}_n$. As the relation $\mu_0\mu_1\mu_\infty = 1$ is automatic in terms of the generators α and σ, the commutation of μ_0, μ_1 and μ_∞ amounts to $\mu_\infty\mu_1\mu_0 = 1$, or $\sigma^2(\sigma\alpha)\sigma^2(\sigma\alpha)^{-1}\alpha\sigma^2\alpha^{-1} = 1$. Using $\alpha^{-1} = \alpha$ and $\alpha\sigma^{-1}\alpha = \sigma\alpha\sigma$, this can be simplified to $(\sigma^3\alpha)^3 = 1$. Moreover, there is the obvious relation $\sigma^{2n} = 1$. The quotient of the modular group by these two relations is $\widehat{C}_n$ because they ensure the commutativity and the correct order for μ_0, μ_1 and μ_∞:

$$\widehat{D_n} = \mathbb{Z}_n \times \mathbb{Z}_n, \qquad \widehat{C}_n = \langle S, T \mid S^2, (ST)^3, T^{2n}, (T^3S)^3 \rangle, \qquad |\widehat{C}_n| = 6n^2. \tag{4.18}$$

Although not obvious at this stage, $\widehat{C}_n$ is isomorphic to the semi-direct product $S_3 : (\mathbb{Z}_n \times \mathbb{Z}_n)$, and possesses an action on $\mathbb{CP}_2$ by

$$A(x; y; z) = (\zeta x; y; z), \quad B(x; y; z) = (x; \zeta y; z) \qquad (\zeta = e^{2i\pi/n}), \tag{4.19}$$

$$\tau_1(x; y; z) = (y; x; z), \quad \tau_2(x; y; z) = (x; z; y). \tag{4.20}$$

We will prove this isomorphism in Section 4.2, when we consider the automorphisms of the Fermat curves.

To summarize, there is a natural universal object for pairs (Σ, h) with Abelian oriented triangular groups. Let Σ_n be the quotient $\mathfrak{H}/C_n$ with punctures filled in. It is a compact Riemann surface, and its group of holomorphic automorphisms permuting the flags is isomorphic to $\widehat{C}_n$. The flags of (Σ, h) can be parametrized as the quotient of $\widehat{C}_n$ by the stabilizer subgroup of a given flag, in fact a subgroup of $\widehat{D}_n$. This subgroup acts as automorphisms on Σ_n and the quotient is nothing but Σ. In other words, Σ_n is a covering of Σ of degree equal to the common order of the stabilizer subgroups. This gives a convenient way to relate the geometry of Σ to that of Σ_n. We will use it in the following sections.

4.2. *Modular forms associated to Fermat curves*

We have seen in Section 3 that certain important features of the RCFT with an affine symmetry based on $su(3)$ were governed by quantities that had a very important role in the description of the geometry of the Fermat curves. Also some similarities emerged: for instance the weights in the alcôve of $su(3)$ at height n are in one-to-one correspondence with the holomorphic differentials on F_n. In this section, we would like to see whether this relationship goes beyond the superficial level by making the holomorphic differentials on the Fermat curves look as much as possible like the characters of a conformal field theory. Our construction is not canonical in a mathematical sense, but it is nevertheless quite natural. We use the vocabulary associated with the combinatorics of triangulations, as presented in the previous section.

Let F_n be the Fermat curve of degree n,

$$u^n + v^n + w^n = 0 \quad \text{in } \mathbb{CP}_2. \tag{4.21}$$

We shall sometimes use the affine model $x^n + y^n = 1$ by setting $x = \xi u/w$ and $y = \xi v/w$ where $\xi \equiv \mathrm{e}^{\mathrm{i}\pi/n}$. The map $t = -u/w$ gives an isomorphism of F_1 and $\mathbb{CP}_1$. The three base points $u = 0$, $v = 0$ and $w = 0$ of F_1 are mapped to 0, 1 and ∞. The inverse image of the real axis gives a triangulation of F_1 with 2 faces, 3 edges, and the base points as vertices. There is a canonical map of degree n^2 from F_n to F_1 given by

$$h_n : (u; v; w) \longrightarrow (u^n; v^n; w^n) \tag{4.22}$$

and ramified only over the base points. Taking the inverse image of the standard triangulation of F_1, F_n is naturally endowed with a triangulation consisting of $2n^2$ faces, $3n^2$ edges and $3n$ vertices (leading quickly to the genus formula). The $3n$ vertices are

$$n \text{ vertices of type } 0\text{:} \quad (0; v_0; w_0) \ \text{ with } v_0^n + w_0^n = 0, \tag{4.23}$$

$$n \text{ vertices of type } 1\text{:} \quad (u_1; 0; w_1) \ \text{ with } u_1^n + w_1^n = 0, \tag{4.24}$$

$$n \text{ vertices of type } \infty\text{:} \quad (u_\infty; v_\infty; 0) \ \text{ with } u_\infty^n + v_\infty^n = 0. \tag{4.25}$$

For $n \geq 3$, the vertices are nothing but the inflexion points of F_n (which are degenerate, the tangent line at a vertex having a contact of order n with the curve). Let us parametrize these points more explicitly by setting $\xi_0 = v_0/w_0$, $\xi_1 = w_1/u_1$ and $\xi_\infty = u_\infty/v_\infty$. These numbers are odd powers of ξ.

Edges have to join vertices of different type, so there cannot be more than $3n \cdot 2n/2$ edges. This is the actual number of edges, so that there is an edge between any two vertices of different type. It remains to describe the faces. There is a unique one-to-one holomorphic map $(u(t); v(t); w(t))$ from the upper-half plane to a (white) triangle on F_n such that $-u^n(t)/w^n(t) = t$. If the images of $t = 0$ and $t = 1$ are given vertices of type 0 and 1, say $(0; v_0; w_0)$ and $(u_1; 0; w_1)$ respectively, then a straightforward computation shows that the vertex of type ∞ in this triangle is $(u_\infty; v_\infty; 0)$ such that $\xi_0\xi_1\xi_\infty = \xi$. An analogous computation for black triangles shows that $(0; v_0; w_0)$, $(u_1; 0; w_1)$ and $(u_\infty; v_\infty; 0)$ are the vertices of a black triangle if and only if $\xi_0\xi_1\xi_\infty = \xi^{-1}$. Note in particular that any three vertices define the interior of at most one triangle, unlike the standard triangulation of the sphere.

We are now in a position to give the explicit action of the triangular group. The reflection σ_0 acts only on ξ_0. If the triangle is white (resp. black) σ_0 multiplies ξ_0 by ξ^{-2} (resp. ξ^2). The other two generators act analogously (just change the labels). From this we deduce the action of the oriented triangular group. If $t(\xi_0, \xi_1, \xi_\infty)$ is the white face with vertices given by ξ_0, ξ_1, ξ_∞ (hence $\xi_\infty\xi_1\xi_0 = \xi$), we have

$$\rho_0 t(\xi_0, \xi_1, \xi_\infty) = t(\xi_0, \xi^{-2}\xi_1, \xi^2\xi_\infty), \tag{4.26}$$

$$\rho_1 t(\xi_0, \xi_1, \xi_\infty) = t(\xi^2\xi_0, \xi_1, \xi^{-2}\xi_\infty), \tag{4.27}$$

$$\rho_\infty t(\xi_0, \xi_1, \xi_\infty) = t(\xi^{-2}\xi_0, \xi^2\xi_1, \xi_\infty). \tag{4.28}$$

In this form, it is obvious that the oriented triangular group is commutative, and that $\rho_0\rho_1\rho_\infty = \rho_0^n = \rho_1^n = \rho_\infty^n = 1$ are the only relations the generators satisfy. According to the results of the previous section, it follows that $\widehat{D}(F_n) = \widehat{D}_n = \mathbb{Z}_n \times \mathbb{Z}_n$ (equal to the oriented triangular group in this case), and that the cartographic group is $\widehat{C}_n$, the group of order $6n^2$ with presentation $\langle \alpha, \sigma \mid \alpha^2, (\alpha\sigma)^3, \sigma^{2n}, (\sigma^3\alpha)^3 \rangle$. But the number of flags on F_n is $6n^2$, precisely the order of $\widehat{C}_n$, so that F_n is isomorphic, as a Riemann surface, to the quotient $\mathfrak{H}/C_n$ with punctures filled in. Also the symmetry group of the triangulation is isomorphic to $\widehat{C}_n$.

Let us observe that $h_m \circ h_n = h_{mn}$ and that h_n not only maps F_n to F_1, but also F_{mn} to F_m for any m. By construction, as a map from F_{mn} to F_m, h_n maps vertices into vertices, edges into edges, faces into faces and flags into flags, and preserves the coloring properties. Moreover h_n intertwines the action of $\widehat{C}_{mn}$ and $\widehat{C}_m$, so that $\widehat{C}_m$ is a quotient group of $\widehat{C}_{mn}$ for any n. As a byproduct, the family $\widehat{C}_n$ indexed by positive integers is a directed projective family of groups, while the C_n is a directed injective family of groups.

The holomorphic automorphisms of F_n permuting the flags form a group isomorphic to $\widehat{C}_n$. It is straightforward to get the corresponding action. In fact, F_n has a number of obvious automorphisms: permutations of the coordinates, multiplication of the coordinates by arbitrary nth roots of unity and combinations thereof. It is clear that this group has order $6n^2$, and that it must coincide with $\widehat{C}_n$, the cartographic group we have just computed. This proves the isomorphism announced in the previous section, $\widehat{C}_n = S_3 : (\mathbb{Z}_n \times \mathbb{Z}_n)$, which otherwise can be proved abstractly. For $n > 3$, this turns out to be the full automorphism group [41] (see also Appendix A). We can view the automorphism group as a quotient of $PSL_2(\mathbb{Z})$ acting on $\mathfrak{H}$ if we uniformize F_n by the following nth roots of the functions uniformizing $\mathfrak{H}/\Gamma_2 \cong \mathbb{CP}_1$:

$$u(\tau) = \prod_{m=1}^{\infty}(1 - q^{m-1/2})^{8/n}, \tag{4.29}$$

$$v(\tau) = \xi \prod_{m=1}^{\infty}(1 + q^{m-1/2})^{8/n}, \tag{4.30}$$

$$w(\tau) = (16\sqrt{q})^{1/n} \prod_{m=1}^{\infty}(1 + q^{m})^{8/n}. \tag{4.31}$$

For definiteness, the above roots are always chosen to be real positive if the argument is real positive. Then the modular transformations

$$S: \quad (u(-1/\tau); v(-1/\tau); w(-1/\tau)) = (w(\tau); v(\tau); u(\tau)), \tag{4.32}$$

$$T: \quad (u(\tau+1); v(\tau+1); w(\tau+1)) = (\xi^{-2}v(\tau); u(\tau); w(\tau)), \tag{4.33}$$

generate a group isomorphic to $\widehat{C}_n$. The generators of Γ_2 act as

$$R_0 : (u; v; w) \longrightarrow (\xi^2 u; v; w), \tag{4.34}$$

$$R_1 : (u; v; w) \longrightarrow (u; \xi^2 v; w), \tag{4.35}$$

$$R_\infty : (u; v; w) \longrightarrow (u; v; \xi^2 w). \tag{4.36}$$

After these preliminaries, we are ready to associate modular forms (for the invariant subgroup C_n of $PSL_2(\mathbb{Z})$) to the holomorphic differentials on the Fermat curves. It is a well known fact in algebraic geometry that if the zero set of $P(u, v, w)$, a homogeneous polynomial of degree $n \geq 3$, is a smooth curve in $\mathbb{CP}_2$, the holomorphic differentials on that curve take the form

$$Q(u, v, w)\frac{w^2}{\partial P/\partial v}\,\mathrm{d}\left(-\frac{u}{w}\right), \tag{4.37}$$

where $Q(u, v, w)$ is a homogeneous polynomial of degree $n - 3$. More precisely, this is the expression of a holomorphic differential on the coordinate patch $w \neq 0$, $\partial P/\partial v \neq 0$, where $-u/w$ is a good local parameter. Because $[w^2/(\partial P/\partial v)]\,\mathrm{d}(-u/w)$ is multiplied, under permutation of the variables, by the signature of the permutation, the above expression gives the most general everywhere holomorphic differential. For F_n, we thus get a standard basis of holomorphic differentials $\{\omega_{r,s,t}\colon 1 \leq r, s, t \leq n-1,\ r+s+t = n\}$, where, in the domain $v \neq 0$, $w \neq 0$,

$$\omega_{r,s,t} = u^{r-1}v^{s-n}w^{t+1}\mathrm{d}\left(-\frac{u}{w}\right). \tag{4.38}$$

The differential $\omega_{r,s,t}$ has zeros of order $r-1$ at the n vertices of type 0, of order $s-1$ at the n vertices of type 1, and of order $t-1$ at the n vertices of type ∞, for a total of $n(n-3)$ zeros as expected. Taking τ as a local parameter, they yield a basis for the modular forms of degree 2 for C_n. Using relation (4.7) and the standard identity $\prod_{m\geq 1}(1+q^m)(1-q^{2m-1}) = 1$, and neglecting a constant factor equal to $(-i\pi)/n\xi^s 16^{t/n}$, one eventually arrives at the following expression (we keep the same name for the differential and for the modular form):

$$\omega_{r,s,t} = q^{t/2n} \prod_{m=1}^{\infty} \left(\frac{1-q^{m/2}}{1+q^{m/2}}\right)^4 (1+q^m)^{8(s+2t)/n}(1+q^{m-\frac{1}{2}})^{8(2s+t)/n}\,(\mathrm{d}\tau). \tag{4.39}$$

It would not be difficult to write explicitly the action of the modular group on this basis of holomorphic forms (see below), and this would allow to compare the corresponding periods along a fixed cycle, as was shown using different methods in Section 3. We shall rather examine the similarities and differences between these modular forms for C_n and the characters of the $su(3)$ affine algebra at level $k = n - 3$.

As mentioned earlier, the number of (unrestricted) characters is the same as the number of ω's. The restricted characters however are not linearly independent. Moreover, characters are functions and the differentials on F_n are forms. This is not too serious. One possible remedy is as follows: on F_3 there is only one holomorphic differential, and the corresponding modular form is easily seen to be $\eta^4(\tau)$, whereas the character at height 3 is the constant function 1. However the denominator of the Weyl–Kac character formula is $\eta^8(\tau)$, so that the numerator is naturally a modular form of weight 4, i.e. a quadratic differential. This makes plausible the fact that to find analogies, it is perhaps better to concentrate on the numerators of characters. We shall elaborate a little bit on that at the end of this section.

Observe that $\omega_{r,s,t}$ does not change if one multiplies r, s, t and n by a common factor (this is clearly related to the map h_m from F_{mn} to F_n), but this property is not shared by the characters (though the alcôve B_n is properly embedded in B_{mn}). However we have seen in Section 2 that the numerators of characters satisfy more involved identities of the same kind having a similar origin.

One might be tempted to see another common point in the fact that both sets carry a representation of the modular group for which only a finite quotient acts, and which is in general highly reducible. For the characters, this is a well known fact. For the holomorphic differentials on F_n, it is related to the regularity of the triangulation induced by the map h_n. However the two representations are very different. From the above formulas, one obtains the modular transformations of (4.39)

$$\omega_{r,s,t}(\tau+1) = \xi^t\,\omega_{s,r,t}(\tau), \qquad \omega_{r,s,t}(-1/\tau) = -\tau^2 16^{(r-t)/n}\,\omega_{t,s,r}(\tau). \tag{4.40}$$

Thus for the holomorphic differentials on F_n, the modular group merely permutes r, s and t and multiplies by phases. This is in striking contrast with the modular transformations of the characters.

One can nevertheless try to push the analogy with the affine $su(3)$ characters by looking at the modular problem for the differentials on F_n. So we set $\tilde{\chi}_{r,s,t} = \omega_{r,s,t}/\omega_{1,1,1}$. The $\tilde{\chi}$ carry a (non-unitary) representation of $PSL_2(\mathbb{Z})$, and we can look for the modular invariant sesquilinear forms in the $\tilde{\chi}$. It turns out to be much easier than the corresponding affine modular problem.

Let N be the matrix specifying a Fermat modular invariant. That it commute with T and S implies, respectively,

$$N_{r,s,t;r',s',t'} = \xi^{t-t'} N_{s,r,t;s',r',t'}, \tag{4.41}$$

$$N_{r,s,t;r',s',t'} = 16^{(r+r'-t-t')/n} N_{t,s,r;t',s',r'}. \tag{4.42}$$

Requiring that the entries of N be positive integers, Eq. (4.41) yields $N_{r,s,t;r',s',t'} = 0$ if $t \neq t'$. If $N_{r,s,t;r',s',t'} \neq 0$, then (4.42) implies $r = r'$ hence $s = s'$, so that only the diagonal couplings $N_{r,s,t} \equiv N_{r,s,t;r,s,t}$ may be non-zero. They must satisfy

$$N_{r,s,t} = N_{s,r,t}, \quad \text{and} \quad N_{r,s,t} = 2^{8(r-t)/n} N_{t,s,r}. \tag{4.43}$$

These conditions mean one can look at the six permutations of (r, s, t) independently of the other triplets, and also that, up to a normalization factor, the modular invariants involving the six permutations is unique. The integrality conditions imply $8r = 8s = 8t \bmod n$, and one finds, assuming $r \leq s \leq t$, that the unique modular invariants reads

$$\begin{aligned} Z_{r,s,t}(F_n) = {} & |\tilde{\chi}_{r,s,t}|^2 + |\tilde{\chi}_{s,r,t}|^2 + 2^{8(t-r)/n} |\tilde{\chi}_{t,s,r}|^2 + 2^{8(t-r)/n} |\tilde{\chi}_{s,t,r}|^2 \\ & + 2^{8(t-s)/n} |\tilde{\chi}_{t,r,s}|^2 + 2^{8(t-s)/n} |\tilde{\chi}_{r,t,s}|^2. \end{aligned} \tag{4.44}$$

Using $r + s + t = n$, the integrality conditions imply $24r = 24s = 24t = 0 \bmod n$. If r, s, t have a common factor, say d, then $\omega_{r,s,t}$ descends to the differential $\omega_{r/d,s/d,t/d}$ on $F_{n/d}$, whereas if $\gcd(r, s, t) = 1$, then n must divide 24.

Thus the analogy between the two modular problems is somewhat disappointing, but there is still a curious fact. The coefficients of the q-expansion of the characters are integers. This is in general not true for the holomorphic differentials on F_n, and in fact happens quite seldom. From our explicit formula, the q-expansion of $\omega_{r,s,t}$ has integer coefficients (or even bounded denominators, which is a normalization invariant statement) if and only if $8(s + 2t)$ and $8(2s + t)$ are both multiples of n. It is then not difficult to make a catalog of all triplets satisfying these conditions. If we assume, without loss of generality, that $\gcd(r, s, t) = 1$, one finds the straightforward but puzzling result:

- n is necessarily a divisor of 24;
- the q-expansion of $\tilde{\chi}_{r,s,t}$ contains only integer coefficients if and only if $\tilde{\chi}_{r,s,t}$ appears in a modular invariant for F_n;
- the four exceptional $su(3)$ modular invariant partition functions appearing at height equal to 8, 12 or 24, involve characters labeled by triplets (r, s, t) which all satisfy the above conditions, so that the corresponding forms $\omega_{r,s,t}$ have integer coefficients in their q-expansion. They, however, do not exhaust the list of triplets with this property.

To prove the first two points, one simply notes that $8(s + 2t) = 8(2s + t) = 0 \bmod n$ implies $24r = 24s = 24t = 0 \bmod n$.

4.3. Rational triangular billiards

A (generalized) billiard is a planar domain with piecewise smooth boundary. A classical particle moving in such a domain is simply reflected when it hits the boundary, but moves freely otherwise. The spectrum of the corresponding quantum mechanical system is related to the Dirichlet problem for the Laplace operator. The general case can be very complicated. When the domain is a Euclidian triangle with rational angles (in units of π), the classical phase space has an interesting geometric structure: it has a foliation by closed topological surfaces. In fact the leaves have a natural complex structure [42]. We will briefly review this construction. On the way we will see that many quantities we encountered in Section 3 reappear quite naturally. We will then present yet another intriguing relation with the exceptional modular invariants for the $su(3)$ WZNW models.

Naïvely, a point in the classical phase space is a pair $(\boldsymbol{x}, \boldsymbol{p})$ where $\boldsymbol{x}$ is a position (a point of the triangle) and $\boldsymbol{p}$ a momentum (an arbitrary two-dimensional vector). However, to take into account reflections when the particle hits the boundary, the real phase space is a quotient. The points $(\boldsymbol{x}, \boldsymbol{p})$ and $(\boldsymbol{x}', \boldsymbol{p}')$ are identified if $\boldsymbol{x} = \boldsymbol{x}'$ and if $\boldsymbol{p}$ is obtained from $\boldsymbol{p}'$ by a reflection in the edge containing $\boldsymbol{x}$. Then the phase space is a union of triangles, labeled by momenta, with some edges identified. More precisely, let us assume that the angles of the triangle are $\pi r/n$, $\pi s/n$ and $\pi t/n$, with r, s, t, n four strictly positive integers satisfying $r + s + t = n$, and $\gcd(r, s, t) = 1$. Clearly the norm of the momentum is irrelevant so we can focus on its phase, writing $\boldsymbol{p} = p\mathrm{e}^{\mathrm{i}\phi}$. If the triangle lies with its base horizontal, the reflections through the boundaries change ϕ according to

$$\sigma_0 : \phi \longrightarrow -\phi - \frac{2\pi s}{n}, \tag{4.45}$$

$$\sigma_1 : \phi \longrightarrow -\phi + \frac{2\pi r}{n}, \tag{4.46}$$

$$\sigma_\infty : \phi \longrightarrow -\phi. \tag{4.47}$$

Here σ_v denotes the reflection through the boundary opposite to the vertex v, and 0, 1 and ∞ correspond, respectively, to the corners r, s, t. The horizontal base is the edge linking 0 (left corner) to 1 (right corner). Obviously, the momentum of the particle on its trajectory can take $2n$ values (we exclude the momenta leading to singular trajectories in which the particle hits the corners). Thus in phase space, the particle moves on a submanifold consisting of $2n$ copies of the triangle (the billiard), labeled by the values of ϕ (and a value of p), and this gives a foliation of the phase space. Each such submanifold is a compact combinatorial connected surface without boundary. It is a surface without boundary because every edge is common to exactly two triangles, due to the above identification, and it is connected because one can reach every triangle from any other by a series of reflections. The surface would not be compact if some angles were irrational, in which case the leaves of the foliation may well be dense in phase space. From now on we restrict to the rational case.

The combinatorial description of the surface made up of the $2n$ triangles is obviously the same for all initial values of the momentum. The reflection group, generated by σ_0, σ_1 and σ_∞, permutes the triangles that build the surface. This action is nothing but the action of the triangular group as defined in Section 4.1. Our first purpose is to compute the triangular and cartographic groups, and to find an algebraic model for the surface. Set r' (resp. s', t') for the common factor between r (resp. s, t) and n, and write $n = r'r'' = s's'' = t't''$. Let $\mathcal{T}_{r,s,t}$ (or simply $\mathcal{T}$ when no confusion is possible) denote the associated combinatorial surface, which is a generic leaf of the foliation of phase space.

From the action of σ_v, the generators ρ_0, ρ_1, and ρ_∞ are represented on ϕ by a clockwise rotation of angle $2\pi r/n$, $2\pi s/n$ and $2\pi t/n$, respectively. They commute and satisfy $\rho_0^{r''} = \rho_1^{s''} = \rho_\infty^{t''} = 1$. They satisfy other relations as well, as it is clear that the oriented triangular group is isomorphic to $\mathbb{Z}_n$, because, since r, s and t are relatively prime, we can find integers a, b and c such that $ar + bs + ct = 1$, so $\rho_0^a \rho_1^b \rho_\infty^c$ is a rotation of angle $2\pi/n$. One can also check that the triangular group is the dihedral group of order $2n$, and that the $\widehat{D}$ group is

$$\widehat{D}(\mathcal{T}_{r,s,t}) = \begin{cases} \mathbb{Z}_{n/3} \times \mathbb{Z}_n & \text{if } n = r - s = 0 \bmod 3, \\ \mathbb{Z}_n \times \mathbb{Z}_n & \text{otherwise.} \end{cases} \tag{4.48}$$

It is amusing to note that the structure of $\widehat{D}$ is very reminiscent of the complementary series of $su(3)$ modular invariants (also called the D series). Following Section 4.1, one can use these results to uniformize $\mathcal{T}_{r,s,t}$. Let us first compute its genus. The triangulation consists of $2n$ triangles, $3n$ edges, r' vertices of type 0, s' vertices of type 1, and t' vertices of type ∞. Indeed for vertices of type 0 for instance, there are $2r''$, twice the order of ρ_0, triangles that meet at each vertex of type 0 (r'' white and r'' black triangles), so that $2n$ such vertices get identified by groups of $2r''$, leaving $2n/2r'' = r'$ distinct ones. One obtains the Euler characteristic [7]:

$$2 - 2g = r' + s' + t' - n. \tag{4.49}$$

We already know one way to put a complex structure on $\mathcal{T}$ via the construction of Section 4.1. Let us indicate another equivalent way. We represent each Euclidean triangle of $\mathcal{T}$ in the complex z-plane and put the corresponding complex coordinate in the interior of the triangles back on $\mathcal{T}$. Different choices differ by affinities ($z \to az + b$), so that the complex coordinates glue holomorphically along the interior of the edge common to two triangles. It remains to deal with the vertices. Let us choose a vertex v, of type ∞ say. The problem is that at v, $2t''$ triangles meet with an incident angle equal to $\pi t/n$, so that the argument of z changes by a total amount of $2\pi t/t'$. If we assume, possibly after an affinity, that v is at the origin in the complex plane, we can choose $Z = z^{t'/t}$ as a local parameter in the neighborhood of v on $\mathcal{T}$. This parameter glues holomorphically with z away from the vertex. Moreover, the parameters Z of the triangles incident at v glue holomorphically to give a global coordinate in a small neighborhood of v. The other types of vertices are treated in an analogous fashion. That this complex structure coincides with the one given in Section 4.1 is clear. A priori, the Euclidean structure of the triangle is crucial for the mechanical problem, whereas the complex structure may look very artificial. However, the differential $\mathrm{d}z$, which is crucial for the classical motion (away from the boundary, the equation of motion says that the velocity $\dot{z}$ is constant), extends holomorphically on $\mathcal{T}$. Close to a vertex, of type ∞ say, we have $\mathrm{d}z \propto Z^{t/t'-1}\mathrm{d}Z$, so that the extension of $\mathrm{d}z$ has a zero of order $t/t' - 1$. The total number of zeros is thus

$$r'\left(\frac{r}{r'}-1\right)+s'\left(\frac{s}{s'}-1\right)+t'\left(\frac{t}{t'}-1\right), \tag{4.50}$$

which is just the opposite of the Euler characteristic, as was to be expected. We shall see later that the other holomorphic differentials on $\mathcal{T}$ also have a very natural interpretation.

Because the oriented triangular group of $\mathcal{T}$ is Abelian, we know from Section 4.1 that there is a holomorphic map from F_n to the algebraic curve associated with $\mathcal{T}$. Counting the triangles on the two curves, we see that the map is of degree n and that the algebraic curve associated to $\mathcal{T}$ is the quotient of F_n by a subgroup of $\widehat{D}_n$ of order n, which coincides, if $(n,3)=1$ or $r-s \neq 0 \bmod 3$, with the isotropy subgroup of a fixed flag. It is not difficult to see that the group fixing a flag of symbol say $(\infty 01)$ on $\mathcal{T}$ consists of the elements $\mu_0^a\mu_1^b\mu_\infty^c$ where the integers a, b and c satisfy $ar+bs+ct=0 \bmod n$. But we know that on the Fermat curve the corresponding transformation $R_0^aR_1^bR_\infty^c$ is

$$(u;v;w) \quad\longrightarrow\quad (\xi^{2a}u;\xi^{2b}v;\xi^{2c}w). \tag{4.51}$$

In the affine model the action is $x \to \xi^{2(a-c)}x$, and $y \to \xi^{2(b-c)}y$. The most obvious functions, invariant under these substitutions, are $X \equiv x^n$, y^n and $Y \equiv x^ry^s$. The first and third satisfy $Y^n = X^r(1-X)^s$, which is just the equation for $C_{r,s,t}(n)$ defined in Section 3. The map $(X,Y)\in C_{r,s,t}(n) \to X$ has obviously degree n, while $(x,y)\in F_n \to x^n$ has degree n^2. Thus the intermediate map $(x,y)\in F_n \to (x^n, x^ry^s)$ has degree n. This implies that the invariants X and Y form a complete set and that the triangular curve $C_{r,s,t}(n)$ is a (singular) model for the algebraic curve associated to $\mathcal{T}_{r,s,t}$.

The holomorphic differentials on $C_{r,s,t}(n)$ are simply the invariant differentials on F_n. Under $R_0^aR_1^bR_\infty^c$, the differential $\omega_{\tilde{r},\tilde{s},\tilde{t}}$ given by (4.38) picks a factor $\xi^{2(a\tilde{r}+b\tilde{s}+c\tilde{t})}$. For a triplet (a,b,c) satisfying $ar+bs+ct=0 \bmod n$, this factor is 1 if and only if there is an integer $h\in\mathbb{Z}_n$ such that $(\tilde{r},\tilde{s},\tilde{t})=(\langle hr\rangle,\langle hs\rangle,\langle ht\rangle)$ (where as before, $\langle m\rangle$ is the representative of m modulo n in the interval $[0,n-1]$). The number of such h, yielding the number of holomorphic 1–forms on $C_{r,s,t}(n)$, is equal to the genus.

Now let $h\in\mathbb{Z}_n^*$ be such that $\langle hr\rangle+\langle hs\rangle+\langle ht\rangle=n$. The triangular group of $\mathcal{T}_{\langle hr\rangle,\langle hs\rangle,\langle ht\rangle}$ does not depend on h, nor does the description of the complex structure. Hence $C_{r,s,t}(n)$ and $C_{\langle hr\rangle,\langle hs\rangle,\langle ht\rangle}(n)$ are isomorphic. Explicitly, if we write $\langle hr\rangle = hr-\bar{r}n$, $\langle hs\rangle = hs-\bar{s}n$, we have the invertible map $(X,Y)\in C_{r,s,t}(n) \longrightarrow (X, Y^hX^{-\bar{r}}(1-X)^{-\bar{s}}) \in C_{\langle hr\rangle,\langle hs\rangle,\langle ht\rangle}(n)$. Moreover, if $h\in\mathbb{Z}_n$ has a common factor with n, say d, the above map is still defined, but has degree d and the image is $C_{\langle hr\rangle/d,\langle hs\rangle/d,\langle ht\rangle/d}(n/d)$. Although not identical, this is quite reminiscent of Section 3. We can now come to another "coincidence".

We have seen in Section 2 that the parity rule puts severe restrictions on the possible couplings among characters in a modular invariant partition function. This parity rule was expressed in terms of the sets $H_{r,s,t}=\{h\in\mathbb{Z}_n^*\colon \langle hr\rangle+\langle hs\rangle+\langle ht\rangle=n\}$ where (r,s,t) were interpreted as the affine Dynkin labels of integrable weights. Then the characters $\chi_{r,s,t}$ and $\chi_{r',s',t'}$ can be coupled only if $H_{r,s,t}=H_{r',s',t'}$. We have just seen that $H_{r,s,t}$ also

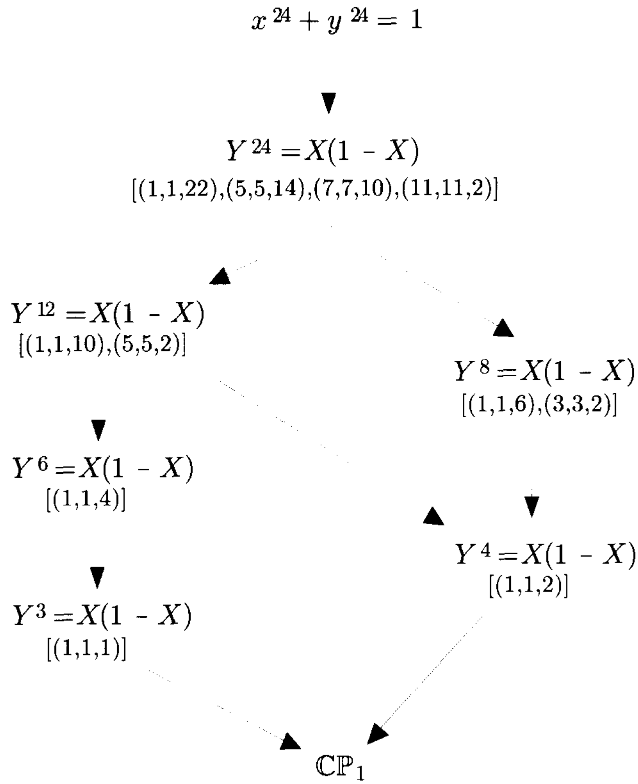

Fig. 3. Triangular curves $C_{1,1,n_0-2}(n_0)$ related to $su(3)$ modular invariants. The top three specify the identity blocks of three exceptional invariants, at height $n_0 = 24$, 12 and 8. The two elliptic curves, corresponding to $(1, 1, 2)$ ($n_0 = 4$) and $(1, 1, 1)$ ($n_0 = 3$), are not isomorphic, having modulus $\tau = i$ and $\tau = e^{2i\pi/3}$, respectively.

describes the billiards that are associated to the same triangular curve $C_{r,s,t}(n)$. But there is a direct and puzzling though incomplete connection between triangular curves and modular invariants, that in addition involves non-invertible elements of $\mathbb{Z}_n$.

We start with F_{24}, the Fermat curve of degree 24. We have seen that F_{24} is a covering of some triangular curves, which themselves are coverings of other triangular curves. Let us first consider the triplet $(1, 1, 22)$, associated with the character of the identity operator at height $n = 24$, and take all its multiples by elements h of $\mathbb{Z}_{24}$. After reduction modulo 24, we keep only those triplets which have no zero component and whose sum is equal to 24, obtaining in this way 11 triplets (or triangles). If one classifies them according to the genus of the associated triangular curve, one finds four triangles of genus 11, two of genus 5, two of genus 3, two of genus 2, and two of genus 1, the last two being associated with two non-isomorphic genus 1 surfaces. Thus there are six different curves which are involved. They are all isomorphic to $C_{1,1,n_0-2}(n_0)$ for some n_0 dividing 24. The six curves are shown in Fig. 3, where the arrows denote covering maps.

The puzzling observation one can make is the following, and concerns the type I exceptional $su(3)$ modular invariants (those which can be written as a sum of squares with only positive coefficients). One observes that the triangles associated with $C_{1,1,n_0-2}(n_0)$ for $n_0 = 24$, 12 and 8 give precisely the content of the block of the identity in the exceptional modular invariant at height n_0. The only element which is not encoded in the picture is whether a character that is labeled by the permutation of a triangle appears or not. More precisely, one sees that:

- For $n_0 = 24$: the four triangles (of genus 11) are $(1, 1, 22)$, $(5, 5, 14)$, $(7, 7, 10)$ and $(11, 11, 2)$. The exceptional invariant at height 24 is

$$E_{24} = |\chi_{(1,1,22)} + \chi_{(5,5,14)} + \chi_{(7,7,10)} + \chi_{(11,11,2)} + \text{all perm.}|^2 + \cdots \tag{4.52}$$

  so all permutations appear.
- For $n_0 = 12$: the two triangles are $(1, 1, 10)$ and $(5, 5, 2)$, and the invariant partition function reads

$$E_{12} = |\chi_{(1,1,10)} + \chi_{(5,5,2)} + \text{all perm.}|^2 + \cdots \tag{4.53}$$

  so again all permutations appear.
- For $n_0 = 8$: there are two triangles, $(1, 1, 6)$ and $(3, 3, 2)$. The partition function reads

$$E_8 = |\chi_{(1,1,6)} + \chi_{(3,3,2)}|^2 + \cdots \tag{4.54}$$

  and the permuted symbols appear in other blocks.

The same pattern persists for the smaller values of n_0: for $n_0 = 6$, the triangle $(1, 1, 4)$ specifies the identity block in the diagonal and complementary invariants depending on whether permutations are included or not, whereas for $n_0 = 4$ and 3, the identity blocks of the diagonal invariants are reproduced. One is tempted to apply the same idea to the other blocks of the exceptional invariants, starting for instance with the triangle $(1, 7, 16)$ appearing in the second block of E_{24}. Alas, the outcome is disappointing, and that is one of the reasons to believe that our observations, however troublesome, are mere coincidences.

5. The Riemann surface of a RCFT on the torus

In this last part, we would like to see to what extent the action of the modular group on the characters of a general rational conformal field theory can be related to its action on algebraic curves, which we might then want to identify. In particular, rational conformal field theories like to organize in families indexed by integers (for example the height in WZNW models), and it is therefore a natural question to ask whether these families can be put in correspondence with families of curves, just like the $su(3)_k$ WZNW models are related to the Fermat curves in the way detailed in the previous sections. We show here that a compact Riemann surface can be canonically associated with any rational conformal field theory. Each such Riemann surface has an algebraic model, but to compute it explicitly turns out to be in practice difficult. Nonetheless general features can be established. We will present the complete details for the $su(3)$ WZNW models, at level $k = 1$ and $k = 2$. The most naïve hope would have been that the associated algebraic curves are the Fermat curves of degree 4 and 5, respectively, but as we shall see, this is not the case. The surprise however is that the curve associated with $su(3)_1$ possesses a covering by the Fermat curve of degree 12, and is nothing but one of the triangular curves.

5.1. General setting

We start with some general facts, which are true for the WZNW models, but that otherwise might well be consequences of the general axioms that a rational conformal field theory has to fulfill. Since we are not aware of a complete derivation of them, we content ourselves with listing them as mere assumptions.

(1) The theory involves only a finite number N of representations of the chiral algebra. We denote them by $\mathcal{R}_p$, $0 \leq p \leq N-1$, with the convention that $\mathcal{R}_0$ contains the identity operator (or the operator of smallest conformal weight in the non-unitary case).

(2) Chiral restricted characters are well defined, that is,

$$\chi_p(\tau) \equiv tr_{\mathcal{R}_p} e^{2i\pi\tau(L_0 - c/24)} \tag{5.1}$$

is holomorphic in the upper-half plane. Two restricted characters are equal if they correspond to complex conjugate representations. These are often the only linear relations among them. [8]

(3) There exist unitary matrices $S_{p,p'}$ (symmetric) and $T_{p,p'}$ (diagonal) such that

$$\chi_p(-1/\tau) = \sum_{p'} S_{p,p'} \chi_{p'}(\tau), \qquad \chi_p(\tau+1) = \sum_{p'} T_{p,p'} \chi_{p'}(\tau). \tag{5.2}$$

They both have finite order and their entries are in a finite Abelian extension of $\mathbb{Q}$ (a simple consequence of [5]). The square of S is the charge conjugation. These matrices yield a representation of $SL_2(\mathbb{Z})$ through the map

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \to S, \qquad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \to T.$$

The restriction of this representation to the subspace of conjugation invariants descends to a representation of $PSL_2(\mathbb{Z})$. This is the subspace we shall be dealing with in the sequel. [9]

(4) The kernel of this representation of $PSL_2(\mathbb{Z})$ (or equivalently of $SL_2(\mathbb{Z})$ for the original representation) is very large [43]. More precisely, the kernel is an invariant subgroup, call it Γ, of finite index in $PSL_2(\mathbb{Z})$. The intuitive reason is that the characters can be written in terms of theta functions of a Euclidean lattice, and that S and T are closely related to the finite Fourier transform on a finite group, namely the quotient of the lattice by a sublattice of finite index. A proof for affine algebras is contained in [9].

---

[8] A counterexample is provided by the affine algebra $\widehat{D}_4$ at $k=1$, where, because of the triality, three inequivalent representations have the same restricted character [9].

[9] When other linear relations among the characters exist, we simply pick a maximal set of linearly independent characters and work with these.

A pedestrian approach in the case of $su(N)_k$ WZNW models, showing that in fact the principal congruence subgroup $\Gamma_{2N(N+k)}$ is in the kernel, can be found in [22]. A general and more conceptual proof, starting from axiomatics of rational conformal field theory, would be very interesting.

These assumptions lead naturally to the following construction. The kernel Γ is a Fuchsian group, and the quotient of the upper-half plane $\mathfrak{H}$ by Γ defines a Riemann surface Σ with punctures, which has a well defined compactification $\overline{\Sigma}$. The surface Σ may be described as the union of $\widehat{\gamma}F$ for all $\widehat{\gamma} \in \widehat{\Gamma} \equiv PSL_2(\mathbb{Z})/\Gamma$, where F is a fundamental domain for $\mathfrak{H}/PSL_2(\mathbb{Z})$, for instance

$$F = \{\tau \in \mathfrak{H}: |\tau| \geq 1 \text{ and } |\mathrm{Re}\,\tau| \leq \tfrac{1}{2}\}. \tag{5.3}$$

Σ has punctures located at the images of $\tau = i\infty$ under $\widehat{\Gamma}$. When one compactifies Σ by filling these punctures, one gets the compact surface $\overline{\Sigma}$, of which a triangulation is given by $\{\widehat{\gamma}F: \widehat{\gamma} \in \widehat{\Gamma}\}$ where those edges and vertices equivalent under Γ are to be identified.

In the rest of this section, we will consider in more detail the association RCFT $\longrightarrow$ compact Riemann surface $\overline{\Sigma}$. [10] More specifically, one would like to answer three questions:

- What general features do these Riemann surfaces have?
- How explicitly can we describe them, for instance by giving equations for an embedding in some affine or projective space?
- Is there some nice way to characterize the family of Riemann surfaces that arise in this way from rational conformal field theories?

Although we have not been able to answer the third question, we can nevertheless make definite statements about these surfaces. Useful references for quotients of $\mathfrak{H}$ by Fuchsian groups are [44,45].

As Γ is an invariant subgroup of $PSL_2(\mathbb{Z})$, we can draw general conclusions about the quotient $\mathfrak{H}/\Gamma$. The projection $\mathfrak{H}/\Gamma = \Sigma \longrightarrow \mathfrak{H}/PSL_2(\mathbb{Z}) \cong \mathbb{C}$ – this last equivalence being via the standard modular function $j(\tau)$ – has a holomorphic extension $\overline{\Sigma} \longrightarrow \mathbb{CP}_1$, ramified only at 0, 1728 and ∞. [11] The group $PSL_2(\mathbb{Z})$ has unique invariant subgroups of index 1, 2 (related to the fact that $j - 12^3 = 216^2 g_3^2/\eta^{24} \equiv j_{1/2}^2$ is a perfect square, the q-expansion of $j_{1/2}$ starting as $q^{-1/2}$) and 3 (related this time to the fact that $j = 12^3 g_2^3/\eta^{24} \equiv j_{1/3}^3$ is a perfect cube, [12] the q-expansion of $j_{1/3}$ starting as $q^{-1/3}$). The associated compact Riemann surfaces have genus 0. If the index $|\widehat{\Gamma}|$ is larger or equal to 4,

---

[10] Because $\overline{\Sigma}$ is defined from the representation carried by the full set of independent characters, we could say that it is the surface associated with the diagonal RCFT. In the same way, one can associate Riemann surfaces to subrepresentations corresponding to non-diagonal theories.

[11] At this point, it would be easy to make contact with the formalism of triangulations briefly presented in Section 4.1. However, starting from the projection $\overline{\Sigma} \to \mathbb{CP}_1$, the algorithm described in Section 4 would construct Σ', a quotient of $\mathfrak{H}$ by a subgroup of Γ_2 with more punctures than Σ, but of course such that $\overline{\Sigma} = \overline{\Sigma}'$. In particular the cartographic group is closely related, but not equal, to $PSL_2(\mathbb{Z})/\Gamma$. But other meromorphic functions ramified only over three points can be used to do cartography. This relationship with triangulations will be explicited in a specific example, in Section 5.2.

[12] $j_{1/3}$ is the character of the only representation of $\widehat{E}_8$, level 1.

the ramification structure of the projection map $\overline{\Sigma} \to \mathbb{CP}_1$ is fixed: the ramification index is 2 above $j = 1728$, 3 above $j = 0$ and n_∞ (the order of T in $\widehat{\Gamma}$) above $j = \infty$. This implies that the Euler characteristic of $\overline{\Sigma}$ is

$$2 - 2g_{\overline{\Sigma}} = |\widehat{\Gamma}| \frac{6 - n_\infty}{6n_\infty}. \tag{5.4}$$

The number of punctures (or cusps) is equal to $|\widehat{\Gamma}|/n_\infty$. Let us describe in some detail the easiest cases, namely the surfaces of genus 0 and 1.

If $|\widehat{\Gamma}| \geq 4$ and $g_{\overline{\Sigma}} = 0$, there are four possibilities (platonic solids): $n_\infty = 2$, $|\widehat{\Gamma}| = 6$ (the dihedral group of order 3, $\Gamma = \Gamma_2$); $n_\infty = 3$, $|\widehat{\Gamma}| = 12$ (the symmetry group of the tetrahedron $\Gamma = \Gamma_3$); $n_\infty = 4$, $|\widehat{\Gamma}| = 24$ (the symmetry group of the octahedron $\Gamma = \Gamma_4$) and $n_\infty = 5$, $|\widehat{\Gamma}| = 60$ (the symmetry group of the icosahedron $\Gamma = \Gamma_5$).

If $n_\infty = 6$, the resulting quotient is a torus, and there is now an infinite sequence of nested invariant subgroups Λ_n of $PSL_2(\mathbb{Z})$ containing T^6 and of finite index. We denote the corresponding quotients by $\widehat{\Lambda}_n$, $n = 1, 2, 3, \ldots$ Let us start with the smallest one, $\widehat{\Lambda}_1$, which is the quotient of $PSL_2(\mathbb{Z})$ by its commutator subgroup $PSL_2(\mathbb{Z})^{\mathrm{comm}}$. It has order 6, and is isomorphic to the cyclic group $\mathbb{Z}_6$ (a simple consequence of $S^2 = (ST)^3 = 1$ plus $ST = TS$). Both $j_{1/2}$, the square root of $j - 12^3$, and $j_{1/3}$, the cubic root of j, carry a one-dimensional (hence Abelian) representation of $PSL_2(\mathbb{Z})$, and they generate the function field of the quotient $\mathfrak{H}/PSL_2(\mathbb{Z})^{\mathrm{comm}}$. This algebraic curve is, as announced, a torus since $j_{1/2}^2 = j_{1/3}^3 - 12^3$. It is isomorphic to the cubic Fermat curve, although its uniformization by $j_{1/2}$ and $j_{1/3}$ is not the one we gave earlier. The other $\widehat{\Lambda}_n$ can be constructed as quotient groups of their projective limit $\widehat{\Lambda}_\infty$.

$\widehat{\Lambda}_\infty$ is the largest factor group with $n_\infty = 6$, and by definition is the quotient of $PSL_2(\mathbb{Z})$ by the smallest invariant subgroup containing T^6. It thus has the presentation $\langle S, T \mid S^2, (ST)^3, T^6 \rangle$, is of infinite order, and is isomorphic to the cartographic and symmetry group of the regular triangulation of the plane. To see this concretely, set $\rho = \mathrm{e}^{\mathrm{i}\pi/3}$, and let s and t be the Euclidean transformations of the complex plane given by $s : z \to 1 - z$ and $t : z \to \rho z$. Then obviously $s^2 = t^6 = 1$, and one checks that $(st)^3 = 1$ as well. So the group generated by s and t is a quotient of $\widehat{\Lambda}_\infty$. The transformation $a = st^3$ is simply the translation $z \to z + 1$, and conjugating by t, we find that $b = tst^2$ is the translation $z \to z + \rho$. Further conjugations by t give unit translations along the other axes of the lattice generated by 1 and ρ. So the group generated by s and t is the semi-direct product of the translations of the lattice and the rotations generated by t, that is, the full symmetry group of the lattice. On the other hand one can check explicitly that in $\widehat{\Lambda}_\infty$, $A = ST^3$ and $B = TST^2$ commute. As a consequence, any element of $\widehat{\Lambda}_\infty$ can be written in a unique way as $T^j A^p B^q$ with j between 0 and 5, and p and q in $\mathbb{Z}$. Indeed we first check that $S = T^3 A^{-1}$, $ST = T^4 A^{-1} B$, $ST^2 = T^5 B$, $ST^3 = A$, $ST^4 = TAB^{-1}$ and $ST^5 = T^2 B^{-1}$. Using these, one checks that the set of elements of $\widehat{\Lambda}_\infty$ that have a decomposition $T^j A^p B^q$ contains 1, is stable under multiplication on the left and on the right by T and S, so that this set is $\widehat{\Lambda}_\infty$. The decomposition is unique because the corresponding decomposition in the group generated by s and t, a priori a quotient of $\widehat{\Lambda}_\infty$, is well known to be unique.

Now for finite n, $\widehat{\Lambda}_n$ is the quotient of $\widehat{\Lambda}_\infty$ by the further relation $A^n = 1$ (or equivalently $B^n = 1$), and has the presentation

$$\widehat{\Lambda}_n = \langle S, T \mid S^2, (ST)^3, T^6, (ST^3)^n \rangle. \tag{5.5}$$

The order of $\widehat{\Lambda}_n$ is $6n^2$. The corresponding Riemann surfaces $\mathfrak{H}/\Lambda_n$ are all isomorphic to the cubic Fermat curve F_3 (with the torsion points of order n as punctures). This is because T induces a cyclic group of automorphisms of order 6 of the associated torus, fixing a point (the coset of the point at infinity in $\mathfrak{H}$). For $n = 3$, the uniformization of F_3 by $\mathfrak{H}/\Lambda_3 = \mathfrak{H}/C_3$ is the one we gave earlier in Section 4.2.

The $\widehat{\Lambda}_n, n \geq 1$, do not exhaust all factor groups of $PSL_2(\mathbb{Z})$ of finite order with $n_\infty = 6$, but all of them are factor groups of the $\widehat{\Lambda}_n$. For instance, quotienting $\widehat{\Lambda}_\infty$ by the relation $AB = 1$ – it implies $A^3 = 1$ –, one obtains a group of order 18 which is $\widehat{\Lambda}_3/\langle ST^2ST^{-2}\rangle$.

Another common feature of all the Riemann surfaces arising from our construction is that they have a rather large group of automorphisms. This group contains $\widehat{\Gamma}$, but in fact, unless $\overline{\Sigma}$ is a sphere or a torus (in which case the automorphism group is infinite), $\widehat{\Gamma}$ is the full automorphism group of $\overline{\Sigma}$. That $\widehat{\Gamma}$ is the group of automorphisms of Σ is the consequence of a general result (see for instance [45]), and the statement relative to the compact surface $\overline{\Sigma}$ is proved in Appendix A.

We now come to the question of the explicit and concrete description of $\overline{\Sigma}$, by means of algebraic equations. We do this by looking at the function field of $\overline{\Sigma}$.

The restricted characters are holomorphic on Σ, and meromorphic on $\overline{\Sigma}$. This is proved by a simple analysis of their behavior at the punctures. Characters are meromorphic at the infinite parabolic point because the eigenvalues of L_0 in the representations of the chiral algebra are rational and bounded below. To conclude for another puncture (necessarily a rational point on the real axis), one chooses an element g of $PSL_2(\mathbb{Z})$ that maps it to $\tau = \mathrm{i}\infty$ and use the fact that $PSL_2(\mathbb{Z})$ acts linearly on the characters. This shows that the singularity of χ_p at a puncture is at most as strong as the singularity of χ_0 at $\tau = \mathrm{i}\infty$. It is weaker if the matrix element of g between χ_p and χ_0 vanishes. This proof parallels the argument showing that $S_{0,p}$ is real positive for any p.

The function field $\mathcal{M}$ of $\overline{\Sigma}$ certainly contains all rational functions of the characters χ_p and of the modular invariant j. That it contains nothing more can be proved in the following way. A classical theorem states that, given a non-constant meromorphic function f on $\overline{\Sigma}$ of degree d, the function field $\mathcal{M}$ is a simple Galois extension of $\mathbb{C}(f)$ of degree d [46]. That is, there exists a function g satisfying an irreducible polynomial equation of degree d with coefficients in $\mathbb{C}(f)$, in terms of which $\mathcal{M} = \mathbb{C}(f)(g) = \mathbb{C}(f, g)$. Choosing $f = j(\tau)$, of degree $|\widehat{\Gamma}|$ shows that $\mathcal{M}$ is a Galois extension of degree $|\widehat{\Gamma}|$ of $\mathbb{C}(j)$, with Galois group $\mathrm{Gal}(\mathcal{M}/\mathbb{C}(j)) = \widehat{\Gamma}$. Now $\widehat{\Gamma}$ acts linearly on the characters, and induces distinct automorphisms of the field $\mathcal{M}_\chi$ generated by the χ's and j, that all fix $\mathbb{C}(j)$. This implies that $\mathcal{M}_\chi$ is a subfield of $\mathcal{M}$ of degree $|\widehat{\Gamma}|$ over $\mathbb{C}(j)$, hence equal to $\mathcal{M}$.

Thus we have $\mathcal{M} = \mathcal{M}_\chi = \mathbb{C}(\chi_0, \chi_1, \ldots, \chi_{N-1}, j)$, but since it is also equal to $\mathbb{C}(j, g)$ for some g, the field is not freely generated by the characters and j. Let us consider the set $I_{\overline{\Sigma}}$ of all polynomial relations $P(\chi_0, \ldots, \chi_{N-1}, j) = 0$. It is fixed by $\widehat{\Gamma}$ since $\widehat{\Gamma}$ acts by automorphisms of $\mathbb{C}(\chi_0, \ldots, \chi_{N-1}, j)$. Moreover, any polynomial $P(\chi_0, \chi_1, \ldots, \chi_{N-1})$

invariant under the action of $\widehat{\Gamma}$ on characters is a modular invariant function of τ, holomorphic in the upper-half plane without poles at finite distance, so a polynomial in j, say $Q(j)$. Hence

$$P(\chi_0, \chi_1, \ldots, \chi_{N-1}) - Q(j) = 0 \tag{5.6}$$

and this yields an element of $I_{\overline{\Sigma}}$.[13]

Every relation of $I_{\overline{\Sigma}}$ gives an equation for $\overline{\Sigma}$. More precisely, the locus in $\mathbb{C}^{N+1}$ where all relations are satisfied is (by definition) an algebraic variety, and evaluation of $\chi_0, \ldots, \chi_{N-1}$ and j gives a holomorphic map from $\overline{\Sigma}$ into this variety, injective except perhaps at a finite number of points. But in fact the elements of $I_{\overline{\Sigma}}$ corresponding to invariants under $\widehat{\Gamma}$ (of the form (5.6)) give a complete set of equations for $\overline{\Sigma}$, because they describe a covering of the j-sphere containing the model for $\overline{\Sigma}$ with at most $|\widehat{\Gamma}|$ leaves. Indeed for every value of j, we get a value for the invariants P_i, and we know from invariant theory [48] that there are at most $|\widehat{\Gamma}|$ points in $\mathbb{C}^N$ corresponding to these values (namely the points in an orbit). Hence this covering is an affine model for $\overline{\Sigma}$. Let us also observe that this affine model is well suited to deal with questions concerning the values characters can take. For instance, the divisors of the characters (namely the zeros and the poles) are nicely encoded.

From the set of equations (5.6) (for all $\widehat{\Gamma}$-invariant polynomials P), elimination leads to irreducible polynomial relations between every single character and j. One easily sees that, if Δ_p denotes the stabilizer of χ_p in $\widehat{\Gamma}$, these equations take the form

$$\prod_{\widehat{\gamma} \in \widehat{\Gamma}/\Delta_p} (X - \widehat{\gamma}\chi_p) = 0. \tag{5.7}$$

The coefficients of this monic equation are polynomials in j, since they are symmetric functions of the roots, which are themselves linear combinations of the characters, holomorphic in $\mathfrak{H}$. Loosely speaking, this means that the characters are algebraic integers over $\mathbb{Q}(j)$.

In fact these arguments also solve the problem of the "second generator" of the function field $\mathcal{M}$, and provide another model for $\overline{\Sigma}$. Since the matrices S and T generate a finite group of order $|\widehat{\Gamma}|$, we can find a linear combination $g = \sum_p c_p \chi_p$ of the characters such that its orbit under $\widehat{\Gamma}$ is of cardinal $|\widehat{\Gamma}|$. From this follows that g satisfies the irreducible polynomial equation:

$$\prod_{\widehat{\gamma} \in \widehat{\Gamma}} (X - \widehat{\gamma} g) = 0. \tag{5.8}$$

As before the coefficients of X^k are polynomials in j. The simple extension of $\mathbb{C}(j)$ obtained by adding g and its powers is of degree $|\widehat{\Gamma}|$, and is therefore equal to the whole of the function field $\mathcal{M} = \mathbb{C}(j, g)$. Eq. (5.8) is a plane curve that is a (highly) singular model for $\overline{\Sigma}$.

Finally let us comment about some automorphisms of $\widehat{\Gamma}$. Set $M_{\text{restr}} = \mathbb{Q}(S^{\text{restr}}_{p,p'}, T_{p,p'})$, the algebraic extension generated by the matrix elements of T and S, *acting on the inde-*

[13] As mentioned before, it can be useful to deal with the numerators of characters rather than with the characters themselves. One way to do it is to look at the ring of projective invariants (invariants up to a phase for the action of $\widehat{\Gamma}$ on characters). Those are polynomials in $j_{1/2}$ and $j_{1/3}$.

pendent restricted characters. We want to show that the Galois group $\mathrm{Gal}(M_{\mathrm{restr}}/\mathbb{Q})$ acts as automorphisms of $\widehat{\Gamma}$. This is obvious for T, because for every Galois transformation, $\sigma(T) = T^h$ for an integer h coprime with n_∞, the order of T. That $\sigma(S)$ is also a word in T and S is less trivial, but can be seen as follows.

First we show that the ideal $I_{\overline{\Sigma}}$ can be generated by polynomials with integral coefficients. In the language of algebraic geometry, this says that $\overline{\Sigma}$ is defined over $\mathbb{Q}$, a property shared with the Fermat curves. The point is that the insertion of the Puiseux series for χ_p and j – they all have integral coefficients – in a polynomial $P(\chi_0, \ldots, \chi_{N-1}, j)$ shows that the condition for P to belong to $I_{\overline{\Sigma}}$ is expressed by a linear system with integral entries, the unknowns being the coefficients of P. We can therefore choose a basis of solutions with integral or rational coefficients. We call it an integral basis.

For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we extend the action of σ on polynomials by acting trivially on the characters and j. Now let P be a polynomial in $I_{\overline{\Sigma}}$ with integral coefficients and X be an element of $\widehat{\Gamma}$ (for instance S). We make the following observations. First $P(\sigma(X) \cdot \chi, j) = \sigma(P(X \cdot \chi, j))$ because P has integral coefficients. But $P(X \cdot \chi, j) = P(X \cdot \chi, X \cdot j)$ because j is invariant under $\widehat{\Gamma}$. Next $P(X \cdot \chi, X \cdot j)(\tau) = P(\chi, j)(X\tau)$ which is identically 0 because $P(\chi, j)$ belongs to $I_{\overline{\Sigma}}$. Hence $P(X \cdot \chi, j)$ belongs to $I_{\overline{\Sigma}}$, and can be expressed as a linear combination (with complex coefficients) of elements of an integral basis for $I_{\overline{\Sigma}}$. The Galois transformation σ acts trivially on the integral basis, so that $P(\sigma(X) \cdot \chi, j) = \sigma(P(X \cdot \chi, j))$ is in $I_{\overline{\Sigma}}$ as well. This means that $\sigma(X)$, a linear transformation of the characters, induces an automorphism of Σ fixing j. The proof is finished since $\widehat{\Gamma}$ is the set of all such automorphisms. This proves at the same time that the extension M_{restr} of $\mathbb{Q}$ is a Galois extension, as already known from [5].

When S and T correspond to the modular transformations of affine characters, one can be more explicit. As mentioned above, there is a principal congruence subgroup, say Γ_N, in the kernel of the representation generated by S and T, so that they form a representation of $PSL_2(\mathbb{Z}_N)$, for some N. In this case, it is conjectured (and shown for large families of examples) that the cyclotomic Galois transformation σ_h acts on S by multiplication by the matrix representing the group element

$$\begin{pmatrix} h & 0 \\ 0 & h^{-1} \end{pmatrix}$$

of $PSL_2(\mathbb{Z}_N)$ (thus h^{-1} is the inverse of h modulo N) [47]. This result implies the following action of σ_h on S:

$$\sigma_h(S) = ST^{h^{-1}}ST^hST^{h^{-1}}S. \tag{5.9}$$

Illustrations of this formula are given in Section 5.2 and in Appendix B.

5.2. The Riemann surface of su(3) level 1

We could illustrate the machinery of the previous section on various rational conformal field theories, but as $su(3)$ was central in our previous investigations, we shall give here the complete treatment of $su(3)$ at level 1, relegating to an appendix the case of $su(3)$, level

2, already much more complex. It will soon become clear that explicit computations of the Riemann surface of a rational conformal field theory tend to be painful. To compute even the genus of the surface is quite a challenge, since most of the time very little is known about the finite group S and T generate.

The affine Lie algebra $\widehat{su(3)}_1$ has three integrable representations, corresponding to the shifted weights $(1, 1)$, $(1, 2)$ and $(2, 1)$. To simplify the notations, we denote the three independent characters as $\chi_0 \equiv \chi_{(1,1)}$, $\chi_1 \equiv \chi_{(1,2)}$, $\chi_2 \equiv \chi_{(2,1)}$. Setting $\xi = e^{2i\pi/12}$ and $\omega = e^{2i\pi/3}$, the expressions for S and T in the basis (χ_0, χ_1, χ_2) are

$$S = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \qquad T = \begin{pmatrix} \xi^{-1} & 0 & 0 \\ 0 & \xi^3 & 0 \\ 0 & 0 & \xi^3 \end{pmatrix}. \tag{5.10}$$

The restricted characters χ_1 and χ_2 being equal, we are left with a two-dimensional representation of the modular group, given in the basis $(\chi_0, \frac{1}{2}(\chi_1 + \chi_2))$ by

$$S = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix}, \qquad T = \begin{pmatrix} \xi^{-1} & 0 \\ 0 & \xi^3 \end{pmatrix}. \tag{5.11}$$

The extension defined in the previous section is clearly $M_{\mathrm{restr}} = \mathbb{Q}(\xi)$, with Galois group over $\mathbb{Q}$ isomorphic to $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$. One easily obtains its action on $\widehat{\Gamma}$: $\sigma_5(S, T) = (ST^6, T^5)$, $\sigma_7(S, T) = (S, T^7)$ and $\sigma_{11}(S, T) = (ST^6, T^{11})$, in agreement with the general formula (5.9).

Finally the Weyl–Kac formula gives the following Puiseux series for the restricted characters:

$$\chi_0 = q^{-1/12}[1 + 8q + 17q^2 + 46q^3 + 98q^4 + \cdots], \tag{5.12}$$

$$\chi_1 = q^{1/4}[3 + 9q + 27q^2 + 57q^3 + 126q^4 + \cdots]. \tag{5.13}$$

As before, let Γ be the kernel (in $PSL_2(\mathbb{Z})$) of the representation (5.11) and $\widehat{\Gamma}$ be the corresponding quotient. Let us recall that our main interest is the study of the Riemann surface with punctures $\Sigma = \mathfrak{H}/\Gamma$ and the corresponding compact surface $\overline{\Sigma}$. Our first task is to compute the order of $\widehat{\Gamma}$.

It is quite clear that T has order 12 in $\widehat{\Gamma}$, but one can also observe that T^3 is central, namely it commutes with S. Consequently $\widehat{\Gamma}$ is a quotient group of $\tilde{\Gamma} = \langle S, T \mid S^2, (ST)^3, T^{12}, ST^3\, ST^{-3} \rangle$. The tetrahedron group $\Gamma_3 = \langle S, T \mid S^2, (ST)^3, T^3 \rangle$, of order 12, is itself a quotient group of $\tilde{\Gamma}$ by the cyclic subgroup generated by T^3. Since T^3 is of order 4 in $\tilde{\Gamma}$, it follows that $|\tilde{\Gamma}| = 48$. On the other hand, the elements T^i and ST^i for $0 \le i \le 11$ are all distinct in $\widehat{\Gamma}$ because S is not a power of T (its matrix representation is not diagonal). Moreover $STS = T^{-1}ST^{-1}$ gives still a distinct element, because $T^{-1}ST^{-1}$ is not a power of T, and STS is not equal to S times a power of T. Thus $|\widehat{\Gamma}| > 24$, which implies $\widehat{\Gamma} = \tilde{\Gamma}$ (since the order of $\widehat{\Gamma}$ must divide that of $\tilde{\Gamma}$). The genus of $\overline{\Sigma}$ is then given by (5.4), which yields $g = 3$ (same genus as the Fermat curve F_4). The number of punctures of Σ is $|\widehat{\Gamma}|/n_\infty = \frac{48}{12} = 4$.

As we have seen in the previous section, invariant theory for the two-dimensional representation of $\widehat{\Gamma}$ on characters will give us a description of $\overline{\Sigma}$. Invariants for finite groups can be computed in a systematic way, but the procedure is generally cumbersome, so that it may be more efficient to find shortcuts based on geometrical insights. We used both to obtain the following results (as well as those of Appendix B).

The generating function for the number of invariants of degree n, call it d_n, under the representation (5.11) of $\widehat{\Gamma}$ is given by the Molien series [48]:

$$F(t) = \sum_{n=0}^{\infty} d_n t^n = \frac{1}{|\widehat{\Gamma}|} \sum_{\widehat{\gamma}\in\widehat{\Gamma}} \frac{1}{\det(1 - t\widehat{\gamma})} = \frac{1}{(1-t^4)(1-t^{12})}. \tag{5.14}$$

The ring of invariants is freely generated [14] by two algebraically independent invariants, of degree 4 and 12, which one can choose as

$$P_4(\chi_0, \chi_1) = \chi_0^3\chi_1 - \chi_1^4 = 3, \tag{5.15}$$

$$P_{12}(\chi_0, \chi_1) = [\chi_0^4 + 8\chi_0\chi_1^3]^3 = j. \tag{5.16}$$

As mentioned before, these invariants are modular invariant functions of τ, holomorphic in $\mathfrak{H}$, that are determined from the Puiseux series of χ_0 and χ_1 by looking at the singular terms in q.

The first invariant (5.15) alone yields a plane curve which is a non-singular model for the Riemann surface associated with the affine model $su(3)$ at level 1:

$$x^3y - y^4 = 3z^4. \tag{5.17}$$

Being smooth of degree 4, its genus is equal to 3, as expected. The second invariant (5.16) gives $\overline{\Sigma}$ as a covering of the j-sphere of degree 48, and allows to compute the divisors of the two restricted characters. In terms of the projective coordinates $(x; y; z)$, χ_0 has four simple zeros located at $(0; y_0; 1)$ with $y_0^4 = -3$ (where $j = 0$), and four simple poles at $(1; 0; 0)$ and $(\omega^k; 1; 0)$ for $k = 0, 1, 2$. Similarly χ_1 has a triple zero at $(1; 0; 0)$ and three simple poles at $(\omega^k; 1; 0)$ for $k = 0, 1, 2$. In particular, χ_0 and χ_1 are of degree 4 and 3, respectively.

It is not difficult to obtain the polynomial equations relating the characters to j, as in (5.7). The stabilizer of χ_1 in $\widehat{\Gamma}$ is of order 3 ($T^4\chi_1 = \chi_1$), so that the irreducible equation relating χ_1 to j is of degree 16, but easily seen to be of degree 4 in χ_1^4 because $\chi_1, \xi^3\chi_1, \xi^6\chi_1$ and $\xi^9\chi_1$ all solve the same equation. The coefficients of the polynomial are easily determined from the Puiseux series of χ_1, and one finds

$$(1 + 3X^4)^3(3 + X^4) - \tfrac{1}{27} jX^4 = 0. \tag{5.18}$$

So $\mathbb{C}(j, \chi_1) = \mathbb{C}(\chi_1)$ is a genus zero algebraic extension of $\mathbb{C}(j)$ of degree 16. However, this extension is not Galois, and the Galois closure defines an algebraic extension of $\mathbb{C}(j)$

[14] An n-dimensional representation of a finite group gives rise to a ring of invariants which is freely generated by algebraically independent invariants iff the group is generated by pseudo-reflections in an n-dimensional complex space [49]. This last paper establishes the classification of such groups. The list, containing 37 entries, can also be found in [48].

of degree 48, isomorphic to the function field of $\overline{\Sigma}$. The other character χ_0 has a trivial stabilizer, and therefore generates, along with j, the function field of $\overline{\Sigma}$. It satisfies a polynomial equation of degree 48, this time of degree 4 in χ_0^{12} (same reason as above), but more complicated:

$$X^{48} + \frac{4(27\,648 - 61j)}{243}X^{36} + \frac{2(6\,115\,295\,232 + 16\,809\,984j + 365j^2)}{177\,147}X^{24} + \frac{4(338\,151\,365\,148\,672 - 256\,842\,399\,744j + 42\,633\,216j^2 - 547j^3)}{387\,420\,489}X^{12} + \frac{j^4}{387\,420\,489} = 0. \tag{5.19}$$

This defines the function field of $\overline{\Sigma}$ as the simple extension $\mathbb{C}(j, \chi_0)$, and provides another projective model for $\overline{\Sigma}$, this time very singular.

It remains to show that $\overline{\Sigma}$ is distinct from the Fermat curve F_4. This one can do by decomposing the Jacobian of $\overline{\Sigma}$, and by proving that it splits into two elliptic curves with modular invariant $j = 1728$, and one elliptic curve with invariant $j = 0$. This will definitely establish the non-isomorphism of $\overline{\Sigma}$ with F_4 since the latter is isogenous to the cube of the elliptic curve with invariant $j = 1728$.

There are many ways to show the decomposition of the Jacobian of $\overline{\Sigma}$, but an instructive one is to resort to yet another algebraic model of the surface, which is in itself interesting since it turns out to be one of the curves we discussed in Section 4.3, in relation with rational billiards. The idea is precisely to use the cartographic machinery. Our general discussion showed that $\overline{\Sigma}$ is defined over $\mathbb{Q}$ (as is confirmed by (5.17)), so that it can be realized as a covering of the Riemann sphere, ramified over three points. A possible choice is the following. Corresponding to $y = 0$, there is one "point at infinity", namely $(x; y; z) = (1; 0; 0)$, while away from $y = 0$, one sets $x^3 = ty^3$ and $3z^4 = (t - 1)y^4$, so that altogether

$$(x; y; z) = \begin{cases} \left(\zeta_3^k \sqrt[3]{t}\,;\ 1\,;\ \zeta_4^\ell \sqrt[4]{\frac{t-1}{3}}\right) & \text{for } t \neq \infty,\ 1 \leq k \leq 3,\ 1 \leq \ell \leq 4, \\ (1; 0; 0) & \text{fot } t = \infty. \end{cases} \tag{5.20}$$

It yields a covering of degree 12, ramified over 0,1 and ∞, where the ramification indices are, respectively, 3,4 and 12. Thus the corresponding triangulation obtained by lifting the standard triangulation of $\mathbb{CP}_1$ consists of 24 faces, 36 edges and 8 vertices, from which one cross-checks that the genus is 3. If one labels the four points above 0 by the numbers 1,3,5,7 (from top to bottom), and the three points above 1 by the numbers 2,4,6, one obtains the triangulation depicted in Fig. 4, where the center represents the point at infinity.

It is not difficult to compute the triangular and cartographic groups, and we only quote the results. To be consistent with the way the vertices have been numbered, we say that the vertices of type 0, lying above 0, are those labeled by an odd number. Numbering the

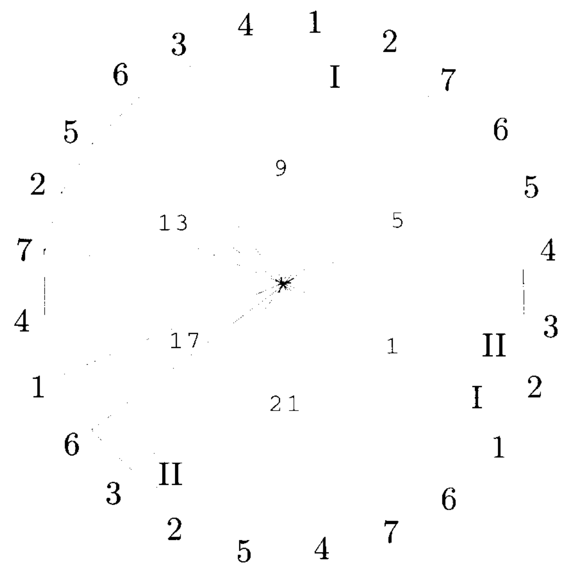

Fig. 4. Triangulation of $\overline{\Sigma}$ as a covering of degree 12 of the sphere. The points above 0 are labeled 1,3,5,7, while those above 1 are numbered 2,4,6. The central point is the point at infinity. There is no identification among the radial edges, but perimetric ones are to be identified by pairs, as exemplified by the edges marked I and II. This leaves 36 distinct edges. The small numbers close to the center label the faces from 1 to 24.

triangles as in Fig. 4, from 1 up to 24, one obtains that the action of the generators of the triangular group on the ith triangle is

$$\sigma_0(i) = i - (-1)^i \bmod 24, \quad \sigma_1(i) = i + (-1)^i \bmod 24,$$
$$\sigma_\infty(i) = i - 7(-1)^i \bmod 24, \tag{5.21}$$

where the representatives modulo 24 are taken between 1 and 24. From this, one easily computes the action of the oriented triangular group

$$\rho_0(i) = i + 8(-1)^i \bmod 24, \quad \rho_1(i) = i - 6(-1)^i \bmod 24,$$
$$\rho_\infty(i) = i - 2(-1)^i \bmod 24. \tag{5.22}$$

The generators satisfy $\rho_0 = \rho_\infty^{-4}$, $\rho_1 = \rho_\infty^3$ and $\rho_\infty^{12} = 1$, so that the oriented triangular group is isomorphic to $\mathbb{Z}_{12}$, from which it follows that the Fermat curve F_{12} covers $\overline{\Sigma}$. Because of the above relations between ρ_0, ρ_1 and ρ_∞, an element $\mu_0^a \mu_1^b \mu_\infty^c$ of $\widehat{D}(\overline{\Sigma})$ fixes a flag of symbol $(\infty 01)$ if and only if $-4a + 3b + c = 0 \bmod 12$. The quotient surface was discussed in Section 4.3, and is nothing but the triangular curve $C_{8,3,1}(12)$. This yields a third algebraic model for $\overline{\Sigma}$.

The projection $F_{12} \to C_{8,3,1}(12)$ allows to compute the period lattice. (The periods of all triangular curves $C_{r,s,t}(n)$ can be found in [32].) From the results of Section 4.3, the holomorphic differentials on $C_{8,3,1}(12)$ are the $\omega_{r,s,t}$ with $(r, s, t) = (\langle 8h \rangle, \langle 3h \rangle, \langle h \rangle)$ mod

12, that is, $\omega_{8,3,1}$, $\omega_{4,3,5}$, and $\omega_{4,6,2}$. From (3.5), the periods of these three differentials along the homology cycles in F_{12} equal

$$\left(\int_{\gamma_{i,j}} \omega_{8,3,1}\ ;\ \int_{\gamma_{i,j}} \omega_{4,3,5}\ ;\ \int_{\gamma_{i,j}} \omega_{4,6,2}\right) = (\xi^{8i+3j}; \xi^{4i+3j}; \xi^{4i+6j}). \tag{5.23}$$

Since cycles in F_{12} descend to cycles in $C_{8,3,1}(12)$, the period lattice of the latter contains the lattice in $\mathbb{C}^3$ formed by all integer combinations of the vectors (5.23). Noticing that the second component of (5.23) is obtained from the first component by the Galois automorphism $\sigma_5(\xi) = \xi^5$, one sees that this lattice is equal to $\{(z, \sigma_5(z), w) : z \in \mathbb{Z}(\xi),\ w \in \mathbb{Z}(\omega)\}$. It is of rank 6 over $\mathbb{Z}$, hence of finite index in the full period lattice, so that the two are isogenous:

$$L(\overline{\Sigma}) \sim \{(z, \sigma_5(z)) : z \in \mathbb{Z}(\xi)\} \oplus \mathbb{Z}(\omega). \tag{5.24}$$

The first factor, which we may call $L_{8,3,1}$, has been analyzed in Section 3.3, where it was found to be isogenous to the square of $\mathbb{Z}(i)$. Altogether we obtain

$$L(\overline{\Sigma}) \sim [\mathbb{Z}(i)]^2 \oplus \mathbb{Z}(\omega). \tag{5.25}$$

6. Conclusions

In this paper, we have tried to give some substance to a suggestion that had been made recently, concerning a possible connection between the modular invariant partition functions of WZNW models based on the affine algebra $\widehat{su(3)}$ and the geometry of the complex Fermat curves. There are many technical similarities between the two problems. In particular, we have shown that the decomposition of the Jacobian of the degree n Fermat curve F_n into simple Abelian varieties is essentially equivalent to the modular problem for the affine $su(3)$, at level $k = n - 3$. The relation was seen at the technical level through the $su(3)$ parity selection rules.

Besides this technical observation, which was at the origin of the suggestion, we have pointed out some intriguing coincidences with a third problem, namely that of the rational triangular billiards and the related algebraic curves. We have described at length the three circles of ideas, and found that many of the concepts in one of them have counterparts in the other two, like for instance holomorphic differentials against affine characters, parity selection rules against complex multiplication, etc. Despite these fine mathematical relationships, we have not been able to find a clear and definitive way to relate them to the list of modular invariants for $su(3)$, nor even to give an indication as to why the list of invariants is what it is.

In an attempt to take the relationship between the modular problem and algebraic curves in a broader sense, we have shown that a Riemann surface can be canonically associated with any rational conformal field theory. This could be done as a consequence of the fact that the matrices S and T, describing the modular transformations of the characters, generate a representation of $PSL_2(\mathbb{Z})$ which has a finite index subgroup in its kernel. The actual Riemann surfaces can be computed using invariant theory, as was illustrated in the cases of $su(3)$, levels 1 and 2. Characterizing all the Riemann surfaces that arise from conformal field theories in the way described in the text may be hard, but the few explicit examples we have analyzed so far suggest the following questions.

We have seen throughout this paper several infinite families of algebraic curves, and in particular the Fermat curves F_n. Is it true that every F_n is the Riemann surface associated with some RCFT, and if so, which one(s) correspond to a given F_n? What about the triangular curves? Is there a more intrinsic way to see if two RCFTs have the same Riemann surface? Is it true that the conformal theories containing dual affine Lie algebras, in the sense of the rank-level duality, have related Riemann surfaces?

According to the discussion in Section 3.4, the complete decomposition into elliptic curves is something rather rare in the context of Fermat curves, and happens for very special values of n only. Is it true that the Riemann surfaces coming from conformal theories have a generically large number of elliptic curves?

There are some indications that the Riemann surfaces arising from RCFT are somewhat special, since for example they have a large group of automorphisms. In general the center of the automorphism group is trivial, but there is no reason to believe that it implies that the Jacobian has no complex multiplication. We saw for instance in $su(3)$, level 1, that the field of complex multiplication was larger than what should have been expected on the sole consideration of the automorphism group. Moreover this field was clearly related to the eigenvalues of the T matrix. Is this more generally so? Do the surfaces coming from RCFTs have always complex multiplication? And if so, is it related to T, and in which precise way since T is not central?

We have no general answers to these questions, but looking at the algebras $su(2)$, $su(3)$ (see the text), $so(8)$, E_6 and E_7, all at level 1, we found the following encouraging results: all have Riemann surfaces isomorphic to triangular curves ($\widehat{so(8)}_1$ has the Fermat curve $F_3 \sim C_{1,1,1}(3)$), which all have complete decomposition in elliptic curves, and which all have complex multiplication. The other two algebras with two independent restricted characters, namely F_4 and G_2, also at level 1, are more complicated, but they have the same Riemann surface.

Acknowledgements

During the course of this work, some of us and sometimes all of us have benefited by the illuminating discussions with Arnaud Beauville, Paula Cohen, Pascal Degiovanni, Terry Gannon, Luc Haine, Victor Kac, Jean Lascoux and Jürgen Wolfart. They also made us aware of some important references. It is a pleasure to thank them warmly. AC thanks Joseph Oesterlé and Jean-Bernard Zuber for kind hospitality.

Appendix A. On automorphisms of quotient surfaces

Let Γ be an invariant subgroup of $PSL_2(\mathbb{Z})$ with finite index. Let Σ be the Riemann surface with punctures $\mathfrak{H}/\Gamma$ and let $\overline{\Sigma}$ be the associated compact Riemann surface. It is known that $\widehat{\Gamma} \equiv PSL_2(\mathbb{Z})/\Gamma$ is the group of automorphisms of Σ (see for instance [45, Theorem 5.9.4]), and thus is a subgroup of Aut $\overline{\Sigma}$, the automorphism group of $\overline{\Sigma}$. Our goal in this appendix is to show that if the genus g of $\overline{\Sigma}$ is larger than 1, then $\widehat{\Gamma} = \text{Aut}\,\overline{\Sigma}$ is the full automorphism group.

Let us assume that $\widehat{\Gamma}$ is of index I in Aut $\overline{\Sigma}$ (a finite group since the genus of $\overline{\Sigma}$ is greater than 1). It is well known that the quotient of $\overline{\Sigma}$ by a subgroup G of Aut $\overline{\Sigma}$ has a natural structure of Riemann surface, the Euler characteristics, hence the genuses, of the two surfaces being related by the Riemann–Hurwitz formula. The number of pre-images of a point $P \in \overline{\Sigma}/G$ by the projection map $\overline{\Sigma} \to \overline{\Sigma}/G$ is $|G|/m_P$ where m_P is the common order of the stability groups of the pre-images of P. Thus P is a ramification point of order m_P and multiplicity $|G|/m_P$. A straightforward application of the Riemann–Hurwitz formula then gives

$$\chi(\overline{\Sigma}) = 2 - 2g = |G| \left(\chi(\overline{\Sigma}/G) - \sum_P \left(1 - \frac{1}{m_P}\right)\right). \tag{A.1}$$

The sum over P is actually finite because only a finite number of points have $m_P \neq 1$.

The projection map $\Sigma \to \Sigma/\widehat{\Gamma}$ has a holomorphic extension $\overline{\Sigma} \to \overline{\Sigma}/\widehat{\Gamma} \cong \overline{\mathfrak{H}/PSL_2(\mathbb{Z})} \cong \mathbb{CP}_1$, ramified only over 0, 1728 and ∞, where the ramification order is respectively 3, 2 and n_∞ (the order of T in $\widehat{\Gamma}$). By the above formula, we have (as mentioned in the text)

$$\chi(\overline{\Sigma}) = -|\widehat{\Gamma}| \left(\frac{1}{6} - \frac{1}{n_\infty}\right). \tag{A.2}$$

On the other hand, the other projection, $\overline{\Sigma} \to \overline{\Sigma}/\text{Aut}\,\overline{\Sigma}$, can be decomposed as $\overline{\Sigma} \to \overline{\Sigma}/\widehat{\Gamma} \cong \mathbb{CP}_1 \to \overline{\Sigma}/\text{Aut}\,\overline{\Sigma}$. Yet another application of the Riemann–Hurwitz formula ensures that a holomorphic map from the Riemann sphere to a compact Riemann surface can exist only if the latter is also a Riemann sphere. Therefore $\overline{\Sigma}/\text{Aut}\,\overline{\Sigma} \cong \mathbb{CP}_1$ and the last map, from $\mathbb{CP}_1$ to $\mathbb{CP}_1$, can be normalized in such a way that it fixes the point at infinity, implying $m_\infty > 1$. Putting $G = \text{Aut}\,\overline{\Sigma}$ in (A.1), the genus of $\overline{\Sigma}$ can be computed from this second projection, and comparison with (A.2) yields

$$\frac{1}{6} - \frac{1}{n_\infty} = I\left(-2 + \left(1 - \frac{1}{m_\infty}\right) + \sum_{P \neq \infty} \left(1 - \frac{1}{m_P}\right)\right). \tag{A.3}$$

It follows from (A.2) that $g > 1$ is equivalent to $n_\infty > 6$, so that the left hand side is positive. This implies that the sum over P has at least two terms, since $1 - 1/m_P < 1$ for $m_P > 1$. Also because $1 - 1/m_P \geq \frac{1}{2}$, the value of the sum over P is at least $\frac{3}{2}$ if it contains three terms or more, whereas if it contains two terms, its minimal value is $\frac{7}{6}$, corresponding to $m_{P_1} = 2$, $m_{P_2} = 3$. (For $m_{P_1} = m_{P_2} = 2$, the sum is smaller, being equal to 1, but it renders the right hand side of (A.3) negative, and must be excluded.) Thus we obtain the inequality

$$\frac{1}{6}-\frac{1}{n_\infty}\geq I\left(\frac{1}{6}-\frac{1}{m_\infty}\right). \tag{A.4}$$

Finally one can observe that m_∞ is a non-zero multiple of n_∞. This is because the elements in $\widehat{\Gamma}$ which fix a point on $\overline{\Sigma}$ form a subgroup of those in Aut $\overline{\Sigma}$ which fix that point. In particular, $m_\infty \geq n_\infty > 6$ and this forces $I = 1$. Therefore $\widehat{\Gamma}$ is the full automorphism group of $\overline{\Sigma}$, as announced.

Using the results of Sections 4 and 5 on the Fermat curves F_n, this gives another proof that the full automorphism group of F_n, $n > 3$, is $\widehat{C}_n$, of cardinal $6n^2$.

Appendix B. $su(3)$ level 2

The $\widehat{su(3)}_2$ WZNW model has six chiral integrable representations, labeled by the six dominant weights $(1,1)$, $(1,2)$, $(2,1)$, $(1,3)$, $(2,2)$ and $(3,1)$, with corresponding characters χ_p. As explained in Section 2, they split into two orbits under the automorphisms. The S and T matrices accordingly factorize into a two-by-two piece acting on the orbit space, and a three-by-three Fourier kernel acting within each orbit. Following our general philosophy, we are interested in the independent restricted characters, and the representation of the modular group they carry, four-dimensional in this case. This amounts to going to the subspace of conjugation invariant characters. One may check that, if one puts the restricted characters in a matrix as

$$\underline{\chi}\equiv\begin{pmatrix}\chi_0 & \chi_1\\ \chi_2 & \chi_3\end{pmatrix}=\begin{pmatrix}\chi_{(1,1)} & \chi_{(2,2)}\\ \chi_{(1,3)}+\chi_{(3,1)} & \chi_{(1,2)}+\chi_{(2,1)}\end{pmatrix}, \tag{B.1}$$

the action of the modular group can be written as

$$S:\underline{\chi}\longrightarrow S_1\,\underline{\chi}\,S_{\mathrm{r}}^{-1},\qquad T:\underline{\chi}\longrightarrow T_1\,\underline{\chi}\,T_{\mathrm{r}}^{-1}, \tag{B.2}$$

where ($\omega = \mathrm{e}^{2\mathrm{i}\pi/3}$)

$$S_1=\frac{\mathrm{i}}{\sqrt{3}}\begin{pmatrix}1 & 1\\ 2 & -1\end{pmatrix},\qquad T_1=\begin{pmatrix}\omega^2 & 0\\ 0 & \omega\end{pmatrix}, \tag{B.3}$$

and ($\zeta = \mathrm{e}^{2\mathrm{i}\pi/5}$)

$$S_{\mathrm{r}}=\frac{2\mathrm{i}}{\sqrt{5}}\begin{pmatrix}\sin\frac{\pi}{5} & \sin\frac{2\pi}{5}\\ \sin\frac{2\pi}{5} & -\sin\frac{\pi}{5}\end{pmatrix},\qquad T_{\mathrm{r}}=\begin{pmatrix}\zeta^4 & 0\\ 0 & \zeta\end{pmatrix}. \tag{B.4}$$

The elements of all these matrices belong to $M_{\mathrm{restr}} = \mathbb{Q}(\zeta_{15})$. The corresponding Galois group, of order 8, consists of σ_h for $h \in \mathbb{Z}_{15}^*$. A general formula for the action of the Galois group on S has been given in Section 5.1, Eq. (5.9). In the present case, S and T generate a representation of $PSL_2(\mathbb{Z}_{15})$, so that the formula yields ($2^{-1} = 8$ mod 15 and $7^{-1} = 13$ mod 15)

$$\sigma_2(S)=ST^8ST^2ST^8S,\qquad \sigma_7(S)=ST^{13}ST^7ST^{13}S. \tag{B.5}$$

These two elements generate the full Galois group. Its action on T is just $\sigma_h(T) = T^h$.

Useful for what follows are the Puiseux series of the restricted characters:

$$\chi_{(1,1)} = q^{-2/15}[1 + 8q + 44q^2 + +128q^3 + 376q^4 + \cdots], \tag{B.6}$$

$$\chi_{(2,2)} = q^{7/15}[8 + 37q + 136q^2 + 404q^3 + 1\,072q^4 + \cdots], \tag{B.7}$$

$$\chi_{(1,3)} = q^{8/15}[6 + 24q + 93q^2 + 264q^3 + 708q^4 + \cdots], \tag{B.8}$$

$$\chi_{(1,2)} = q^{2/15}[3 + 24q + 90q^2 + 288q^3 + 777q^4 + \cdots]. \tag{B.9}$$

One easily checks that $S_\mathrm{l}^2 = (S_\mathrm{l}T_\mathrm{l})^3 = -1$ and $T_\mathrm{l}^3 = 1$, and similarly $S_\mathrm{r}^2 = (S_\mathrm{r}T_\mathrm{r})^3 = -1$ and $T_\mathrm{r}^5 = 1$. Of course the normalizations in the left and right factors are arbitrary since only their product matters, but our choice makes all four matrices have determinant 1. Then S_l and T_l on the one hand, S_r and T_r on the other hand, generate subgroups of $SL_2(\mathbb{C})$. If we consider the quotients of these subgroups by -1, and keep the classification of finite subgroups of the special linear group in two complex dimensions in mind, we see that the left group $\widehat{\Gamma_\mathrm{l}}$ is the double cover of the tetrahedron group, hence of order 2×12, and that the right group $\widehat{\Gamma_\mathrm{r}}$ is the double cover of the icosahedron group, of order 2×60.

Let us denote the matrix that acts on the characters as $R_\mathrm{l}\,\underline{\chi}\,R_\mathrm{r}^{-1}$ by $R_\mathrm{l} \times R_\mathrm{r}$. Then T^6 acts as $1 \times T_\mathrm{r}$, and T^{10} acts as $T_\mathrm{l} \times 1$. Similarly $(ST^6)^9$ acts as $S_\mathrm{l} \times 1$, while $(ST^{10})^9$ acts as $1 \times S_\mathrm{r}$. This is enough to show that there is a surjection from $\widehat{\Gamma_\mathrm{l}} \times \widehat{\Gamma_\mathrm{r}}$ onto $\widehat{\Gamma}$, the group generated by the matrices S and T on the restricted characters, and that $\widehat{\Gamma} \cong \widehat{\Gamma_\mathrm{l}} \times \widehat{\Gamma_\mathrm{r}}$ modulo the kernel of this map, which is the diagonal $\mathbb{Z}_2 = \{1 \times 1, -1 \times -1\}$ of order 2. Therefore the order of $\widehat{\Gamma}$ is $\frac{1}{2}(2 \cdot 12)(2 \cdot 60) = 1440$. On the other hand the order of T is manifestly 15, so the general formula (5.4) implies that the genus of the Riemann surface associated with $su(3)_2$ is equal to 73. The non-compactified surface Σ has $1440/15 = 96$ punctures.

This number looks frightening, and to compute an algebraic model for it seems hopeless. Let us recall that according to the general discussion of Section 5.1, what we have to do is to find a basis of polynomials in the characters which are invariant for the action of $\widehat{\Gamma}$. There is at least one polynomial invariant which is easy to obtain: since all left and right matrices have determinant 1, the determinant of $\underline{\chi}$ is invariant under $\widehat{\Gamma}$. A look at the Puiseux series shows that it is regular at $q = 0$, and that the zeroth order coefficient is equal to 6, so that it is exactly equal to 6:

$$P_2(\chi_i) = \chi_0\chi_3 - \chi_1\chi_2 = 6. \tag{B.10}$$

The ring of polynomial invariants for $\widehat{\Gamma}$ is more complicated than in the level 1 case. The Molien series for the number of invariants is

$$F(t) = \frac{1 + t^{12} + t^{20} + t^{24} + 2t^{30} + t^{36} + t^{40} + t^{48} + t^{60}}{(1 - t^2)(1 - t^{12})(1 - t^{20})(1 - t^{30})}. \tag{B.11}$$

It shows that the ring is not freely generated by four invariants, but that there are more generators with relations among them. In this case, the ring of invariants is a free module over $\mathbb{C}(P_2, P_{12}, P_{20}, P_{30})$ with basis $\{1, R_{12}, R_{20}, R_{24}, R_{30}, R'_{30}, R_{36}, R_{40}, R_{48}, R_{60}\}$, where the P_i's are "fundamental" invariants of degree i, and the R_j's are "auxiliary" invariants. Every R_j can be expressed algebraically in terms of the P_i's, but not polynomially. What we want to do is to compute enough independent irreducible invariants, namely three or four depending on whether they are equal to trivial functions of j or not. We have already found one, namely P_2 given in (B.10), which clearly accounts for the factor $(1-t^2)^{-1}$ in $F(t)$.

In order to compute invariants for $\widehat{\Gamma}$, one can take advantage of the quasi-factorized form of $\widehat{\Gamma} = \widehat{\Gamma}_l \times \widehat{\Gamma}_r/\mathbb{Z}_2$. In fact we deal with a true (even if not faithful) representation of $\widehat{\Gamma}_l \times \widehat{\Gamma}_r$ so the $\mathbb{Z}_2$ factor is automatically taken into account. Given four indeterminates w, x, y, z (they will soon become $\chi_0, \ldots, \chi_3$), an element $\widehat{\gamma}_l \times \widehat{\gamma}_r$ acts on them by left and right multiplication

$$\widehat{\gamma}_l \begin{pmatrix} w & x \\ y & z \end{pmatrix} \widehat{\gamma}_r^{-1}.$$

If we write the variables w, x, y, z in terms of four others u_1, u_2, v_1, v_2 through

$$\begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} \times (v_1 \quad v_2), \tag{B.12}$$

then obviously $\widehat{\gamma}_l$ acts on the u's whereas $\widehat{\gamma}_r$ acts on the v's. It is clear that upon this substitution, a polynomial invariant $P(w, x, y, z)$ for $\widehat{\Gamma}$ becomes a (perhaps identically vanishing) linear combination of product polynomials $P^l(u_1, u_2)P^r(v_1, v_2)$ with P^l invariant under $\widehat{\Gamma}_l$ and P^r invariant under $\widehat{\Gamma}_r$.

We would like to go backwards as well, i.e. start with polynomial invariants $P^l(u_1, u_2)$ for $\widehat{\Gamma}_l$ and $P^r(v_1, v_2)$ for $\widehat{\Gamma}_r$ and construct a polynomial invariant $P(w, x, y, z)$ for $\widehat{\Gamma}$. This involves a nice analogy with Wick contractions. We define formal two-point functions $\langle u_1v_1\rangle = w$, $\langle u_1v_2\rangle = x$, $\langle u_2v_1\rangle = y$, $\langle u_2v_2\rangle = z$, and all others zero. The expectation value of a monomial in u_1, u_2, v_1 and v_2 is the polynomial in w, x, y and z obtained by doing all Wick contractions (obviously, this gives 0 unless the degrees in the u and v variables are equal), and we extend to all polynomials by linearity. We also include a normalization factor and shall use the explicit general formula

$$\langle u_1^{\alpha} u_2^{n-\alpha} v_1^{\beta} v_2^{n-\beta}\rangle = \binom{n}{\alpha}^{-1} \sum_{a=\max(0,\alpha+\beta-n)}^{\min(\alpha,\beta)} \binom{\beta}{a}\binom{n-\beta}{\alpha-a} w^a x^{\alpha-a} y^{\beta-a} z^{n-\alpha-\beta+a}. \tag{B.13}$$

As is clear from the properties of correlation functions in field theory, for consistency Wick contractions must transform covariantly under linear transformations of the fields. A formal argument is easy to build. In particular if one does a linear transformation of the fields that leaves the polynomial in the fields invariant, the correlator is invariant. Thus, if $P^l(u_1, u_2)$ is an invariant for $\widehat{\Gamma}_l$ and $P^r(v_1, v_2)$ an invariant for $\widehat{\Gamma}_r$, $P(w, x, y, z) = \langle P^l(u_1, u_2)P^r(v_1, v_2)\rangle$ is an invariant for $\widehat{\Gamma}$.

Moreover, with the chosen normalization, substitution of the u and v variables in $P(w, x, y, z) = \langle P^l(u_1, u_2)\, P^r(v_1, v_2)\rangle$ gives back $P^l(u_1, u_2)P^r(v_1, v_2)$.

So if we start from an arbitrary polynomial invariant $P(w,x,y,z)$, substitute the u and v variables according to Eq. (B.12), and take the expectation value, we get a new polynomial $Q(w,x,y,z)$ such that $P-Q$ gives 0 upon the substitution of the u and v variables. Now we use a trivial fact from algebra, related to the simplest Plücker embedding of algebraic geometry: the ideal of polynomials in w, x, y and z vanishing identically upon substituting the u and v variables is principal and generated by the determinant $wz-xy$. Hence $P-Q$ has to be a multiple of $wz-xy$ and the quotient is of course invariant because $wz-xy$ is. We can repeat the construction. At every step the degree decreases so the procedure must stop. This shows that all invariants are polynomials in the determinant $wz-xy$ with coefficients being the expectation value invariants.

If $d_n^{(\mathrm{l})}$ and $d_n^{(\mathrm{r})}$ denote the number of degree n invariants for $\widehat{\Gamma}_\mathrm{l}$ and $\widehat{\Gamma}_\mathrm{r}$, the above construction yield $d_n^{(\mathrm{l})}d_n^{(\mathrm{r})}$ invariants for $\widehat{\Gamma}$ of degree n. From

$$F_\mathrm{l}(t)=\sum_{n=0}^{\infty} d_n^{(\mathrm{l})}t^n=\frac{1+t^{12}}{(1-t^6)(1-t^8)}, \tag{B.14}$$

$$F_\mathrm{r}(t)=\sum_{n=0}^{\infty} d_n^{(\mathrm{r})}t^n=\frac{1+t^{30}}{(1-t^{12})(1-t^{20})}, \tag{B.15}$$

one finds the generating function for the number of invariants for $\widehat{\Gamma}$ induced from those of $\widehat{\Gamma}_\mathrm{l}$ and $\widehat{\Gamma}_\mathrm{r}$:

$$\sum_{n=0}^{\infty} d_n^{(\mathrm{l})}d_n^{(\mathrm{r})}t^n=\frac{1+t^{12}+t^{20}+t^{24}+2t^{30}+t^{36}+t^{40}+t^{48}+t^{60}}{(1-t^{12})(1-t^{20})(1-t^{30})}. \tag{B.16}$$

As announced, the missing factor is due to the contribution of $wz-xy$. We now proceed to give the invariants of lowest degree explicitly.

From (B.14), all polynomial invariants for $\widehat{\Gamma}_\mathrm{l}$ can be expressed in terms of only three invariants, of degree 6,8 and 12:

$$P_6^\mathrm{l}=8\,u_1^6-20\,u_1^3u_2^3-u_2^6, \tag{B.17}$$

$$P_8^\mathrm{l}=8\,u_1^7u_2+7\,u_1^4u_2^4-u_1u_2^7, \tag{B.18}$$

$$R_{12}^\mathrm{l}=64\,u_1^{12}+704\,u_1^9u_2^3+88\,u_1^3u_2^9-u_2^{12}. \tag{B.19}$$

There are two left invariants of degree 12, $[P_6^\mathrm{l}]^2$ and R_{12}^l, and two of degree 20, namely $[P_6^\mathrm{l}]^2P_8^\mathrm{l}$ and $R_{12}^\mathrm{l}P_8^\mathrm{l}$.

Likewise for the right factor, all invariants can be written in terms of three invariants of degree 12, 20 and 30:

$$P_{12}^\mathrm{r}=v_1^{11}v_2+11\,v_1^6v_2^6-v_1v_2^{11}, \tag{B.20}$$

$$P_{20}^\mathrm{r}=v_1^{20}-228\,v_1^{15}v_2^5+494\,v_1^{10}v_2^{10}+228\,v_1^5v_2^{15}+v_2^{20}, \tag{B.21}$$

$$R_{30}^\mathrm{r}=v_1^{30}+522\,v_1^{25}v_2^5-10\,005\,v_1^{20}v_2^{10}-10\,005\,v_1^{10}v_2^{20} -522\,v_1^5v_2^{25}+v_2^{30}. \tag{B.22}$$

There is one right invariant of degree 12, and one of degree 20.

From the generating function (B.11), the degrees of the five lowest irreducible invariants for $\widehat{\Gamma}$ are 2, 12, 12, 20 and 20. In terms of left and right invariants, they are given by the following Wick products:

$$P_2 = wz - xy \quad (= 6), \tag{B.23}$$

$$P_{12} = \langle\, [P_6^{\rm l}]^2\, P_{12}^{\rm r} \,\rangle \quad \left(= \tfrac{512}{q} + \tfrac{1\,341\,120}{7} + \cdots\right), \tag{B.24}$$

$$P_{12}' = \langle\, R_{12}^{\rm l}\, P_{12}^{\rm r} \,\rangle \quad \left(= \tfrac{512}{q} + 199\,488 + \cdots\right), \tag{B.25}$$

$$P_{20} = \langle\, [P_6^{\rm l}]^2\, P_8^{\rm l}\, P_{20}^{\rm r} \,\rangle \quad \left(= \tfrac{6\,144}{q^2} + \tfrac{103\,882\,752}{17q} + \tfrac{536\,266\,607\,616}{187} + \cdots\right), \tag{B.26}$$

$$P_{20}' = \langle\, R_{12}^{\rm l}\, P_8^{\rm l}\, P_{20}^{\rm r} \,\rangle \quad \left(= \tfrac{6\,144}{q^2} - \tfrac{235\,855\,872}{17q} - \tfrac{197\,872\,671\,744}{17} + \cdots\right). \tag{B.27}$$

We have indicated in parenthesis the first terms of the Puiseux series of the invariants when one substitutes $\chi_0, \chi_1, \chi_2, \chi_3$ for w, x, y, z. One sees, upon the same substitution, that P_2, $P_{12} - P_{12}'$ and $P_{20} - P_{20}' - \frac{512}{17} P_2^4\, P_{12}'$ are modular invariant functions, holomorphic in the upper-half plane, hence equal to pure constants, given respectively by 6, $-\frac{55\,296}{7}$ and $\frac{1\,256\,788\,721\,664}{187}$. They form a complete set of algebraic equations that describe the Riemann surface associated to $su(3)$ level 2. Their explicit form is just a matter of computing Wick contractions using (B.13). For completeness, we quote the final results:

$$\chi_0\chi_3 - \chi_1\chi_2 = 6, \tag{B.28}$$

$$\begin{aligned}
&28\,[\chi_1\,\chi_2 + \chi_0\,\chi_3]\,[24\,(\chi_0^5\,\chi_2^5 - \chi_1^5\,\chi_3^5)\\
&\quad -(64\,\chi_0^3\,\chi_1^3 + 3\,\chi_2^3\chi_3^3)\,(2\,\chi_0^2\,\chi_3^2 + 7\,\chi_0\,\chi_1\,\chi_2\,\chi_3 + 2\,\chi_1^2\,\chi_2^2)]\\
&\quad -14\,[\chi_0\,\chi_3 + 3\,\chi_1\,\chi_2]\,[64\,\chi_0^8\,\chi_2^2 - 3\,\chi_1^2\,\chi_3^8]\\
&\quad -14\,[3\,\chi_0\,\chi_3 + \chi_1\,\chi_2]\,[3\,\chi_0^2\,\chi_2^8 - 64\,\chi_1^8\,\chi_3^2]\\
&\quad +16\,[\chi_1^6\,\chi_2^6 + 36\,\chi_0\,\chi_1^5\,\chi_2^5\,\chi_3 + 225\,\chi_0^2\,\chi_1^4\,\chi_2^4\,\chi_3^2 + 400\,\chi_0^3\,\chi_1^3\,\chi_2^3\,\chi_3^3\\
&\quad +225\,\chi_0^4\,\chi_1^2\,\chi_2^2\,\chi_3^4 + 36\,\chi_0^5\,\chi_1\,\chi_2\,\chi_3^5 + \chi_0^6\,\chi_3^6]\\
&\quad +7\,\chi_2^{11}\,\chi_3 + 77\,\chi_2^6\,\chi_3^6 - 7\,\chi_2\,\chi_3^{11} + 27\,648 = 0,
\end{aligned} \tag{B.29}$$

$$\begin{aligned}
&\{247\,\chi_2^9\,\chi_3^9\,\chi_0\,\chi_3 + \chi_0\,\chi_2^4\,(8\,\chi_0^3 - \chi_2^3)^4\,(\chi_0^3 + \chi_2^3) - 57\,\chi_2^{14}\,\chi_3^4\,(3\,\chi_0\,\chi_3 + \chi_1\,\chi_2)\\
&\quad +\tfrac{26}{17}\,[4\,096\,\chi_0^6\,\chi_1^6 - 31\,\chi_2^6\,\chi_3^6] \times [14\,\chi_1^4\,\chi_2^4 + 80\,\chi_0\,\chi_1^3\,\chi_2^3\,\chi_3 + \tfrac{135}{2}\,\chi_0^2\,\chi_1^2\,\chi_2^2\,\chi_3^2]\\
&\quad +\tfrac{4\,992}{17}\,[\chi_0^5\,\chi_2^5 - \chi_1^5\,\chi_3^5] \times [21\,\chi_1^5\,\chi_2^5 + 175\,\chi_0\,\chi_1^4\,\chi_2^4\,\chi_3 + 450\,\chi_0^2\,\chi_1^3\,\chi_2^3\,\chi_3^2]\\
&\quad +\tfrac{208}{17}\,[64\,\chi_0^3\,\chi_1^3 + 11\,\chi_2^3\,\chi_3^3]\\
&\quad \times[2\,\chi_1^7\,\chi_2^7 + 35\,\chi_0\,\chi_1^6\,\chi_2^6\,\chi_3 + 189\,\chi_0^2\,\chi_1^5\,\chi_2^5\,\chi_3^2 + 420\,\chi_0^3\,\chi_1^4\,\chi_2^4\,\chi_3^3]\\
&\quad -\tfrac{832}{187}\,[\chi_1^{10}\,\chi_2^{10} + 100\,\chi_0\,\chi_1^9\,\chi_2^9\,\chi_3 + 2\,025\,\chi_0^2\,\chi_1^8\,\chi_2^8\,\chi_3^2 + 14\,400\,\chi_0^3\,\chi_1^7\,\chi_2^7\,\chi_3^3\\
&\quad +44\,100\,\chi_0^4\,\chi_1^6\,\chi_2^6\,\chi_3^4 + 31\,752\,\chi_0^5\,\chi_1^5\,\chi_2^5\,\chi_3^5]\\
&\quad -\tfrac{4}{17}\,[4\,096\,\chi_0^{11}\,\chi_1 + 31\,\chi_2\,\chi_3^{11}] \times [273\,\chi_1^4\,\chi_2^4 + 455\,\chi_0\,\chi_1^3\,\chi_2^3\,\chi_3\\
&\quad +210\,\chi_0^2\,\chi_1^2\,\chi_2^2\,\chi_3^2 + 30\,\chi_0^3\,\chi_1\,\chi_2\,\chi_3^3 + \chi_0^4\,\chi_3^4]
\end{aligned}$$

$$
\begin{aligned}
&-\tfrac{8}{17}\,[64\,\chi_0^8\,\chi_2^2 - 11\,\chi_1^2\,\chi_3^8] \times [1287\,\chi_1^5\,\chi_2^5 + 5005\,\chi_0\,\chi_1^4\,\chi_2^4\,\chi_3 \\
&+6006\,\chi_0^2\,\chi_1^3\,\chi_2^3\,\chi_3^2 + 2730\,\chi_0^3\,\chi_1^2\,\chi_2^2\,\chi_3^3 + 455\,\chi_0^4\,\chi_1\,\chi_2\,\chi_3^4 + 21\,\chi_0^5\,\chi_3^5] \\
&+\tfrac{256}{17}[\chi_0\,\chi_3 - \chi_1\,\chi_2]^4 \times [64\,\chi_0^{11}\,\chi_1 + 352\,\chi_0^6\,\chi_1^6 - \chi_2^{11}\,\chi_3 - \tfrac{11}{2}\,\chi_2^6\,\chi_3^6 \\
&+22\,(8\,\chi_0^8\,\chi_2^2 - \chi_1^2\,\chi_3^8)\,(\chi_0\,\chi_3 + 3\,\chi_1\,\chi_2) \\
&+44\,(8\,\chi_0^3\,\chi_1^3 + \chi_2^3\,\chi_3^3)\,(2\,\chi_1^3\,\chi_2^3 + 9\,\chi_0\,\chi_1^2\,\chi_2^2\,\chi_3)] \\
&+(\chi_0, \chi_1, \chi_2, \chi_3) \longrightarrow (\chi_1, -\chi_0, \chi_3, -\chi_2)\} + \tfrac{628\,394\,360\,832}{187} = 0. \qquad \text{(B.30)}
\end{aligned}
$$

References

[1] A. Cappelli, C. Itzykson and J.-B. Zuber, The *A-D-E* classification of minimal and $A_1^{(1)}$ conformal invariant theories, Commun. Math. Phys. 113 (1987) 1–26;
A. Kato, Classification of modular invariant partition functions in two dimensions, Modern. Phys. Lett. A 2 (1987) 585–600.

[2] T. Gannon, The classification of affine $su(3)$ modular invariant partition functions, Commun. Math. Phys. 161 (1994) 233–264.

[3] T. Gannon, WZW commutants, lattices, and level-one partition functions, Nuclear. Phys. B 396 (1993) 708–736.

[4] P. Ruelle, E. Thiran and J. Weyers, Implications of an arithmetical symmetry of the commutant for modular invariants, Nuclear Phys. B 402 (1993) 693–708.

[5] A. Coste and T. Gannon, Remarks on Galois symmetry in rational conformal field theories, Phys. Lett. B 323 (1994) 316–321.

[6] N. Koblitz and D. Rohrlich, Simple factors in the Jacobian of a Fermat curve, Canad. J. Math. XXX (1978) 1183–1205.

[7] E. Aurell and C. Itzykson, Rational billiards and algebraic curves, J. Geom. Phys. 5 (1988) 191–208.

[8] P. Cohen, J. Wolfart, M. Bauer and C. Itzykson, in: *The Grothendieck Theory of Dessins d'enfants*, ed. L. Schneps, LMSLNS 200 (Cambridge University Press, Cambridge)

[9] V.G. Kac, *Infinite Dimensional Lie Algebras*, 3rd Ed. (Cambridge University Press, Cambridge, 1990).

[10] C. Itzykson and J.-M. Drouffe, *Théorie statistique des champs* (éditions du CNRS, Paris, 1989).

[11] V.G. Kac and M. Wakimoto, Modular and conformal invariance constraints in representation theory of affine algebras, Adv. in Math. 70 (1988) 156–236.

[12] E. Witten, Non-Abelian bosonization in two dimensions, Commun. Math. Phys. 92 (1984) 455–472.

[13] P. Goddard and D. Olive, Kac–Moody and Virasoro algebras in relation to quantum physics, Int. J. Modern. Phys. A1 (1983) 303–414.

[14] G. Moore and N. Seiberg, Naturality in conformal field theory, Nuclear Phys. B 313 (1989) 16–40.

[15] J. Cardy, The operator content of two-dimensional conformally invariant theories, Nuclear Phys. B 270 (1986) 186–204.

[16] W. Nahm, Lie group exponents and $SU(2)$ current algebras, Commun. Math. Phys. 118 (1988) 171–176.

[17] P. Di Francesco and J.-B. Zuber, $SU(N)$ lattice integrable models associated with graphs, Nuclear Phys. B 338 (1990) 602–646.

[18] T. Gannon, The level two and three modular invariants of $SU(n)$, preprint (November 1995).

[19] T. Gannon, Towards a classification of $su(2) \oplus \cdots \oplus su(2)$ modular invariant partition functions, J. Math. Phys. 36 (1995) 675–706.

[20] T. Gannon, P. Ruelle and M. Walton, Automorphism modular invariants of current algebras, Commun. Math. Phys. 179 (1996) 121–156.

[21] T. Gannon, Kac–Peterson, Perron–Frobenius, and the classification of conformal field theories, preprint (q-alg 9510026).

[22] M. Bauer and C. Itzykson, Modular transformations of $SU(N)$ affine characters and their commutant, Commun. Math. Phys. 127 (1990) 617–636.

[23] P. Ruelle, Dimension of the commutant for the $SU(N)$ affine algebras, Commun. Math. Phys. 133 (1990) 181–196.

[24] E. Buffenoir, A. Coste, J. Lascoux, P. Degiovanni and A. Buhot, Precise study of some number fields and Galois actions occurring in conformal field theory, Ann. Inst. Poincaré, Theor. Phys. 63 (1995) 41–79.
[25] C. Vafa, Toward classification of conformal theories, Phys. Lett. 206B (1988) 421–426.
G. Anderson and G. Moore, Rationality in conformal field theory, Commun. Math. Phys. 117 (1988) 441–450.
[26] J. de Boer and J. Goeree, Markov traces and II_1 factors in conformal field theory, Commun. Math. Phys. 139 (1991) 267–304.
[27] P. Ruelle, E. Thiran and J. Weyers, Modular invariants for affine $\widehat{SU}(3)$ theories at prime heights, Commun. Math. Phys. 133 (1990) 305–322.
[28] J. Fuchs, B. Gato-Rivera, B. Schellekens and C. Schweigert, Modular invariants and fusion rule automorphisms from Galois theory, Phys. Lett. B 334 (1994) 113–120.
[29] J. Fuchs, B. Schellekens and C. Schweigert, Galois modular invariants of WZW models, Nuclear Phys. B 437 (1995) 667–694.
[30] J.-B. Bost, Les Houches lectures "Introduction to compact Riemann surfaces, Jacobians and Abelian varieties", in: *From Number Theory to Physics*, eds. M. Waldschmidt, P. Moussa, J.-M. Luck and C. Itzykson (Springer, Berlin, 1990).
[31] H.P.F. Swinnerton-Dyer, *Analytic Theory of Abelian Varieties* (Cambridge University Press, Cambridge, 1974).
[32] S. Lang, *Introduction to Algebraic and Abelian Functions*, GTM 89 (Springer, Berlin, 1982).
[33] N. Aoki, Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves, Amer. J. Math. 113 (1991) 779–833.
[34] D. Rohrlich, appendix to B. Gross, On the periods of Abelian integrals and a formula of Chowla and Seiberg, Invent. Math. 45 (1978) 193–211.
[35] A. Weil, Sur les périodes d'intégrales abéliennes, Commun. Pure Appl. Math. XXIX (1976) 813–819.
[36] S. Lang, *Complex Multiplication* (Springer, Berlin, 1983).
[37] G. Shimura and Y. Taniyama, Complex multiplication of Abelian varieties and its applications to number theory, Publ. Math. Soc. Japan 6 (1961).
[38] N. Koblitz, Gamma function identities and elliptic differentials on Fermat curves, Duke Math. J. 45 (1978) 87–99.
[39] A. Grothendick, Esquisse d'un programme.
[40] A.W. Knapp, *Elliptic Curves* (Princeton University Press, Princeton, 1992).
[41] Arithmetic and Geometry of Fermat Curves, *Proc. of the Algebraic Geometry Seminar*, Singapore (1987).
[42] P.J. Richens and M.V. Berry, Pseudo-integrable systems in classical and quantum mechanics, Physica D 2 (1981) 495–512.
[43] D. Gepner, E. Witten, String theory on group manifolds, Nuclear Phys. B 278 (1986) 493–549.
[44] R.C. Gunning, *Lectures on Modular Forms*, Annals of Mathematics Studies 48 (Princeton University Press, Princeton, 1992).
[45] G.A. Jones and D. Singerman, *Complex Functions* (Cambridge University Press, Cambridge, 1987).
[46] C.L. Siegel, *Topics in Complex Function Theory*, Vol. II (Wiley, New York, 1971).
[47] M. Bauer, unpublished.
[48] D.J. Benson, *Polynomial Invariants of Finite Groups*, LMSLNS 190 (Cambridge University Press, Cambridge, 1993).
[49] G.C. Shephard and J.A. Todd, Finite unitary reflection groups, Canad J. Math. VI (1954) 274–304.