Publ. RIMS Kyoto Univ. **49** (2013), 413–496
DOI 10.4171/PRIMS/110

On Arithmetic Monodromy Representations of Eisenstein Type in Fundamental Groups of Once Punctured Elliptic Curves

Dedicated to Professor Yasutaka Ihara on the occasion of his 75th birthday

by

Hiroaki Nakamura

Abstract

We discuss certain arithmetic invariants arising from the monodromy representation in fundamental groups of a family of once punctured elliptic curves of characteristic zero. An explicit formula in terms of Kummer properties of modular units is given to describe these invariants. In the complex analytic model, the formula turns out to feature generalized Dedekind–Rademacher functions as the main periodic part of the invariant.

2010 Mathematics Subject Classification: Primary 14H30; Secondary 11G16, 11F20.
Keywords: Galois representation, arithmetic fundamental group, elliptic curve.

Contents

Communicated by S. Mochizuki. Received May 31, 2011. Revised March 12, 2012, April 18, 2012.

H. Nakamura: Department of Mathematics, Faculty of Science,
Okayama University, Okayama 700-8530, Japan;
e-mail: h-naka@math.okayama-u.ac.jp

§1. Introduction

In this paper, we study certain invariants arising from (geometrically meta-abelian) arithmetic fundamental groups of once punctured elliptic curves. Suppose we are given an elliptic curve E over a number field k with Weierstrass equation

$$E : y^2 = 4x^3 - g_2x - g_3 \tag{1.1}$$

with discriminant $\Delta = \Delta(E, dx/y) = g_2^3 - 27g_3^2 \in k^\times$. The local coordinate $t := -2x/y$ at the infinity point O of $E \setminus \{O\} := \mathrm{Spec}(k[x,y]/(4x^3 - g_2x - g_3 - y^2))$ gives rise to a tangential base point $\overrightarrow{\mathfrak{w}}$ and a split exact sequence of profinite fundamental groups

$$1 \to \pi_1(E_{\bar{k}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}) \to \pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}}) \overset{\curvearrowleft}{\longrightarrow} G_k = \mathrm{Gal}(\bar{k}/k) \to 1. \tag{1.2}$$

It is well known that the geometric fundamental group $\pi_1(E_{\bar{k}} \setminus \{O\}, \overrightarrow{\mathfrak{w}})$ has a presentation with generators $\mathbf{x}_1, \mathbf{x}_2, \mathbf{z}$ and relation $[\mathbf{x}_1, \mathbf{x}_2]\mathbf{z} = \mathbf{x}_1\mathbf{x}_2\mathbf{x}_1^{-1}\mathbf{x}_2^{-1}\mathbf{z} = 1$ so that $\mathbf{z}$ generates an inertia subgroup over the missing infinity point O.

Let l be a rational prime and π the maximal pro-l quotient of $\pi_1(E_{\bar{k}} \setminus \{O\}, \overrightarrow{\mathfrak{w}})$. Write $\varphi_{\overrightarrow{\mathfrak{w}}} : G_k \to \mathrm{Aut}(\pi)$ for the Galois representation induced from (1.2). In [Bl84], S. Bloch considered an elliptic analog of Ihara's construction of the universal power series for Jacobi sums [Ih86a], and proposed a new power series representation

$$\mathcal{E} : G_{k(E_{l^\infty})} \to \mathbb{Z}_l[[T_1, T_2]] \cong \mathbb{Z}_l[[\pi^{\mathrm{ab}}]] \quad (\sigma \mapsto \mathcal{E}_\sigma) \tag{1.3}$$

from the meta-abelian reduction of $\varphi_{\overrightarrow{\mathfrak{w}}}$ in π/π''. Here $k(E_{l^\infty})$ is the field obtained by adjoining the coordinates of all l-power torsion points of E, and $\mathbb{Z}_l[[\pi^{\mathrm{ab}}]]$ is the l-adic complete group algebra of the abelianization π^{ab} of π identified with the commutative ring of two-variable formal power series in $T_i :=$ 'the image of $\mathbf{x}_i$'-1 $(i = 1, 2)$. This construction was first applied by H. Tsunogai [Tsu95a] to deduce a result of anabelian geometry. Subsequently, an explicit formula for the coefficients of $\mathcal{E}_\sigma$ using Kummer properties of special values of the fundamental theta function $\theta(z,\tau) = \Delta(\tau)e^{-6\eta(z,\tau)z}\sigma(z,\tau)^{12}$ at $z = x_1\tau + x_2$ $((x_1, x_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2)$ was given in [N95]. The main motivation of the present paper is to generalize these results to more general $\sigma \in G_k$ not necessarily contained in $G_{k(E_{l^\infty})}$.

In [Tsu95a], Tsunogai also derived an equation (see Remark 3.4.4 below) suggesting a naive difficulty of extending Bloch's construction of $\mathcal{E}_\sigma$ to general $\sigma \in G_k$, which makes the elliptic case more complicated than Ihara's case of $\pi_1(\mathbf{P}^1 - \{0, 1, \infty\})$. In fact, Ihara's universal power series for Jacobi sums is naturally defined on $G_{\mathbb{Q}}$, whereas Bloch's power series $\mathcal{E}_\sigma$ is not on G_k. In this paper, we

propose a way to bypass the difficulty in the elliptic case by still extending Tsunogai's treatment but in a somewhat twisted way. Consequently, for each l-power m, we will construct a certain continuous mapping

$$\mathbb{E}_m : G_k \times \mathbb{Z}_l^2 \to \mathbb{Z}_l \quad \Big(\big(\sigma, \tbinom{u}{v}\big) \mapsto \mathbb{E}_m(\sigma; u, v)\Big) \tag{1.4}$$

from the meta-abelian reduction $G_k \to \mathrm{Aut}(\pi/\pi'')$ of $\varphi_{\overrightarrow{\mathfrak{w}}}$. The value $\mathbb{E}_m(\sigma; u, v)$ is not periodic in u, v modulo m for general $\sigma \in G_k$, but turns out to be periodic for $\sigma \in G_{k(E_{l^\infty})}$ so that it determines an element $\mathbb{E}_m(\sigma)$ of the finite group ring $\mathbb{Z}_l[(\mathbb{Z}/m\mathbb{Z})^2]$. Then $\mathcal{E}_\sigma$ can be recovered as the limit measure on $\mathbb{Z}_l^2$:

$$\mathcal{E}_\sigma = \varprojlim_m \big(\mathbb{E}_m(\sigma) + \tfrac{1}{12}\rho_{\Delta(E, mdx/y)}(\sigma)\mathbf{e}_m\big) \quad (\sigma \in G_{k(E_{l^\infty})}), \tag{1.5}$$

where $\rho_{\Delta(E,mdx/y)}$ means a Kummer 1-cocycle along (a specified sequence of) l-power roots of $\Delta(E, mdx/y) = m^{-12}(g_2^3 - 27g_3^2)$, and $\mathbf{e}_m \in \mathbb{Z}_l[(\mathbb{Z}/m\mathbb{Z})^2]$ designates the group element sum (cf. §6.10 for details).

In this paper, we work in a slightly more general setting of pro-$\mathcal{C}$ versions, namely we allow π to be the maximal pro-$\mathcal{C}$ quotient of the geometric fundamental group for any full class $\mathcal{C}$ of finite groups closed under formation of subgroups, quotients and extensions. Moreover, we consider elliptic curves in the Weierstrass form (1.1) for k being regular algebras B over $\mathbb{Q}$, which naturally fits in the language of $\Gamma(1)$-test objects in the sense of N. Katz [K76]. One can leave the role of G_k to $\pi_1(S, \bar{b})$ for $S = \mathrm{Spec}(B)$ with a chosen base point $\bar{b}$ on S, and start the same group-theoretical construction from the monodromy representation $\varphi_{\overrightarrow{\mathfrak{w}}} : \pi_1(S, \bar{b}) \to \mathrm{Aut}(\pi)$. Writing $|\mathcal{C}| := \{m \in \mathbb{N} \mid \mathbb{Z}/m\mathbb{Z} \in \mathcal{C}\}$, $\mathbb{Z}_\mathcal{C} := \varprojlim_{M \in |\mathcal{C}|}(\mathbb{Z}/M\mathbb{Z})$, we then obtain the invariants (as continuous mappings in profinite topology)

$$\mathbb{E}_m : \pi_1(S, \bar{b}) \times \mathbb{Z}_\mathcal{C}^2 \to \mathbb{Z}_\mathcal{C} \quad (m \in |\mathcal{C}|). \tag{1.6}$$

These invariants, collected over all $m \in |\mathcal{C}|$, will turn out to recover the meta-abelian reduction of $\varphi_{\overrightarrow{\mathfrak{w}}}$ in π/π'' (Proposition 3.4.5(ii)). Meanwhile, $\mathcal{E}_\sigma$ is defined on the pro-$\mathcal{C}$ congruence kernel $\pi_1(S^\mathcal{C}, \bar{b}^\mathcal{C})$, the kernel of the monodromy representation $\rho^\mathcal{C} : \pi_1(S, \bar{b}) \to \mathrm{Aut}(\pi^{\mathrm{ab}}) \cong \mathrm{GL}_2(\mathbb{Z}_\mathcal{C})$ in the abelianization π^{ab} of π. One then also gets a generalization of the above formula (1.5) on $\pi_1(S^\mathcal{C}, \bar{b}^\mathcal{C})$ (cf. Theorem 6.10.3).

At this stage, enters the anabelian geometry of the moduli space $M_{1,1}^\omega$ $(= \mathrm{Spec}(\mathbb{Q}[g_2, g_3, 1/\Delta]))$ and the universal once punctured elliptic curve $M_{1,2}^\omega$ over it: In the geometric fundamental group of the punctured Tate elliptic curve $\mathrm{Tate}(q) \setminus \{O\}$, we can specify a standard generator system $\mathbf{x}_1, \mathbf{x}_2, \mathbf{z}$ with relation $[\mathbf{x}_1, \mathbf{x}_2]\mathbf{z} = 1$ by the van Kampen gluing of $\pi_1(\mathbf{P}^1 - \{0, 1, \infty\})$ along Néron poly-

gons as considered in [IN97], [N99-02, §4]. Then, choosing such a generator system in the geometric fiber of an arbitrary elliptic curve $E\setminus\{O\}\to S$ over $\bar{b}$ corresponds to choosing a specific path on $M^{\omega}_{1,1}$ from the representing point of $\bar{b}$ to the locus of the Tate elliptic curve $\mathrm{Tate}(q)/\mathbb{Q}((q))$. In §5, we will discuss location of several significant tangential base points on $M^{\omega}_{1,2}$ and $M^{\omega}_{1,1}$ in the spirit of our collaboration with L. Schneps [NS00] and H. Tsunogai–S. Yasuda [NT03-06, NTY10] on the "Galois–Teichmüller theory" of Grothendieck's programme [G84].

Our first main theorem is an explicit formula for the values of $\mathbb{E}_m(\sigma;u,v)$ in approximation modulo arbitrarily higher modulus in $\mathbb{Z}_{\mathcal{C}}$:

Theorem A (Modular unit formula, Theorem 6.2.1). *Let $\sigma\in\pi_1(S,\bar{b})$. For any $M\in|\mathcal{C}|$ and $(u,v)\in\mathbb{Z}^2_{\mathcal{C}}\setminus(m\mathbb{Z}_{\mathcal{C}})^2$, pick two pairs of rational integers $\mathbf{r}=(r_1,r_2)$, $\mathbf{s}=(s_1,s_2)$ such that $\mathbf{r}\equiv(u,v)$ mod $mM^2 2^{\varepsilon}$ (where $\varepsilon=0,1$ according as $2\nmid M$, $2\,|\,M$ respectively) and $\binom{s_1}{s_2}\equiv\rho^{\mathcal{C}}(\sigma)\binom{r_1}{r_2}$ mod $m^2M^2e_{\mathcal{C}}$, where $e_{\mathcal{C}}=1,3,4$, or 12 according as $\mathcal{C}$ contains both, either or none of $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ (cf. §5.10). Then*

$$\mathbb{E}_m(\sigma;u,v)\equiv\tfrac{1}{12}\big(\kappa^{m,m^2M^2}_{\mathbf{r}/m\to\mathbf{s}/m}(\sigma)-\rho_{\Delta(E,mdx/y)}(\sigma)\big)\ \mathrm{mod}\ M^2,$$

where $\kappa^{m,m^2M^2}_{\mathbf{r}/m\to\mathbf{s}/m}(\sigma)\in\hat{\mathbb{Z}}_{\mathcal{C}}$ is defined by certain Kummer properties of power roots of modular units "$\sigma(\sqrt[*]{\theta_{\mathbf{r}/m}})/(\sqrt[*]{\theta_{\mathbf{s}/m}})$" for rational pairs $\mathbf{r}/m=(r_1/m,r_2/m)$, $\mathbf{s}/m=(s_1/m,s_2/m)$ with specified branches of $\sqrt[*]{\square}$'s introduced in §5. □

Here we also note that by definition, $\mathbb{E}_m(\sigma;0,0)=0$ and that $\mathbb{E}_m(\sigma;u,v)$ for $(u,v)\in(m\mathbb{Z}_{\mathcal{C}})^2$ can be evaluated from $\mathbb{E}_m(\sigma;u+1,v)$, $\mathbb{E}_m(\sigma;1,0)$ together with an elementary arithmetic term (cf. Proposition 3.4.8).

Application of the above theorem to the complex analytic case of the universal (once punctured) elliptic curve provides us with exact integer values of $\mathbb{E}_m(\sigma;u,v)$ for $\sigma\in B_3$ (3-strand braids) and $(u,v)\in\mathbb{Z}^2$, as the congruence assumptions modulo $mM^2 2^{\varepsilon}$, $m^2M^2e_{\mathcal{C}}$ turn out to be void (or hold true for $M=\infty$) when $\mathbf{s}$ is obtained from $\mathbf{r}=(u,v)$ by multiplication with a matrix in $\mathrm{SL}_2(\mathbb{Z})$. In §7, we are led to evaluation of the quantity $\kappa^{m,m^2\infty}_{\mathbf{r}/m\to\mathbf{s}/m}(\sigma)$ through examining specific choices of logarithms of Siegel units. It turns out that the main periodic term can be described in terms of the generalized Rademacher function of weight two studied by B. Schoeneberg [Sch74] and G. Stevens [St82, St85, St87], which is, for $x=(x_1,x_2)\in\mathbb{Q}^2$ and $A=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$, given explicitly by

$$\Phi_x(A)\ (=\Phi_x(-A))$$
$$=\begin{cases}-\dfrac{P_2(x_1)}{2}\dfrac{b}{d} & (c=0),\\[2ex] -\dfrac{P_2(x_1)}{2}\dfrac{a}{c}-\dfrac{P_2(ax_1+cx_2)}{2}\dfrac{d}{c}+\displaystyle\sum_{i=0}^{c-1}P_1\left(\frac{x_1+i}{c}\right)P_1\left(x_2+a\frac{x_1+i}{c}\right) & (c>0),\end{cases}$$

where P_1 and P_2 denote the fist and second periodic Bernoulli functions respectively. We shall also deduce an explicit formula evaluating the complementary non-periodic term "$K_x(A) \in \mathbb{Q}$" by comparing the infinite product expansions of Siegel units and generalized Dedekind functions. Our main assertion in this setting is then summarized as follows:

Theorem B (Generalized Dedekind sum formula, Theorem 7.2.3). *Let $B_3 = \langle \tau_1, \tau_2 \rangle$ be the braid group of three strands with relation $\tau_1\tau_2\tau_1 = \tau_2\tau_1\tau_2$, and let $\rho_\Delta : B_3 \to \mathbb{Z}$ be the abelianization homomorphism given by $\tau_1, \tau_2 \mapsto -1$. For each $\sigma \in B_3$, let $A_\sigma \in \mathrm{SL}_2(\mathbb{Z})$ denote the transposed matrix of the image of σ in the homomorphism $B_3 \to \mathrm{SL}_2(\mathbb{Z})$ determined by $\tau_1 \mapsto \left(\begin{smallmatrix} 1 & 0 \\ -1 & 1 \end{smallmatrix}\right)$, $\tau_2 \mapsto \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Let $m \geq 1$, and for $(r_1, r_2) \in \mathbb{Z}^2 \setminus (m\mathbb{Z})^2$, set $x = (x_1, x_2) = (r_1/m, r_2/m)$. Then, for $\sigma \in B_3$,*

$$\mathbb{E}_m(\sigma; r_1, r_2) = K_x(A_\sigma) - \Phi_x(A_\sigma) - \tfrac{1}{12}\rho_\Delta(\sigma). \qquad \square$$

Since each of the above three terms $\frac{1}{12}\rho_\Delta(\sigma)$, $\Phi_x(A_\sigma)$ and $K_x(A_\sigma)$ generally has a rational value with denominator, it would be of interest to find how the integer value $\mathbb{E}_m(\sigma; r_1, r_2)$ can be composed of those three rational values in the above right hand side, say, in computer calculations (see Example 7.2.4). We will also obtain an explicit formula to compute $\mathbb{E}_m(\sigma; mk_1, mk_2)$ from elementary arithmetic functions (see Proposition 7.5.1).

As mentioned above, our main motivation is to construct an elliptic analogue of Ihara's universal power series for Jacobi sums [Ih86a] hoping to discuss analogs of deep arithmetic phenomena in $\pi_1(\mathbf{P}^1 - \{0, 1, \infty\})$ studied by Deligne, Ihara and other authors (cf. e.g., [De89], [Ih90, Ih02], [MS03] etc.) Our approach basically follows the combinatorial group-theoretical line of S. Bloch [Bl84] and H. Tsunogai [Tsu95a], and the principal idea of our proof of Theorem A is, generalizing [N95], to closely observe monodromy permutations of inertia subsets in $\pi_1(E \setminus \{O\})$ distinguished by punctures on a certain family of meta-abelian coverings of $E\setminus\{O\}$. Along with our early work [N95, N99] together with subsequent complementary results of [N01, N02j, N03j], the author realized that the main obstruction to integration of his results in a uniform theory lies in the problem of descending the field of definition of $\mathcal{E}_\sigma$ from $G_{k(E_{l^\infty})}$ to G_k. This obstruction is, as suggested in the equation derived by Tsunogai (Remark 3.4.4), an essential feature which distinguishes the treatment of Galois representations in $\pi_1(E - \{O\})$ from those in $\pi_1(\mathbf{P}^1 - \{0, 1, \infty\})$. We hope that our innovation of the bypass object $\mathbb{E}_m(\sigma; u, v)$ could provide one possible solution to the problem. It is probably good to stress that, in our approach here, the extension is constructed so as to keep integrality of values of invariants even after extension to G_k. In topological higher genus mapping class groups, this sort of extension problem was successfully treated by

S. Morita [Mor93] by introducing the "extended Johnson homomorphism" which keeps the cocycle property but allows denominators. In the genus one case, we should still leave it for future studies to investigate an unknown extension in Morita's direction.

Connections of $\mathcal{E}_\sigma$ to Eisenstein series of weight > 2, especially to Eichler–Shimura type periods of them have been studied to some extent in [N01, N02j, N03j]. In future work, we hope to discuss them in more detail. More investigation of anabelian geometry of moduli spaces of pointed elliptic curves should also be pursued from the viewpoint of [NT03-06], [NTY10].

Before closing this introduction, we should like to mention some related work suggesting further hopeful directions. The good reduction criterion of Oda–Tamagawa (cf. [Od90-95], [Ta97]) ensures that one can think about the pro-l version of $\mathbb{E}_m(\sigma; u, v)$, say, at Frobenius elements σ for primes (not equal to l, bad primes), in which we might expect some newtype arithmetic nature of elliptic curves. The fundamental groups of once punctured elliptic curves have also been studied in depth by M. Asada [As01], B. Enriquez [E10], R. Hain [Ha97], M. Kim [Ki07], S. Mochizuki [Moc02], J. Stix [Sti08] and H. Tsunogai [Tsu95b, Tsu03], which enlarges (and enriches) our perspective on these fundamental objects. Z. Wojtkowiak [Woj04] studied Galois actions on torsors of paths on once punctured elliptic curves from a viewpoint close to [N95]. It would certainly be interesting to investigate this direction from the point of view of the present paper. It seems apparently relevant to the motivic aspects of elliptic polylogarithms studied by several authors, e.g., Beilinson–Levin [BL94] and Bannai–Kobayashi [BK10]. At the time of writing this paper, however, the author does not see explicit links between their work and ours. We hope to see relations to their work in future studies.

The construction of this paper is as follows. In §2, we prepare some terminology on elliptic curves and our basic objects, especially recalling some language of $\Gamma(N)$-test objects in the sense of N. Katz. In §3, we introduce and discuss our main object $\mathbb{E}_m$ mainly from the combinatorial group-theoretical viewpoint. In §4, we review basic modular forms, especially, Siegel units and Eisenstein series and their behaviors under the GL_2-action. In §5, we focus on the universal once punctured elliptic curves $M^{\omega}_{1,2}$ over the moduli space $M^{\omega}_{1,1}$ and discuss their anabelian geometry from the viewpoint of Galois–Teichmüller theory in the sense of Grothendieck [G84], Drinfeld [Dr90] and Ihara [Ih90]. In §6, we present our first main theorem (Theorem A, modular unit formula), and the most part of that section is devoted to its proof. In §7, we apply the modular unit formula to the complex analytic model, and deduce our second main theorem (Theorem B, generalized Dedekind sum formula).

§2. Some terminology on elliptic curves

In this section, we shall prepare some notation and terminology on elliptic curves and their moduli space, following mainly the paper by N. Katz [K76]. Since we will only be concerned with the Galois theory of fundamental groups of algebraic varieties of characteristic zero, we restrict ourselves to treating schemes over $\mathbb{Q}$-algebras.

§2.1. $\Gamma(1)$-test objects

An *elliptic curve over a $\mathbb{Q}$-algebra B* is a smooth family of elliptic curves over $S = \mathrm{Spec}(B)$ with a fixed 0-section $O : S \to E$ of the structure morphism $f : E \to S$. The direct image sheaf of the relative differentials $\omega_{E/S} := f_*(\Omega_{E/S})$ is a locally free sheaf over $\mathcal{O}_S$; suppose that we are given a global basis ω of $\omega_{E/S}$ ("nowhere vanishing invariant differential"). Following [K76], we shall call the triple (E, O, ω) a $\Gamma(1)$-*test object* defined over B. If I_O denotes the ideal sheaf of the (image of the) zero section O, then, for each $n \geq 2$, the direct image sheaf $f_*(I_O^{-n})$ is locally free of rank n on S (cf. [KM85, Chap. 2]). Thus, everywhere locally, one has an affine neighborhood $\mathrm{Spec}(A) \subset S$ such that the restriction $E_A = E \otimes_B A$ has a formal parameter t near the zero section O and a unique basis $\{1, x, y\}$ of $f_*(I_O^{-3})$ such that

(1) the formal completion $(E_A/O)^\wedge$ is isomorphic to $\mathrm{Spf}(A[[t]])$;
(2) $\omega|_{E_A}$ is of the form $(1 + O(t))dt$;
(3) $x \sim t^{-2}$, $y \sim -2t^{-3}$ ($\sim$ means "up to a factor of $1 + O(t)$");
(4) the affine ring $H^0(E_A \setminus \{O\}, \mathcal{O}) = \varinjlim_n H^0(E_A, I_O^{-n})$ is of the form

$$A[x, y]/(y^2 = 4x^3 - g_2 x - g_3) \quad \text{for some } g_2, g_3 \in A.$$

The above x, y and g_2, g_3 are uniquely determined on each $\mathrm{Spec}(A)$ independently of the choice of t's. Moreover, $g_2^3 - 27g_3^2 \in A^\times$.

§2.2. The moduli space $M_{1,1}^\omega$ and associated parameters

The universal $\Gamma(1)$-test object is defined over the affine variety

$$M_{1,1}^\omega := \mathrm{Spec}\left(\mathbb{Q}\left[g_2, g_3, \frac{1}{g_2^3 - 27g_3^2}\right]\right)$$

where g_2, g_3 are indeterminates. We understand the superscript ω of $M_{1,1}^\omega$ here as only a symbol (not indicating a particular differential form etc.) Note that, over $M_{1,1}^\omega$, there is a canonical family of elliptic curves $\mathcal{E} \subset \mathbf{P}^2_{M_{1,1}^\omega}$ defined by

the equation $y^2z = 4x^3 - g_2xz^2 - g_3z^3$ with a specific zero section O given by $(x : y : z) = (0 : 1 : 0)$.

To see the universal property of $(\mathcal{E}/M^{\omega}_{1,1}, O, \omega = dx/y)$ for the moduli problem of $(E/B, O, \omega)$ (in characteristic zero), suppose we are given any $\Gamma(1)$-test object $(E/B, O, \omega)$. Pick any Zariski open covering $\mathcal{U} = \{\mathrm{Spec}(A_i)\}_{i\in I}$ of $S = \mathrm{Spec}(B)$ as in §2.1, and consider the family of representative morphisms $f_{A_i} : \mathrm{Spec}(A_i) \to M^{\omega}_{1,1}$. By the uniqueness of x, y and g_2, g_3 for each E_{A_i}, one sees that the f_{A_i} patch together to yield a (canonical) morphism $S \to M^{\omega}_{1,1}$.

It is obvious from the construction that any $\Gamma(1)$-test object $(E/B, O, \omega)$ can be realized as the pull-back of $(\mathcal{E}/M^{\omega}_{1,1}, O, \omega = dx/y)$ by a unique morphism $S = \mathrm{Spec}(B) \to M^{\omega}_{1,1}$. Through the pull-back morphisms, we in particular find specific elements $g_2, g_3 \in B$ and $x, y \in H^0(E, I_O^{-3})$ satisfying

$$E \setminus \{O\} = \mathrm{Spec}(B[x, y]/(y^2 = 4x^3 - g_2x - g_3)).$$

Then it turns out that $\omega = dx/y$ and the function $t = -2x/y$ could play the role of t of §2.1 globally over B. We shall call the tuple (x, y, g_2, g_3, t) the *associated parameter* for the $\Gamma(1)$-test object $(E/B, O, \omega)$.

§2.3. Weierstrass tangential base point

Let $(E/B, O, \omega)$ be a $\Gamma(1)$-test object with the associated parameter (x, y, g_2, g_3, t). In this and the following subsections, we assume that B is a regular domain ($\supset \mathbb{Q}$). Note that the formal power series ring $B[[t]]$ is then also a regular domain, hence in particular is a noetherian normal domain (cf. [Mh86, Th. 19.4, 19.5]).

Suppose we are given a geometric point $\bar{b} : \mathrm{Spec}(\Omega) \to S = \mathrm{Spec}(B)$ (Ω an algebraically closed field) which is defined by a ring homomorphism $B \to \Omega$. We shall define a tangential base point $\overrightarrow{\mathfrak{w}}_{\bar{b}}$ on $E \setminus \{O\}$ near the origin lying over $\bar{b}$ as follows, and call it the *Weierstrass tangential base point over* $\bar{b}$. Observe first that the coefficientwise application of the above ring homomorphism $B \to \Omega$ induces a homomorphism of $B[[t]]$ into the (algebraically closed) field of Puiseux power series, $\Omega\{\{t\}\} := \bigcup_{n=1}^{\infty} \Omega((t^{1/n}))$, which gives a base point for $\pi_1^O((E/O)^{\wedge})$, the fundamental group of the formal completion $(E/O)^{\wedge} = \mathrm{Spf}(B[[t]])$ with ramifications allowed only along the regular divisor O in the sense of Grothendieck–Murre [GM71]. Obviously this tangential base point naturally lies in the geometric fiber $E_{\bar{b}} = E \otimes_B \Omega$ over $\bar{b}$ minus O; denote it and its natural images on $E_{\bar{b}} \setminus \{O\}$, $(E/O)^{\wedge}$ by the same symbol $\overrightarrow{\mathfrak{w}}_{\bar{b}}$ for simplicity. Also let $\overrightarrow{\mathfrak{w}}'_{\bar{b}}$, $\bar{b}'$ be their natural images in the universal family $\mathcal{E}/M^{\omega}_{1,1}$. Then, applying the Grothendieck–Murre theory ([GM71]), we obtain a commutative diagram of exact sequences of fundamental groups:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \hat{\mathbb{Z}}(1) & \longrightarrow & \pi_1^O((E/O)^\wedge, \overrightarrow{\mathfrak{w}}_{\bar{b}}) & \longrightarrow & \pi_1(S, \bar{b}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}}) & \longrightarrow & \pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}}) & \longrightarrow & \pi_1(S, \bar{b}) & \longrightarrow & 1 \\
 & & \| & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \pi_1(\mathcal{E}_{\bar{b}'} \setminus \{O\}, \overrightarrow{\mathfrak{w}}'_{\bar{b}}) & \longrightarrow & \pi_1(\mathcal{E} \setminus \{O\}, \overrightarrow{\mathfrak{w}}'_{\bar{b}}) & \longrightarrow & \pi_1(M^\omega_{1,1}, \bar{b}') & \longrightarrow & 1
\end{array}$$

In fact, the exactness of the bottom sequence follows from the fact that $M^\omega_{1,1}(\mathbb{C})$ is $K(\pi, 1)$ and from the center-triviality of $\pi_1(E_{\bar{b}} \setminus \{O\})$. The injectivity of the left horizontal arrow follows from this observation (and from the GAGA interpretation of $\hat{\mathbb{Z}}(1)$), since the upper left vertical arrow (hence the upper middle vertical one too) is injective (it is an embedding of $\hat{\mathbb{Z}}(1)$ into a free profinite group of rank 2). This explains the exactness of the above three lines.

§2.4. Weierstrass tangential section

We keep our assumption that B is a regular domain $\supset \mathbb{Q}$. We shall write $\mathcal{R}(*)$ to denote the total quotient ring of $*$ (the fraction field when $*$ is a domain).

In the above diagram, we would also like to have a canonical section $\pi_1(S, \bar{b}) \to \pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ (depending only on the choice of t and its power root system $\{t^{1/n}\}$), which we shall call the *Weierstrass tangential section*. The following argument to construct such a section may be viewed as a simple digest of (a special case of) "tangential morphism" explained in [Ma97] or in a more thorough formulation using log geometry [Moc99], [Ho09]. Here we shall argue in the classical context using the device of Grothendieck–Murre [GM71] to construct an exact functor of Galois categories $\Phi : \mathrm{Rev}^O((E/O)^\wedge) \to \mathrm{Rev}(S)$ (in the sense of SGA1 [GR71, Exp. V]) which produces a section $\pi_1(\mathrm{Spec}(B), \bar{b}) \to \pi_1^O(\mathrm{Spf}(B[[t]]), \overrightarrow{\mathfrak{w}}_{\bar{b}})$ as follows.

First, we interpret the top exact sequence in the diagram of §2.3 under the assumption that $\bar{b}$ is a generic geometric point, i.e., Ω includes the regular domain B. Let $B^{\mathrm{ur}} \subset \Omega$ be the universal etale cover of B. The structure of $\pi_1^O((E/O)^\wedge, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ as an extension of $\pi_1(B, \bar{b})$ by $\hat{\mathbb{Z}}(1)$ implies that any connected object of $\mathrm{Rev}^O((E/O)^\wedge)$, i.e., a finite connected cover of $(E/O)^\wedge = \mathrm{Spf}(B[[t]])$ with ramification only over $\{t = 0\}$, is dominated by $\mathrm{Spf}(B^{\mathrm{ur}}[[t^{1/n}]])$ for some multiplicatively large enough n.

Given any $Y = \mathrm{Spf}(C)$ of $\mathrm{Rev}^O((E/O)^\wedge)$, take a multiplicatively large enough n so that each component of Y is dominated by $\mathrm{Spf}(B^{\mathrm{ur}}[[t^{1/n}]])$. Form the $B[[t^{1/n}]]$-algebra $C \otimes_{B[[t]]} B[[t^{1/n}]]$ and denote by $\tilde{C}$ the integral closure of $B[[t^{1/n}]]$ in $\mathcal{R}(C \otimes_{B[[t]]} B[[t^{1/n}]])$. Then, by Abhyankar's lemma and the Zariski–

Nagata purity theorem, $\tilde{C}$ is etale over $B[[t^{1/n}]]$ in the category of schemes (cf. [GM71, 4.3.4 a])). Let $\hat{C}$ denote the formal completion of $\tilde{C}$ along $t = 0$, which is etale over $\mathrm{Spf}(B[[t^{1/n}]])$ in the category of formal schemes ([GM71, Prop. 3.2.3]). But since the category of finite etale covers over $\mathrm{Spf}(B[[t^{1/n}]])$ (for fixed n) is equivalent to the category of those over $\mathrm{Spec}(B)$ ([GM71, 3.2.4]; indeed, only its easy direction suffices here), there corresponds to $\hat{C}$ a finite etale cover $\Phi(Y)$ over $S = \mathrm{Spec}(B)$ which turns out to be determined independently of n.

This construction gives an exact functor $\Phi : \mathrm{Rev}^{O}((E/O)^{\wedge}) \to \mathrm{Rev}(S)$. Indeed, for a given diagram $\mathrm{Spf}(C) \to \mathrm{Spf}(D) \leftarrow \mathrm{Spf}(C')$ in $\mathrm{Rev}^{O}((E/O)^{\wedge})$, pick n multiplicatively large enough so that $\mathrm{Spf}(B^{\mathrm{ur}}[[t^{1/n}]])$ dominates each component of $\mathrm{Spf}(C) \cup \mathrm{Spf}(C') \cup \mathrm{Spf}(D)$. Then we have (by use of [B-1, Chap. 2, §3, Prop. 8] (twice) and [B-1, §5, Prop. 3] (once))

$$(C \otimes_{B[[t]]} B[[t^{1/n}]]) \otimes_{D \otimes B[[t^{1/n}]]} (C' \otimes_{B[[t]]} B[[t^{1/n}]]) = (C \otimes_{D} C') \otimes_{B[[t]]} B[[t^{1/n}]].$$

Through the LHS above, $\tilde{C} \otimes_{\tilde{D}} \tilde{C}'$ sits in the total quotient ring $\mathcal{R}\big((C \otimes_D C') \otimes_{B[[t]]} B[[t^{1/n}]]\big)$ of the RHS as an etale cover over $B[[t^{1/n}]]$ which is itself normal and has the same total quotient ring (EGA I, 3.4.9). From this observation it follows that the functor Φ preserves fiber products. That Φ preserves finite sums follows immediately from a basic property of integral closures in products of rings ([B-2, Chap. 5, §1, Prop. 9]). It is also obvious from the construction that a non-empty Y gives rise to a non-empty $\Phi(Y)$. Thus, by [GR71, Exp. V, Prop. 6.1], we conclude that Φ gives an exact functor of Galois categories.

Conversely, if a connected finite etale cover $\mathrm{Spec}(B')$ over $\mathrm{Spec}(B)$ is given $(B \subset B' \subset B^{\mathrm{ur}})$, then the above Φ turns $Y = \mathrm{Spf}(B'[[t]])$ back to $\mathrm{Spec}(B')$ itself. Thus, the functor $Y \mapsto \Phi(Y)$ inverts the canonical pull-back functor $\mathrm{Rev}(S) \to \mathrm{Rev}^{O}((E/O)^{\wedge})$.

Once the functor Φ is obtained, it is not difficult to check that, for any base point $\bar{b}$ on S, the fiber functor $\overrightarrow{\mathfrak{w}}_{\bar{b}} : \mathrm{Rev}^{O}((E/O)^{\wedge}) \to \mathit{Sets}$ is the composite of Φ with $\bar{b} : \mathrm{Rev}(S) \to \mathit{Sets}$. Slightly more generally, for any two base points $\bar{b}$, $\bar{b}'$ on S, there arises a natural mapping of etale homotopy classes of chains $\pi_1(S; \bar{b}, \bar{b}') \to \pi_1(E \setminus \{O\}; \overrightarrow{\mathfrak{w}}_{\bar{b}}, \overrightarrow{\mathfrak{w}}_{\bar{b}'})$. It is also a rather routine task to see that this gives a section of the canonical projection $\pi_1(E \setminus \{O\}; \overrightarrow{\mathfrak{w}}_{\bar{b}}, \overrightarrow{\mathfrak{w}}_{\bar{b}'}) \to \pi_1(S; \bar{b}, \bar{b}')$. We shall write the constructed section associated with the parameter $t = -2x/y$ as

$$s_{\overrightarrow{\mathfrak{w}}} : \pi_1(S; \bar{b}, \bar{b}') \to \pi_1(E \setminus \{O\}; \overrightarrow{\mathfrak{w}}_{\bar{b}}, \overrightarrow{\mathfrak{w}}_{\bar{b}'})$$

and call it the Weierstrass tangential section (in π_1).

§2.5. Pro-$\mathcal{C}$ monodromy representation

Below, we suppose that any full class $\mathcal{C}$ of finite groups is given and denote the maximal pro-$\mathcal{C}$ quotient of $\Pi_{1,1}$ by $\Pi_{1,1}(\mathcal{C})$. Denote by $|\mathcal{C}|$ the set of positive integers N with $\mathbb{Z}/N\mathbb{Z} \in \mathcal{C}$, and write $\mathbb{Z}_{\mathcal{C}} = \varprojlim_{N \in |\mathcal{C}|} (\mathbb{Z}/N\mathbb{Z})$.

We continue our discussion of a $\Gamma(1)$-test object (E, O, ω) over a regular algebra $B(\supset \mathbb{Q})$ which gives rise to the exact sequence discussed in §2.3:

$$1 \to \Pi_{1,1} = \pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}}) \to \pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}}) \to \pi_1(S, \bar{b}) \to 1$$

with the Weierstrass section $s_{\overrightarrow{\mathfrak{w}}}$ (§2.4). Conjugation with $s_{\overrightarrow{\mathfrak{w}}}$ induces a monodromy representation

$$\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}} : \pi_1(S, \bar{b}) \to \mathrm{Aut}(\Pi_{1,1}(\mathcal{C})).$$

We shall call it the *pro-$\mathcal{C}$ monodromy representation* arising from the $\Gamma(1)$-test object $(E/B, O, \omega)$. By the comparison theorem ([GR71]), the geometric fundamental group $\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ may be identified with a free profinite group presented as $\Pi_{1,1} = \langle \mathbf{x}_1, \mathbf{x}_2, \mathbf{z} \mid [\mathbf{x}_1, \mathbf{x}_2]\mathbf{z} = 1 \rangle$ so that $\mathbf{z}$ generates an inertia subgroup over O. We will take $\mathbf{z}$ to be a unique generator of the image of $\pi_1^O((E_{\bar{b}}/O)^\wedge, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ (§2.4) having the monodromy property $t^{1/n}|_{\mathfrak{a}_{\mathbf{z}}} = \zeta_n^{-1} t^{1/n}$ $(n \geq 1)$ in our later terminology of §6.1. It is then easy to see that $\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}}(\pi_1(S, \bar{b}))$ stabilizes $\langle \mathbf{z} \rangle$ and acts on it by the $\mathcal{C}$-adic cyclotomic character.

The monodromy representation in the maximal abelian quotient of $\Pi_{1,1}(\mathcal{C})$ gives the action on the first etale homology group of the corresponding elliptic curve. It can be described in a more concrete way by matrices as follows. The abelianization of $\Pi_{1,1}(\mathcal{C})$ is nothing but $\pi_1^{\mathcal{C}}(E_{\bar{b}})$ $(\cong \mathbb{Z}_{\mathcal{C}}^2)$, which is canonically identified with the $\mathcal{C}$-adic Tate module $\varprojlim_{N \in |\mathcal{C}|} E_{\bar{b}}[N]$. Reduction of $\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}}$ to this quotient gives the representation

$$\rho^{\mathcal{C}} : \pi_1(S, \bar{b}) \to \mathrm{GL}(\mathbb{Z}_{\mathcal{C}}^2) = \mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}}).$$

§2.6. Isogeny cover by multiplication by N

For convenience of illustrations, we suppose that an identification of the geometric fundamental group $\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ with a free profinite group $\Pi_{1,1} = \langle \mathbf{x}_1, \mathbf{x}_2, \mathbf{z} \mid [\mathbf{x}_1, \mathbf{x}_2]\mathbf{z} = 1 \rangle$ is given and fixed, so that $\mathbf{z}$ generates the (specific) inertia group over O as in the previous subsection.

Let $N \in |\mathcal{C}|$. Then there is a canonical isomorphism between the set $E_{\bar{b}}[N]$ of N-division points of $E_{\bar{b}}$ and the quotient $\pi_1(E_{\bar{b}})/N\pi_1(E_{\bar{b}})$, and after selecting the generators $\mathbf{x}_1, \mathbf{x}_2$ of $\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}}) \cong \Pi_{1,1}$, we may identify the latter quotient with $(\mathbb{Z}/N\mathbb{Z})^2$ by $\mathbf{x}_1 \mapsto (1, 0)$, $\mathbf{x}_2 \mapsto (0, 1)$. Let $\rho^N : \pi_1(S, \bar{b}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the monodromy representation obtained as the N-th component of $\rho_{\mathcal{C}}$ under this

identification, and let $(S^N = \mathrm{Spec}(B^N), \bar{b}^N)$ be a pointed etale cover of $(S, \bar{b})$ corresponding to the kernel of ρ^N. If E^N denotes the pull-backed elliptic curve over B^N, then the group scheme $E^N[N]$, the kernel of the isogeny $E^N \to E^N$ given by multiplication by N, is a finite etale cover of B^N with trivial monodromy, hence is the disjoint union of N^2 copies of B^N which bijectively corresponds to the set $E_{\bar{b}}[N]$. Through this identification, the elliptic curve E^N/B^N has B^N-rational sections of N-division points labeled by $(\mathbb{Z}/N\mathbb{Z})^2$. This, together with the nowhere vanishing differential ω_N inherited from ω, defines a $\Gamma(N)$-test object $(E^N/B^N, \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E^N[N], \omega_N)$ in the sense of [K76].

The ring B_N necessarily contains μ_N, the N-th roots of unity. Indeed, there is a morphism of flat commutative group schemes $e_N : E^N[N] \times E^N[N] \to \mu_N$ over B^N called the *Weil pairing*. This canonically defines a primitive N-th root of unity $\zeta_N = e_N(\alpha(1,0), \alpha(0,1)) \in B^N$.

One can choose a sequence of pointed covers $(S^N, \bar{b}^N)$ of $(S, \bar{b})$ to be multiplicatively compatible for all $N \in |\mathcal{C}|$ so that their inverse limit $(S^{\mathcal{C}} = \mathrm{Spec}(B^{\mathcal{C}}), \bar{b}^{\mathcal{C}})$ forms a pro-etale cover of $(S, \bar{b})$. The associated elliptic curve $E^{\mathcal{C}}/B^{\mathcal{C}}$ has the rational $\mathcal{C}$-torsion sections whose "Tate module" is denoted by $\mathbb{Z}^2_{\mathcal{C}}$. Under this setting, the fundamental group $\pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})$ is, as a subgroup of $\pi_1(S, \bar{b})$, nothing but the kernel of the representation $\rho^{\mathcal{C}} : \pi_1(S, \bar{b}) \to \mathrm{GL}(\mathbb{Z}^2_{\mathcal{C}})$. We shall call it the *pro-$\mathcal{C}$ congruence kernel* of $\pi_1(S, \bar{b})$. Note that the restriction of $\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}}$ to the pro-$\mathcal{C}$ congruence kernel is the same as the monodromy representation of $\pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})$ on $\pi_1^{\mathcal{C}}((E^{\mathcal{C}})_{\bar{b}^{\mathcal{C}}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}^{\mathcal{C}}})$ for the $\Gamma(1)$-test object $(E^{\mathcal{C}}/B^{\mathcal{C}}, O, \omega_{\mathcal{C}})$.

§2.7. Anti-homomorphism $\mathfrak{a} : \pi_1(S, \bar{b}) \to \mathrm{Aut}(S^N/S)$

The covering transformation group $\mathrm{Aut}(S^N/S)$ acts on S^N from the left. The elements of $\mathrm{Aut}(S^N/S)$ bijectively correspond to the image of $\rho^N : \pi_1(S, \bar{b}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as follows. Let $S^N(\bar{b})$ be the geometric fiber of $S^N \to S$ over $\bar{b}$ which contains the above selected particular point $\bar{b}^N$. Then the fundamental group $\pi_1(S, \bar{b})$ acts on $S^N(\bar{b})$ from the left. The action of $\mathrm{Aut}(S^N/S)$ on $S^N(\bar{b})$ commutes with that of $\pi_1(S, \bar{b})$ and is simply transitive. Therefore, for each $\sigma \in \pi_1(S, \bar{b})$, there is a unique $\mathfrak{a}_\sigma \in \mathrm{Aut}(S^N/S)$ such that $\sigma(\bar{b}^N) = \mathfrak{a}_\sigma(\bar{b}^N)$. This mapping satisfies

$$\mathfrak{a}_{\sigma\sigma'} = \mathfrak{a}_{\sigma'}\mathfrak{a}_\sigma \quad (\sigma, \sigma' \in \pi_1(S, \bar{b})) \tag{2.7.1}$$

and induces an anti-isomorphism

$$\mathfrak{a}^N : \mathrm{Im}(\rho^N) \xrightarrow{\sim} \mathrm{Aut}(S^N/S). \tag{2.7.2}$$

By the anti-functoriality of $\mathrm{Spec}(*)$, each $\mathfrak{a} \in \mathrm{Aut}(S^N/S)$ comes from a unique automorphism of the ring B^N which we shall write as $b \mapsto b|_{\mathfrak{a}}$ $(b \in B^N)$. Note that

the mapping $\sigma \mapsto (\,|_{\mathfrak{a}_\sigma})$ gives a (non-canonical) isomorphism $\mathrm{Im}(\rho) \cong \mathrm{Aut}(B^N/B)$. If we change the choice of $\bar{b}^N$ in $S^N(\bar{b})$, then the above anti-homomorphism differs by conjugation by an element of $\mathrm{Aut}(S^N/S)$.

With each morphism $\phi : T = \mathrm{Spec}(R) \to S^N$ there is associated a $\Gamma(N)$-test object $(E_\phi/R, \alpha_\phi : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E_\phi[N], \omega_\phi)$ by natural fiber product formation. Given an automorphism $\mathfrak{a} \in \mathrm{Aut}(S^N/S)$, we obtain another morphism $\phi' = \mathfrak{a} \circ \phi$ and the induced $\Gamma(N)$-test object $(E_{\phi'}, \alpha_{\phi'} : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E_{\phi'}[N], \omega_{\phi'})$. Suppose that the morphisms ϕ, ϕ' correspond to ring homomorphisms $\phi_R, \phi'_R : B^N \to R$ respectively. Then the values of the "functions" b and $b|_{\mathfrak{a}} \in B^N$ at those T-valued points ϕ, ϕ' are related by

$$\phi'_R(b) = \phi_R(b|_{\mathfrak{a}}) \quad (b \in B^N,\ \phi' = \mathfrak{a} \circ \phi). \tag{2.7.3}$$

[For example, if $s \in S^N(\mathbb{C})$ is any complex point, then $b(\mathfrak{a}s) = (b|_{\mathfrak{a}})(s)$.] Since the two morphisms $T \to S$ through ϕ, ϕ' are the same, we may canonically identify $E_\phi = E_{\phi'}$. Thus, we have

$$\alpha_{\phi'} = \alpha_\phi \circ \rho^N(\sigma) \quad (\phi' = \mathfrak{a}_\sigma \circ \phi). \tag{2.7.4}$$

Using this and a standard argument on the Weil pairing, one sees that

$$(\zeta_N|_{\mathfrak{a}_\sigma}) = \zeta_N^{\det(\rho^N(\sigma))} = \zeta_N^{\chi(\sigma)} \quad (N \in |\mathcal{C}|,\ \sigma \in \pi_1(S, \bar{b})), \tag{2.7.5}$$

where $\chi : \pi_1(S, \bar{b}) \to \mathbb{Z}_{\mathcal{C}}^\times$ the $\mathcal{C}$-adic cyclotomic character.

§2.8. Relation of $\rho^N(\sigma)$ and $\mathfrak{a}^N(\sigma)$ on $M_{1,1}[N]$

Now we shall consider the moduli stack $M_{1,1}$ of elliptic curves. The relative moduli problem of naive level N structures for $N \geq 3$ over elliptic curves is known to be relatively representable by a scheme $M_{1,1}[N]$ which is etale over the stack $M_{1,1}$ with Galois group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Write (E, O) for the universal family of elliptic curves over $M_{1,1}$, and (E^N, O) for its pull-back over $M_{1,1}[N]$ which has the (universal) level N-structure $\alpha^N : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E^N[N]$. Pick any base point $\bar{b}$ on $M_{1,1}$ and its lift $\bar{b}^N$ on $M_{1,1}[N]$. Then we obtain the identification $\alpha_{\bar{b}^N} : (\mathbb{Z}/N\mathbb{Z})^2 \cong E^N_{\bar{b}^N}[N] \cong E_{\bar{b}}[N]$. This gives us the monodromy representation $\rho^N : \pi_1(M_{1,1}, \bar{b}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. On the other hand, for each $\sigma \in \pi_1(M_{1,1}, \bar{b})$, let $\mathfrak{a}_\sigma$ be the unique automorphism of $M_{1,1}[N]$ over $M_{1,1}$ determined by $\sigma(\bar{b}^N) = \mathfrak{a}_\sigma(\bar{b}^N)$. Given a morphism $\phi : T = \mathrm{Spec}(R) \to M_{1,1}[N]$, we obtain a pull-backed elliptic curve E_ϕ over R with a level N-structure $\alpha_\phi : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E_\phi[N]$. The composition $\phi' = \mathfrak{a}_\sigma \circ \phi$ induces another elliptic curve $E_{\phi'}$ with level N-structure $\alpha_{\phi'} : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E_{\phi'}[N]$. Similar to (2.7.3)–(2.7.4), the two morphisms $T \to M_{1,1}$ through ϕ, ϕ' are

the same, so that after identifying $E_\phi = E_{\phi'}$, we have

$$\alpha_{\phi'} = \alpha_\phi \circ \rho^N(\sigma) \quad (\phi' = \mathfrak{a}_\sigma \circ \phi). \tag{2.8.1}$$

§2.9. Complex modular curves

The complex model of the "universal elliptic curve $\mathcal{E}/\{\pm 1\}$" over the "j-line" $Y_1(\mathbb{C}) := \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ is given as the quotient space of $\mathbb{C}\times\mathfrak{H}$ modulo the left action of $\mathbb{Z}^2 \rtimes \mathrm{SL}_2(\mathbb{Z})$ by (cf. [Mum83, §9])

$$(z,\tau) \mapsto \left(\frac{z+(2\pi i)(m\tau+n)}{c\tau+d}, \frac{a\tau+b}{c\tau+d}\right) \quad \left(\left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}),\ (m,n)\in\mathbb{Z}^2\right). \tag{2.9.1}$$

Fix an embedding $\mathbb{Q}(\mu_N) \hookrightarrow \mathbb{C}$. Then there arises a commutative diagram

$$\begin{array}{ccc} E^N \otimes \mathbb{C} & \longrightarrow & \mathbb{Z}^2 \rtimes \Gamma(N)\backslash\mathbb{C}\times\mathfrak{H} \\ \downarrow & & \downarrow \\ M_{1,1}[N]\otimes\mathbb{C} & \twoheadrightarrow & Y(N)\otimes\mathbb{C} = \Gamma(N)\backslash\mathfrak{H} \end{array} \tag{2.9.2}$$

where $\otimes\mathbb{C}$ are taken over $\mathbb{Q}(\mu_N)$, in such a way that the section $\alpha^N(x,y) : M_{1,1}[N] \to E^N$ $(x,y\in\mathbb{Z}/N\mathbb{Z})$ is mapped to the image of $\{((2\pi i)(\frac{\tau}{N}x+\frac{1}{N}y),\tau) \mid \tau\in\mathfrak{H}\}$.

Since the natural morphism of $M_{1,1}[N]$ to the modular curve $Y(N)/\mathbb{Q}(\mu_N)$ of level N is the quotient by $\{\pm 1\} \subset \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, each $\mathfrak{a}_\sigma$ $(\sigma\in\pi_1(M_{1,1},\bar{b}))$ induces also an automorphism $\mathfrak{a}_\sigma^*$ of $Y(N)$. Suppose $\mathfrak{a}_\sigma$ fixes μ_N. Then $\mathfrak{a}_\sigma^*$ gives a $\mathbb{Q}(\mu_N)$-automorphism of $Y(N)$ which naturally comes from an element of $\mathrm{Aut}(Y(N)/Y(1)\otimes\mathbb{Q}(\mu_N)) \cong \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$. Now, we realize that there arise two matrices in our discussions so far. One is the image $\rho^N(\sigma)\in\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, where $\rho^N : \pi_1(S,\bar{b}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is the monodromy representation in the N-division points (§2.6). The other is the covering transformation $A\in\mathrm{PSL}_2(\mathbb{Z})$ of $\mathfrak{H}$ lifting $\mathfrak{a}_\sigma^*$. We then claim

$$\rho^N(\sigma) \equiv {}^tA \quad \text{in } \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z}). \tag{2.9.3}$$

Proof. Let τ_0 designate the image of a small segment $\tau = iy$ $(\mathbb{R}\ni y \gg 0)$ on $Y(N)(\mathbb{C})$ and let $A = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{PSL}_2(\mathbb{Z}/N\mathbb{Z})$ act on it as an automorphism of the modular curve. Then, as explained in (2.9.2), the level structures on elliptic curves on the images of τ_0 and $A(\tau_0) = \frac{a\tau_0+b}{c\tau_0+d}$ are given by the images of $\alpha_\phi : (x,y) \mapsto (2\pi i(\frac{\tau_0}{N}x+\frac{1}{N}y),\tau_0)$ and $\alpha_{\phi'} : (x,y) \mapsto (2\pi i(\frac{A(\tau_0)}{N}x+\frac{1}{N}y), A(\tau_0))$ modulo the action of $\mathbb{Z}^2\rtimes\Gamma(N)$ respectively. Let us compute the latter, taking into account

the equivalences under the action of $\mathbb{Z}^2 \rtimes \mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{C} \times \mathfrak{H}$. It then follows that

$$\left(2\pi i\left(\frac{x}{N}\,\frac{a\tau_0+b}{c\tau_0+d}+\frac{y}{N}\right),\frac{a\tau_0+b}{c\tau_0+d}\right)=\left(2\pi i\left(\frac{\frac{a\tau_0+b}{N}x+\frac{c\tau_0+d}{N}y}{c\tau_0+d}\right),\frac{a\tau_0+b}{c\tau_0+d}\right)$$
$$\sim\left(2\pi i\left(\frac{\tau_0}{N}(ax+cy)+\frac{1}{N}(bx+dy)\right),\tau_0\right).$$

The interpretation is that the point represented by the elliptic curve $\mathcal{E}_{\tau_0}$ with level structure $\alpha_\phi : (x,y) \mapsto 2\pi i\big(\frac{\tau_0}{N}x+\frac{1}{N}y\big)$ is transformed to the point represented by the same elliptic curve but with level structure $\alpha_{\phi'} : (x,y) \mapsto 2\pi i(\frac{\tau_0}{N}(ax+cy)+\frac{1}{N}(bx+dy))$ under the automorphism of $Y(N)$ induced by the matrix A. Namely, the corresponding action of $\rho^N(\sigma)/\pm 1$ on $\mathcal{E}[N]$ must come from $\binom{x}{y} \mapsto \left(\begin{smallmatrix} a & c \\ b & d\end{smallmatrix}\right)\binom{x}{y}$. Hence $\alpha_{\phi'} = \pm\alpha_\phi \circ \left(\begin{smallmatrix} a & c \\ b & d\end{smallmatrix}\right)$, which implies $\rho^N(\sigma) = \pm\left(\begin{smallmatrix} a & c \\ b & d\end{smallmatrix}\right)$ by (2.7.3). □

§3. Monodromy invariants of Eisenstein type

§3.1. Setting

In this section, we fix a full class $\mathcal{C}$ of finite groups and a $\Gamma(1)$-test object (E,O,ω) over a connected regular affine scheme $S = \mathrm{Spec}(B)$ of characteristic zero with associated parameter (x,y,g_2,g_3,t) as in §2.2. Pick a geometric basepoint $\bar{b}$ on S which induces the Weierstrass tangential basepoint $\overrightarrow{\mathfrak{w}}_{\bar{b}}$ on the once punctured elliptic curve $E_{\bar{b}}\setminus\{O\}$. We then consider the pro-$\mathcal{C}$ monodromy representation $\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}_{\bar{b}}}$: $\pi_1(S,\bar{b}) \to \mathrm{Aut}(\pi_1(E_{\bar{b}}\setminus\{O\},\overrightarrow{\mathfrak{w}}_{\bar{b}})(\mathcal{C}))$ as in §2.5. Set $\pi := \pi_1(E_{\bar{b}}\setminus\{O\},\overrightarrow{\mathfrak{w}}_{\bar{b}})(\mathcal{C})$, and write $\pi' := [\pi,\pi]$ (resp. $\pi'' := [\pi',\pi']$) for the commutator (resp. double commutator) subgroup of π in the sense of profinite groups. Denote by $\pi^{\mathrm{ab}} := \pi/\pi'$ the abelianization of π. The abelianization map extends to a natural projection of the complete group algebra of π to that of π^{ab}:

$$(*)^{\mathrm{ab}} : \mathbb{Z}_{\mathcal{C}}[[\pi]] \to \mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]].$$

The purpose of this section is to extract a sequence of arithmetic representations of $\pi_1(S,\bar{b})$, which we wish to call of Eisenstein type, from the action of $\pi_1(S,\bar{b})$ on the meta-abelian quotient π/π'' in a combinatorial group-theoretical way.

§3.2. Pro-$\mathcal{C}$ free differential calculus

Suppose we are given a free generator system $\mathbf{x}_1,\mathbf{x}_2$ of π so that $\mathbf{z} := [\mathbf{x}_1,\mathbf{x}_2]^{-1}$ generates an inertia subgroup over the puncture on $E_{\bar{b}}\setminus\{O\}$. The pro-$\mathcal{C}$ free differential operator $\frac{\partial}{\partial \mathbf{x}_i} : \mathbb{Z}_{\mathcal{C}}[[\pi]] \to \mathbb{Z}_{\mathcal{C}}[[\pi]]$ $(i=1,2)$ is well defined and is characterized by the formula

$$\lambda = \varepsilon(\lambda) + \frac{\partial\lambda}{\partial\mathbf{x}_1}(\mathbf{x}_1-1) + \frac{\partial\lambda}{\partial\mathbf{x}_2}(\mathbf{x}_2-1), \tag{3.2.1}$$

where $\varepsilon : \mathbb{Z}_{\mathcal{C}}[[\pi]] \to \mathbb{Z}_{\mathcal{C}}$ is the augmentation map. Concerning the abelianization images of the terms in the above formula, we have a pro-$\mathcal{C}$ version of the Blanchfield–Lyndon exact sequence of $\mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]]$-modules:

$$0 \to \pi'/\pi'' \xrightarrow{\partial} \mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]]^{\oplus 2} \xrightarrow{d} \mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]] \to 0, \tag{3.2.2}$$

where $\partial(s) := \left(\frac{\partial s}{\partial \mathbf{x}_1}\right)^{\mathrm{ab}} \oplus \left(\frac{\partial s}{\partial \mathbf{x}_2}\right)^{\mathrm{ab}}$ and $d(\mu_1 \oplus \mu_2) := \mu_1(\bar{\mathbf{x}}_1 - 1) + \mu_2(\bar{\mathbf{x}}_2 - 1)$ for $\bar{\mathbf{x}}_i := (\mathbf{x}_i)^{\mathrm{ab}}$ $(i = 1, 2)$. It is known by [Ih86a, Ih99-00] that π'/π'' is a free $\hat{\mathbb{Z}}[[\pi^{\mathrm{ab}}]]$-cyclic module generated by the image $\bar{\mathbf{z}}$ of $\mathbf{z} \in \pi'$ in π'/π''. In view of this fact, we can write each element $\bar{s} \in \pi'/\pi''$ uniquely as $\mu \cdot \bar{\mathbf{z}}$ $(\mu \in \mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]])$. The embedding ∂ of π'/π'' in (3.2.2) is often useful to calculate the "coordinate" μ of $\bar{s}$. In fact, since $\partial(\bar{\mathbf{z}}) = (\bar{\mathbf{x}}_2 - 1, 1 - \bar{\mathbf{x}}_1)$, we have

$$\mu = \left(\frac{\partial s}{\partial \mathbf{x}_1}\right)^{\mathrm{ab}} / (\bar{\mathbf{x}}_2 - 1) = \left(\frac{\partial s}{\partial \mathbf{x}_2}\right)^{\mathrm{ab}} / (1 - \bar{\mathbf{x}}_1) \tag{3.2.3}$$

for $\bar{s} = \mu \cdot \bar{\mathbf{z}} \in \pi'/\pi''$ given as the image of $s \in \pi'$.

§3.3. G_{uv}-invariants

For simplicity below, we shall write the action of $\sigma \in \pi_1(S, \bar{b})$ via $\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}_{\bar{b}}}$ just as

$$\sigma(x) := \varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}_{\bar{b}}}(\sigma)(x) \quad (\sigma \in \pi_1(S, \bar{b}),\ x \in \pi = \pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})(\mathcal{C})). \tag{3.3.1}$$

As explained in §2.5, the monodromy action on the abelianization $\pi^{\mathrm{ab}} = \mathbb{Z}_{\mathcal{C}}\bar{\mathbf{x}}_1 \oplus \mathbb{Z}_{\mathcal{C}}\bar{\mathbf{x}}_2$ can be expressed by 2 by 2 matrices: we shall write

$$\rho(\sigma) = \rho^{\mathcal{C}}(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \quad (\sigma \in \pi_1(S, \bar{b})), \tag{3.3.2}$$

so that $\sigma(\mathbf{x}_1) \equiv \mathbf{x}_1^{a(\sigma)}\mathbf{x}_2^{c(\sigma)}$ and $\sigma(\mathbf{x}_2) \equiv \mathbf{x}_1^{b(\sigma)}\mathbf{x}_2^{d(\sigma)}$ mod π'. Observe that, for each pair $(u, v) \in \mathbb{Z}_{\mathcal{C}}^2$, the quotient

$$\mathcal{S}_{uv}(\sigma) := \sigma(\mathbf{x}_2^{-v}\mathbf{x}_1^{-u}) \cdot (\mathbf{x}_1^{a(\sigma)u + b(\sigma)v}\mathbf{x}_2^{c(\sigma)u + d(\sigma)v}) \tag{3.3.3}$$

lies in π', which gives us a unique element $G_{uv}(\sigma) \in \mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]]$ determined by the equation

$$\mathcal{S}_{uv}(\sigma) \equiv G_{uv}(\sigma) \cdot \bar{\mathbf{z}} \tag{3.3.4}$$

in π'/π''.

§3.4. Integral invariant $\mathbb{E}^{\mathcal{C}}_m(\sigma)$

Let $m \in |\mathcal{C}|$. The above element $G_{uv}(\sigma) \in \mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]]$ can be regarded as a $\mathbb{Z}_{\mathcal{C}}$-valued measure (written $dG_{uv}(\sigma)$) on the profinite space $\pi^{\mathrm{ab}} \cong \mathbb{Z}_{\mathcal{C}}^2$. So one can think about the volume of the subspace $(m\mathbb{Z}_{\mathcal{C}})^2 \subset \mathbb{Z}_{\mathcal{C}}^2$ under this measure:

Definition 3.4.1. For $m \in |\mathcal{C}|$, $\sigma \in \pi_1(S_{\bar{b}})$ and $(u,v) \in \mathbb{Z}_{\mathcal{C}}^2$, we define

$$\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v) := \int_{(m\mathbb{Z}_{\mathcal{C}})^2} dG_{uv}(\sigma).$$

Note that, by definition, $\mathcal{S}_{00}(\sigma) = 1$, $G_{00}(\sigma) = 0$, hence $\mathbb{E}_m^{\mathcal{C}}(\sigma;0,0) = 0$. For readers unfamiliar with measure interpretation of Iwasawa algebras, we shall here quickly rephrase the above definition of $\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v)$ in more elementary terms: Recalling that $\mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]] = \varprojlim_{n\in\mathcal{C}} \mathbb{Z}_{\mathcal{C}}[\bar{\mathbf{x}}_1,\bar{\mathbf{x}}_2]/(\bar{\mathbf{x}}_1^n - 1, \bar{\mathbf{x}}_2^n - 1)$ (where the projective system is formed over $n \in \mathcal{C}$ multiplicatively), for $m \in \mathcal{C}$, take the m-th component of $G_{uv}(\sigma) \in \mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]]$ and write

$$G_{uv}(\sigma) \equiv \sum_{i=0}^{m-1}\sum_{j=0}^{m-1} a_{ij}\bar{\mathbf{x}}_1^i\bar{\mathbf{x}}_2^j \bmod (\bar{\mathbf{x}}_1^m - 1, \bar{\mathbf{x}}_2^m - 1)$$

in the group ring $\mathbb{Z}_{\mathcal{C}}[(\mathbb{Z}/m\mathbb{Z})^2] = \mathbb{Z}_{\mathcal{C}}[\bar{\mathbf{x}}_1,\bar{\mathbf{x}}_2]/(\bar{\mathbf{x}}_1^m - 1, \bar{\mathbf{x}}_2^m - 1)$. The volume of Definition 3.4.1 is then nothing but the principal coefficient $a_{00} \in \mathbb{Z}_{\mathcal{C}}$ of this expression: $\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v) = a_{00}$.

One of our principal concerns in this and the following subsections is to examine the dependence of $\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v)$ on $(u,v) \in \mathbb{Z}_{\mathcal{C}}^2$ modulo m. Let us first express G_{uv} by G_{10} and G_{01}.

Proposition 3.4.2. *For each $\sigma \in \pi_1(S,\bar{b})$, we have*

$$G_{uv}(\sigma) = \frac{(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v - 1}{\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d} - 1} G_{01}(\sigma) + (\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v \frac{(\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u - 1}{\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c} - 1} G_{10}(\sigma) - \mathrm{Rest}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\binom{u}{v}.$$

Here, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \rho^{\mathcal{C}}(\sigma) \in \mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}})$ and $\mathrm{Rest}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\binom{u}{v}$ is an explicit element in $\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2$ defined by

$$\mathrm{Rest}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\binom{u}{v} := R_{b,d}^v + (\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v R_{a,c}^u + \frac{\bar{\mathbf{x}}_1^{-bv} - 1}{\bar{\mathbf{x}}_1 - 1} \frac{\bar{\mathbf{x}}_2^{-cu} - 1}{\bar{\mathbf{x}}_2 - 1} \bar{\mathbf{x}}_2^{-dv},$$

where, for any $\alpha, \beta, \gamma \in \mathbb{Z}_{\mathcal{C}}$,

$$R_{\alpha,\beta}^{\gamma} := \frac{1}{\bar{\mathbf{x}}_1 - 1}\left(\frac{(\bar{\mathbf{x}}_1^{-\alpha}\bar{\mathbf{x}}_2^{-\beta})^\gamma - 1}{\bar{\mathbf{x}}_1^{-\alpha}\bar{\mathbf{x}}_2^{-\beta} - 1} \cdot \frac{\bar{\mathbf{x}}_2^{-\beta} - 1}{\bar{\mathbf{x}}_2 - 1} - \frac{\bar{\mathbf{x}}_2^{-\beta\gamma} - 1}{\bar{\mathbf{x}}_2 - 1}\right).$$

Note. In the above notation $\mathrm{Rest}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\binom{u}{v}$, the dot between $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\binom{u}{v}$ separates the matrix component and the vector component. Namely, Rest gives a map from $\mathrm{SL}_2(\mathbb{Z}_{\mathcal{C}}) \times \mathbb{Z}_{\mathcal{C}}^2$ to $\mathbb{Z}_{\mathcal{C}}$.

Proof. What we need to do is to evaluate (3.3.3) in π'/π''. We may decompose $\mathcal{S}_{uv}$ into three factors lying in π' as follows:

$$\mathcal{S}_{uv} = \big((\mathcal{S}_{01}\mathbf{x}_2^{-d}\mathbf{x}_1^{-b})^v\mathbf{x}_1^{bv}\mathbf{x}_2^{dv}\big)\cdot\mathbf{x}_2^{-dv}\mathbf{x}_1^{-bv}\big((\mathcal{S}_{10}\mathbf{x}_2^{-c}\mathbf{x}_1^{-a})^u\mathbf{x}_1^{au}\mathbf{x}_2^{cu}\big)\mathbf{x}_1^{bv}\mathbf{x}_2^{dv}$$
$$\cdot(\mathbf{x}_2^{-dv}\mathbf{x}_1^{-bv}\mathbf{x}_2^{-cu}\mathbf{x}_1^{bv}\mathbf{x}_2^{cu+dv}).$$

Then, apply (3.2.2)–(3.2.3) to each of the three factors. Note that in free differential calculus, we can make use of basic laws of Leibniz type as shown in [Ih86b, p. 440]. Only one non-trivial point is to show a formula like

$$\left(\frac{\partial(\mathbf{x}_2^{-d}\mathbf{x}_1^{-b})^v\mathbf{x}_1^{bv}\mathbf{x}_2^{dv}}{\partial\mathbf{x}_2}\right)^{\mathrm{ab}} = \frac{(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v-1}{\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d}-1}\cdot\frac{\bar{\mathbf{x}}_2^{-d}-1}{\bar{\mathbf{x}}_2-1}-\frac{\bar{\mathbf{x}}_2^{-dv}-1}{\bar{\mathbf{x}}_2-1},$$

which, however, follows easily by induction for non-negative integers v, and then by the standard continuity argument. (Alternatively, one may skip induction by using the general formula $\frac{\partial f^v}{\partial\mathbf{x}_i}=\frac{f^v-1}{f-1}\frac{\partial f}{\partial\mathbf{x}_i}$ from [Ih86b, p. 440 (iv)].) □

Remark 3.4.3. In general, there are no reasons to expect periodicity of the values $\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v)$ in (u,v) with any modulus. But we will see later (see Corollary 6.9.8) that $\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v)$ mod M^2 ($M\in|\mathcal{C}|$) is determined by the residue class of (u,v) in $(\mathbb{Z}/mM^2 2^\varepsilon\mathbb{Z})^2$, where $\varepsilon=0,1$ according as $2\nmid M$, $2|M$ respectively. Namely, we have a well defined mapping

$$\mathbb{E}_{m,M^2}:\pi_1(S,\bar{b})\to(\mathbb{Z}/M^2\mathbb{Z})[(\mathbb{Z}/mM^2 2^\varepsilon)^2].$$

In fact, one can refine $\mathbb{E}_{m,M^2}$ more minutely by replacing M^2 with M, which amounts to examining elementary arithmetic divisibility of $\int_{(m\hat{\mathbb{Z}})^2}dR_{\alpha,\beta}^{mM2^\varepsilon}$. We discuss it in a separate article [N12].

Remark 3.4.4. In [Tsu95a, Prop. 1.12], H. Tsunogai derived, by applying σ to the relation $[\mathbf{x}_1,\mathbf{x}_2]\mathbf{z}=1$, an equation satisfied by $G_{-1,0}:=G_{-1,0}(\sigma)$ and $G_{0,-1}:=G_{0,-1}(\sigma)$:

$$(\bar{\mathbf{x}}_1^b\bar{\mathbf{x}}_2^d-1)G_{-1,0}-(\bar{\mathbf{x}}_1^a\bar{\mathbf{x}}_2^c-1)G_{0,-1}$$
$$=(ad-bc)-\frac{(\bar{\mathbf{x}}_2^d-1)(\bar{\mathbf{x}}_1^a\bar{\mathbf{x}}_2^c-1)-(\bar{\mathbf{x}}_2^c-1)(\bar{\mathbf{x}}_1^b\bar{\mathbf{x}}_2^d-1)}{(\bar{\mathbf{x}}_1-1)(\bar{\mathbf{x}}_2-1)}$$

in the notation of the above proposition. Since $(\bar{\mathbf{x}}_1^a\bar{\mathbf{x}}_2^c-1)$, $(\bar{\mathbf{x}}_1^b\bar{\mathbf{x}}_2^d-1)$ are not zero-divisors in $\mathbb{Z}_{\mathcal{C}}[[\mathbb{Z}_{\mathcal{C}}^2]]$ as shown in [Ih99-00, Part I, Prop. 2.1.1(i)], the above Tsunogai's equation implies that $G_{-1,0}$ determines $G_{0,-1}$ and vice versa.

Proposition 3.4.5. *Let $\sigma\in\pi_1(S,\bar{b})$ with $\rho^{\mathcal{C}}(\sigma)=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$. For $(u,v)\in(\mathbb{Z}_{\mathcal{C}})^2$, denote by $C_m(u,v)\subset\mathbb{Z}_{\mathcal{C}}^2$ the coset modulo $(m\mathbb{Z}_{\mathcal{C}})^2$ represented by $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right).\binom{u}{v}=u\binom{a}{c}+v\binom{b}{d}$.*

(i) *We have*

$$\int_{C_m(u,v)} dG_{10}(\sigma) = \mathbb{E}^{\mathcal{C}}_m(\sigma; u+1, v) - \mathbb{E}^{\mathcal{C}}_m(\sigma; u, v) + \left\lfloor \frac{au+bv}{m} \right\rfloor \cdot \left(\left\lfloor \frac{c(u+1)+dv}{m} \right\rfloor - \left\lfloor \frac{cu+dv}{m} \right\rfloor \right),$$

where $\lfloor \frac{\alpha}{m} \rfloor := -\int_{m\mathbb{Z}_{\mathcal{C}}} d\big(\frac{x^{-\alpha}-1}{x-1}\big)$ *for* $\alpha \in \mathbb{Z}_{\mathcal{C}}$.

(ii) *The values of* $\{\mathbb{E}^{\mathcal{C}}_m(\sigma; u, v) \mid (u,v) \in \mathbb{Z}^2_{\mathcal{C}},\ m \in |\mathcal{C}|\}$ *determine the action of* σ *on* π/π''.

Proof. By a simple calculation from the definition, it follows that

$$\begin{aligned} G_{uv}(\sigma) &= G_{u+1,v}(\sigma) - (\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u (\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v G_{10}(\sigma) \\ &\quad + \mathrm{Rest}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\binom{u+1}{v} - \mathrm{Rest}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\binom{u}{v} \\ &= G_{u+1,v}(\sigma) - (\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u (\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v G_{10}(\sigma) \\ &\quad + \bar{\mathbf{x}}_2^{-cu-dv} \frac{\bar{\mathbf{x}}_2^{-c}-1}{\bar{\mathbf{x}}_2 - 1} \frac{\bar{\mathbf{x}}_1^{-au-bv}-1}{\bar{\mathbf{x}}_1 - 1}. \end{aligned} \tag{3.4.6}$$

Integrating measures represented by the above terms over the subspace $(m\mathbb{Z}_{\mathcal{C}})^2 \subset \mathbb{Z}^2_{\mathcal{C}}$ enables us to find $\int_{C_m(u,v)} dG_{10}(\sigma) - \mathbb{E}^{\mathcal{C}}_m(\sigma; u+1, v) + \mathbb{E}^{\mathcal{C}}_m(\sigma; u, v)$ equal to

$$\int_{m\mathbb{Z}_{\mathcal{C}}} d\left(\frac{\bar{\mathbf{x}}_1^{-au-bv}-1}{\bar{\mathbf{x}}_1 - 1}\right) \cdot \int_{m\mathbb{Z}_{\mathcal{C}}} d\left(\frac{\bar{\mathbf{x}}_2^{-cu-dv-c} - \bar{\mathbf{x}}_2^{-cu-dv}}{\bar{\mathbf{x}}_2 - 1}\right),$$

from which (i) follows immediately. The formula (i) determines the measure $G_{10}(\sigma) \in \mathbb{Z}_{\mathcal{C}}[[\mathbb{Z}^2_{\mathcal{C}}]]$ from the collection of values $\mathbb{E}^{\mathcal{C}}_m(\sigma; u, v)$ $((u,v) \in \mathbb{Z}^2_{\mathcal{C}},\ m \in |\mathcal{C}|)$. If we put $u = -1, v = 0$, then we find that it also determines

$$G_{-1,0}(\sigma) = -\bar{\mathbf{x}}_1^a \bar{\mathbf{x}}_2^c G_{1,0}(\sigma) - \frac{\bar{\mathbf{x}}_1^a - 1}{\bar{\mathbf{x}}_1 - 1} \frac{\bar{\mathbf{x}}_2^c - 1}{\bar{\mathbf{x}}_2 - 1}.$$

Tsunogai's equation (Remark 3.4.4) then also determines $G_{0,-1}(\sigma)$. Thus, both $\mathcal{S}_{-1,0}(\sigma) = \sigma(\bar{\mathbf{x}}_1)\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c}$ and $\mathcal{S}_{0,-1}(\sigma) = \sigma(\bar{\mathbf{x}}_2)\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d}$ are determined modulo π''. The assertion (ii) follows since π is generated by $\mathbf{x}_1$, $\mathbf{x}_2$. □

Remark 3.4.7. We may use the notation

$$\left\lfloor \frac{\alpha}{m} \right\rfloor := -\int_{m\mathbb{Z}_{\mathcal{C}}} d\left(\frac{x^{-\alpha}-1}{x-1}\right) \quad \left(\text{resp. } \left\lceil \frac{\alpha}{m} \right\rceil := \int_{m\mathbb{Z}_{\mathcal{C}}} d\left(\frac{x^{\alpha}-1}{x-1}\right)\right)$$

for $m \in |\mathcal{C}|$, $\alpha \in \mathbb{Z}_{\mathcal{C}}$ to designate the pro-$\mathcal{C}$ floor (resp. ceiling) function. Obviously, $\lceil -\alpha/m \rceil = -\lfloor \alpha/m \rfloor$. In fact, it is not difficult to verify the following: If $\alpha = m\beta$, then $\lceil \alpha/m \rceil = \beta$. When $m \nmid \alpha$, writing $\alpha \equiv \langle \alpha \rangle_m \bmod m$ with $\langle \alpha \rangle_m \in [0, m) \subset \mathbb{N}$, it follows that $\lceil \alpha/m \rceil = 1 + (\alpha - \langle \alpha \rangle_m)/m$.

The following proposition allows us to compute $\mathbb{E}^{\mathcal{C}}_m(\sigma;u,v)$ with both u and v divisible by m in $\mathbb{Z}_{\mathcal{C}}$ from the values of $\mathbb{E}^{\mathcal{C}}_m(\sigma;1,0)$, $\mathbb{E}^{\mathcal{C}}_m(\sigma;u+1,v)$ and an arithmetically elementary term.

Proposition 3.4.8. *If $(u,v)\in(m\mathbb{Z}_{\mathcal{C}})^2$, then, for each $\sigma\in\pi_1(S,\bar{b})$ with $\rho^{\mathcal{C}}(\sigma)=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$,*

$$\mathbb{E}^{\mathcal{C}}_m(\sigma;u,v)=\mathbb{E}^{\mathcal{C}}_m(\sigma;u+1,v)-\mathbb{E}^{\mathcal{C}}_m(\sigma;1,0)+\left\lfloor\frac{au+bv}{m}\right\rfloor\cdot\left\lfloor\frac{c}{m}\right\rfloor.$$

Proof. Considering terms on the RHS of (3.4.6) as measures on the space $\mathbb{Z}_{\mathcal{C}}^2$, we find that the multiplications by $(\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v$, $\bar{\mathbf{x}}_2^{-cu-dv}$ in the second and third terms turn out to have no effect upon integration over $(m\mathbb{Z}_{\mathcal{C}})^2$ under the assumption $(u,v)\in(m\mathbb{Z}_{\mathcal{C}})^2$. This observation proves the proposition. □

§3.5. Twisted invariants and their composition rule

Let $\sigma\in\pi_1(S,\bar{b})$ and regard σ as acting on π^{ab} through $\rho(\sigma)\in\mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}})$. Noting that the G_{uv}-invariant may be rewritten as

$$G_{uv}(\sigma)=\sigma\left(\frac{\bar{\mathbf{x}}_2^{-v}-1}{\bar{\mathbf{x}}_2^{-1}-1}\right)G_{01}(\sigma)+\sigma\left(\bar{\mathbf{x}}_2^{-v}\frac{\bar{\mathbf{x}}_1^{-u}-1}{\bar{\mathbf{x}}_1^{-1}-1}\right)G_{10}(\sigma)-\mathrm{Rest}\,\rho(\sigma).\tbinom{u}{v},\tag{3.5.1}$$

we shall introduce its twist by a matrix $\epsilon\in\mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}})$ as follows:

(3.5.2)
$$\begin{aligned}G^{\epsilon}_{\binom{u}{v}}(\sigma):=&\left[(\sigma\epsilon)\left(\frac{\bar{\mathbf{x}}_2^{-v}-1}{\bar{\mathbf{x}}_2^{-1}-1}\right)\right]\cdot G_{\epsilon\binom{0}{1}}(\sigma)+\left[(\sigma\epsilon)\left(\bar{\mathbf{x}}_2^{-v}\frac{\bar{\mathbf{x}}_1^{-u}-1}{\bar{\mathbf{x}}_1^{-1}-1}\right)\right]\cdot G_{\epsilon\binom{1}{0}}(\sigma)\\&-\left[\mathrm{Rest}\,\rho(\sigma)\epsilon.\tbinom{u}{v}\right]+\chi(\sigma)\cdot\sigma\left[\mathrm{Rest}\,\epsilon.\tbinom{u}{v}\right].\end{aligned}$$

Since $\mathrm{Rest}\,I.\binom{u}{v}=0$ for the unit matrix $I=\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$, it turns out that $G^{I}_{\binom{u}{v}}(\sigma)=G_{uv}(\sigma)$.

The merit of introducing the ϵ-twisted invariants is the following composition rule:

Proposition 3.5.3. *For $\sigma,\tau\in\pi_1(S,\bar{b})$ and $\epsilon\in\mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}})$, we have*

$$G^{\epsilon}_{\binom{u}{v}}(\sigma\tau)=G^{\rho(\tau)\epsilon}_{\binom{u}{v}}(\sigma)+\chi(\sigma)\cdot\sigma(G^{\epsilon}_{\binom{u}{v}}(\tau)).$$

Proof. We start by studying composition rules for G_{10} and G_{01}. Let $\rho(\sigma)=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$, $\rho(\tau)=\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$ so that $\rho(\sigma\tau)=\left(\begin{smallmatrix}a\alpha+b\gamma & a\beta+b\delta\\ c\alpha+d\gamma & c\beta+d\delta\end{smallmatrix}\right)$. Then in π'/π'' we have

$$G_{10}(\sigma\tau)\cdot\bar{\mathbf{z}}\equiv\mathcal{S}_{10}(\sigma\tau)=(\sigma\tau)(\mathbf{x}_1^{-1})\mathbf{x}_1^{a\alpha+b\gamma}\mathbf{x}_2^{c\alpha+d\gamma}.$$

As $(\sigma\tau)(\mathbf{x}_1^{-1})=\sigma\big((G_{10}(\tau)\cdot\bar{\mathbf{z}}^{\chi(\sigma)})\mathbf{x}_2^{-\gamma}\mathbf{x}_1^{-\alpha}\big)$, one can decompose the RHS as the product of two factors $G_{10}(\tau)(\sigma\bar{\mathbf{x}}_1,\sigma\bar{\mathbf{x}}_2)\cdot\bar{\mathbf{z}}^{\chi(\sigma)}$ and $\sigma(\mathbf{x}_2)^{-\gamma}\sigma(\mathbf{x}_1)^{-\alpha}\mathbf{x}_1^{a\alpha+b\gamma}\mathbf{x}_2^{c\alpha+d\gamma}$,

where in the former factor $G_{10}(\tau)(\sigma\bar{\mathbf{x}}_1, \sigma\bar{\mathbf{x}}_2)$ means the element obtained from $G_{10}(\tau) = G_{10}(\tau)(\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2) \in \mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]]$ by substituting $(\sigma\bar{\mathbf{x}}_1, \sigma\bar{\mathbf{x}}_2) = (\bar{\mathbf{x}}_1^a\bar{\mathbf{x}}_2^c, \bar{\mathbf{x}}_1^b\bar{\mathbf{x}}_2^d)$ for $(\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2)$, and the latter factor is equivalent to $G_{\alpha\gamma}(\sigma)\cdot\bar{z} \bmod \pi''$ with $G_{\alpha\gamma}$ given as in §3.4. Applying the parallel argument to G_{01}, we obtain

$$G_{10}(\sigma\tau) = \chi(\sigma)G_{10}(\tau)(\sigma\bar{\mathbf{x}}_1, \sigma\bar{\mathbf{x}}_2) + G_{\alpha\gamma}(\sigma), \tag{3.5.4}$$

$$G_{01}(\sigma\tau) = \chi(\sigma)G_{01}(\tau)(\sigma\bar{\mathbf{x}}_1, \sigma\bar{\mathbf{x}}_2) + G_{\beta\delta}(\sigma). \tag{3.5.5}$$

Putting these together into $G_{uv}(\sigma\tau)$ developed by the formula (3.5.1) and collecting terms according to the definition (3.5.2), we obtain

$$G_{uv}(\sigma\tau) = \chi(\sigma)\cdot\sigma(G_{uv}(\tau)) + G^{\rho(\tau)}_{\binom{u}{v}}(\sigma) \quad (\sigma, \tau \in \pi_1(S, \bar{b})). \tag{3.5.6}$$

Now, if $f : S \to M^{\omega}_{1,1}$ is the representing morphism, then the monodromy representation from $\pi_1(S, \bar{b})$ factors through $\pi_1(M^{\omega}_{1,1}, f(\bar{b}))$ and the above formula can hold true for all elements $\sigma, \tau \in \pi_1(M^{\omega}_{1,1}, f(\bar{b}))$. Because of the surjectivity of ρ in the universal elliptic curves, any given $\epsilon \in \mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}})$ is realized as the image under ρ of some $\tau \in \pi_1(M^{\omega}_{1,1}, f(\bar{b}))$. Applying then (3.5.6) to $\sigma = \sigma_1\sigma_2$, one gets

$$\begin{aligned} G^{\epsilon}_{\binom{u}{v}}(\sigma) &= G_{uv}(\sigma_1\sigma_2\tau) - \chi(\sigma_1\sigma_2)\cdot\sigma_1\sigma_2(G_{uv}(\tau)) \\ &= \big\{\chi(\sigma_1)\cdot\sigma_1(G_{uv}(\sigma_2\tau)) + G^{\rho(\sigma_2\tau)}_{\binom{u}{v}}(\sigma_1)\big\} - \chi(\sigma_1)\cdot\sigma_1\big(\chi(\sigma_2)\cdot\sigma_2(G_{uv}(\tau))\big) \\ &= \chi(\sigma_1)\cdot\sigma_1(G^{\rho(\tau)}_{\binom{u}{v}}(\sigma_2)) + G^{\rho(\sigma_2)\epsilon}_{\binom{u}{v}}(\sigma_1). \end{aligned}$$

This concludes the proof. □

As in §3.4, for each $m \in |\mathcal{C}|$, one can consider the volume of the subspace $(m\mathbb{Z}_{\mathcal{C}})^2 \subset \mathbb{Z}^2_{\mathcal{C}}$ under the measure $dG^{\epsilon}_{\binom{u}{v}}(\sigma)$, i.e.,

$$\mathbb{E}^{\epsilon}_m(\sigma; u, v)\ (= \mathbb{E}^{\mathcal{C},\epsilon}_m(\sigma; u, v)) := \int_{(m\mathbb{Z}_{\mathcal{C}})^2} dG^{\epsilon}_{\binom{u}{v}}(\sigma). \tag{3.5.7}$$

Concerning the composition, noticing that the subspace $(m\mathbb{Z}_{\mathcal{C}})^2$ is invariant under the $\mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}})$-action on $\mathbb{Z}^2_{\mathcal{C}}$, one derives easily from Proposition 3.5.3 that

$$\mathbb{E}^{\epsilon}_m(\sigma\tau; u, v) = \mathbb{E}^{\rho(\tau)\epsilon}_m(\sigma; u, v) + \chi(\sigma)\mathbb{E}^{\epsilon}_m(\tau; u, v) \qquad (\sigma, \tau \in \pi_1(S, \bar{b}),\ (u, v) \in \mathbb{Z}^2_{\mathcal{C}}).$$

§3.6. Measure $\mathcal{E}^{\mathcal{C}}_{\sigma}$ on the congruence kernel

In our argument so far, we have not allowed m to vary over the integers $m \in |\mathcal{C}|$, as our invariant $\mathbb{E}^{\mathcal{C}}_m(\sigma; u, v)$ does not directly provide a coherent sequence in the projective system of the group ring $\mathbb{Z}_{\mathcal{C}}[(\mathbb{Z}/m\mathbb{Z})^2]$ in general. However, this is the case if σ lies in the congruence kernel $\pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}}) = \ker(\pi_1(S, \bar{b}) \to \mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}}))$, i.e.,

$\rho^{\mathcal{C}}(\sigma) = I$. In fact, in this case, Tsunogai's equation (Remark 3.4.4) reduces to the equation (originally observed by S. Bloch [Bl84])

$$(\bar{\mathbf{x}}_2 - 1)G_{-1,0}(\sigma) - (\bar{\mathbf{x}}_1 - 1)G_{0,-1}(\sigma) = 0, \tag{3.6.1}$$

from which it follows that there exists a unique measure $\mathcal{E}^{\mathcal{C}}_{\sigma} \in \mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]]$ such that $G_{-1,0}(\sigma) = (\bar{\mathbf{x}}_1 - 1)\mathcal{E}^{\mathcal{C}}_{\sigma}$ and $G_{0,-1}(\sigma) = (\bar{\mathbf{x}}_2 - 1)\mathcal{E}^{\mathcal{C}}_{\sigma}$. On the other hand, by (3.4.6), we have $G_{-1,0}(\sigma) = -\bar{\mathbf{x}}_1 G_{10}(\sigma)$ and by Proposition 3.4.2, we see

$$G_{uv}(\sigma) = \frac{\bar{\mathbf{x}}_2^{-v} - 1}{\bar{\mathbf{x}}_2^{-1} - 1} G_{01}(\sigma) + \bar{\mathbf{x}}_2^{-v} \frac{\bar{\mathbf{x}}_1^{-u} - 1}{\bar{\mathbf{x}}_1^{-1} - 1} G_{10}(\sigma) \tag{3.6.2}$$

when $\rho^{\mathcal{C}}(\sigma) = I$. Applying $u = 0$, $v = -1$ in the latter gives also $G_{0,-1}(\sigma) = -\bar{\mathbf{x}}_2 G_{01}(\sigma)$. Thus, putting the above equations together we conclude

$$G_{uv}(\sigma) = (\bar{\mathbf{x}}_1^{-u}\bar{\mathbf{x}}_2^{-v} - 1) \cdot \mathcal{E}^{\mathcal{C}}_{\sigma} \quad (\sigma \in \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})). \tag{3.6.3}$$

This equation implies that the image of $G_{uv}(\sigma)$ in $\mathbb{Z}_{\mathcal{C}}[(\mathbb{Z}/m\mathbb{Z})^2]$, hence that of $\mathbb{E}^{\mathcal{C}}_m(\sigma; u, v)$, depends only on (u, v) modulo m: for $\sigma \in \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})$, it defines $\mathbb{E}^{\mathcal{C}}_m(\sigma) \in \mathbb{Z}_{\mathcal{C}}[(\mathbb{Z}/m\mathbb{Z})^2]$.

Now, write the image of $\mathcal{E}^{\mathcal{C}}_{\sigma}$ in $\mathbb{Z}_{\mathcal{C}}[(\mathbb{Z}/m\mathbb{Z})^2]$ as $\sum_{\mathbf{a} \in (\mathbb{Z}/m\mathbb{Z})^2} \mathcal{E}^{\mathcal{C}}_m(\sigma, \mathbf{a})\mathbf{e}_{\mathbf{a}}$, where $\mathbf{e}_{\mathbf{a}}$ denotes the image of $\bar{\mathbf{x}}_1^u\bar{\mathbf{x}}_2^v$ under the projection $\mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]] \to \mathbb{Z}_{\mathcal{C}}[\bar{\mathbf{x}}_1, \bar{\mathbf{x}}_2]/(\bar{\mathbf{x}}_1^m - 1, \bar{\mathbf{x}}_2^m - 1) = \mathbb{Z}_{\mathcal{C}}[(\mathbb{Z}/m\mathbb{Z})^2]$ for any representative $(u, v) \in \mathbb{Z}^2_{\mathcal{C}}$ of the class $\mathbf{a} \in (\mathbb{Z}/m\mathbb{Z})^2$. Then (3.6.3) allows us to express

$$\mathbb{E}^{\mathcal{C}}_m(\sigma, \mathbf{a}) = \mathcal{E}^{\mathcal{C}}_m(\sigma, \mathbf{a}) - \mathcal{E}^{\mathcal{C}}_m(\sigma; 0, 0). \tag{3.6.4}$$

From this, for any fixed $\sigma \in \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})$, the incoherence of $\mathbb{E}^{\mathcal{C}}_m(\sigma) \in \mathbb{Z}_{\mathcal{C}}[(\mathbb{Z}/m\mathbb{Z})^2]$ with respect m, in other words, the main reason for the sequence $\{\mathbb{E}^{\mathcal{C}}_m(\sigma)\}_m$ to fail to form a measure on $\mathbb{Z}^2_{\mathcal{C}}$, turns out to amount to the "error term" sequence $\{\mathcal{E}^{\mathcal{C}}_m(\sigma; 0, 0)\}$. In §6.10, we will relate $\mathbb{E}^{\mathcal{C}}_m(\sigma)$ and $\mathcal{E}^{\mathcal{C}}_{\sigma}$ by estimating exactly this error term to be $\frac{1}{12}$ of the Kummer cocycle along power roots of "$\Delta(E, m\omega)$", which will be introduced in the next section.

Remark 3.6.5. If two full classes $\mathcal{C}, \mathcal{C}'$ of finite groups satisfy $\mathcal{C} \subset \mathcal{C}'$, the natural projection $\Pi_{1,1}(\mathcal{C}') \to \Pi_{1,1}(\mathcal{C})$ induces $\mathbb{Z}_{\mathcal{C}'}[[\Pi_{1,1}(\mathcal{C}')^{\mathrm{ab}}]] \to \mathbb{Z}_{\mathcal{C}}[[\Pi_{1,1}(\mathcal{C})^{\mathrm{ab}}]]$. Then it is easily seen that $\mathbb{E}^{\mathcal{C}'}_m$ is mapped to $\mathbb{E}^{\mathcal{C}}_m$. This means that our pro-$\mathcal{C}$ formulation of $\mathbb{E}^{\mathcal{C}}_m$ is somehow superfluous, i.e., one can say that the full profinite version is essentially enough. However, this is not the case when considering $\mathcal{E}^{\mathcal{C}}_{\sigma}$, as it is defined only on the congruence kernel $\pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})$—depending on the set of primes in $|\mathcal{C}|$ as a subgroup of $\pi_1(S, \bar{b})$ with respect to $\mathcal{C}$.

Proposition 3.6.6. *The mapping* $\mathcal{E}^{\mathcal{C}} : \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}}) \to \mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]]$ $(\sigma \mapsto \mathcal{E}^{\mathcal{C}}(\sigma) = \mathcal{E}^{\mathcal{C}}_{\sigma})$ *is an additive homomorphism, i.e.,*

$$\mathcal{E}^{\mathcal{C}}(\sigma\tau) = \mathcal{E}^{\mathcal{C}}(\sigma) + \mathcal{E}^{\mathcal{C}}(\tau) \quad (\sigma, \tau \in \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})).$$

Moreover, it is "$\det \otimes \mathrm{GL}_2$*"-equivariant in the sense that*

$$\mathcal{E}^{\mathcal{C}}(\sigma\tau\sigma^{-1}) = \det(\rho(\sigma)) \cdot \sigma(\mathcal{E}^{\mathcal{C}}(\tau)) \quad (\sigma \in \pi_1(S, \bar{b}),\ \tau \in \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})).$$

This assertion can be proven in the same way as [N95, (4.8)]. We will give an alternative proof in §6.10 using (3.5.8).

§4. Review of algebraic modular forms

In this section, we review special families of modular functions and forms—so called the modular units and Eisenstein series—in an algebraic style convenient for our later discussions.

§4.1. Fundamental theta functions

We begin by introducing the fundamental theta function $\theta(z, \mathfrak{L})$ $(z \in \mathbb{C})$ for a lattice $\mathfrak{L} \subset \mathbb{C}$. Let $\wp(z) = \wp(z, \mathfrak{L})$ be the Weierstrass $\wp$-function. As is well known, the associated parameters for the $\Gamma(1)$-test object $(\mathbb{C}/\mathfrak{L}, dz)$ are given by $x = \wp(z)$, $y = \wp'(z)$, $g_2 := 60 \sum'_{\omega} \omega^{-4}$ and $g_3 = 140 \sum'_{\omega} \omega^{-6}$ ($\sum'_{\omega}$ means the sum over $\omega \in \mathfrak{L}' = \mathfrak{L} \setminus \{0\}$). Then we define

$$\theta(z, \mathfrak{L}) := \Delta(\mathfrak{L}) e^{-6\boldsymbol{\eta}(z,\mathfrak{L})z} \sigma(z, \mathfrak{L})^{12}. \tag{4.1.1}$$

Here $\Delta(\mathfrak{L}) = g_2^3 - 27g_3^2$, $\sigma(z, \mathfrak{L})$ is the Weierstrass σ-function of $\mathfrak{L}$:

$$\sigma(z, \mathfrak{L}) = z \prod_{\omega \in \mathfrak{L}'} \left(1 - \frac{z}{\omega}\right) \exp\left(\frac{z}{\omega} + \frac{1}{2}\left(\frac{z}{\omega}\right)^2\right), \tag{4.1.2}$$

and $\boldsymbol{\eta} : \mathbb{C} \to \mathbb{C}$ is the $\mathbb{R}$-linear extension of the period function $\mathfrak{L} \to \mathbb{C}$ $(\omega \mapsto -\int_*^{*+\omega} \wp(z)\, dz)$. Note here that $\wp(z)dz = xdx/y$ is a meromorphic differential form of the second kind, i.e., without residues; hence the integral is well defined. It is easy to see that

$$\theta(z, \mathfrak{L}) = \theta(\lambda z, \lambda\mathfrak{L}) \quad (\lambda \in \mathbb{C}^{\times},\ z \in \mathbb{C}). \tag{4.1.3}$$

According to the above definition of $\boldsymbol{\eta}(z, \mathfrak{L})$, the function $\theta(z, \mathfrak{L})$ is not holomorphic in z. When z lies in $\mathbb{Q}\mathfrak{L}$, one can show from [KL81, (K2), p. 28] that $\theta(z, \mathfrak{L})$ behaves

like an "almost" periodic function with respect to $\mathfrak{L}$, i.e.,

$$\text{(4.1.4)}\qquad \begin{cases} \theta(z+\omega,\mathfrak{L}) = \zeta\theta(z,\mathfrak{L}) & (z \in \frac{1}{N}\mathfrak{L},\ \omega \in \mathfrak{L},\ \zeta \in \mu_N), \\ \theta(z+\omega,\mathfrak{L}) = \theta(z,\mathfrak{L}) & (z \in \frac{1}{N}\mathfrak{L},\ \omega \in N\mathfrak{L}). \end{cases}$$

The following distribution relations are also essential in our later applications.

Proposition 4.1.5. *Let m, n, d, and r be integers such that $n = md$ and $r =$ l.c.m.(m,d). Then*

$$\text{(1)}\qquad \theta(\omega_0, m\mathfrak{L}) = \zeta \prod_{\omega \in m\mathfrak{L}/n\mathfrak{L}} \theta(\omega_0+\omega, n\mathfrak{L}) \qquad (\omega_0 \in \mathfrak{L}\setminus n\mathfrak{L},\ \exists\zeta \in \mu_r);$$

$$\text{(2)}\qquad d^{12} = \zeta \prod_{\omega \in m\mathfrak{L}/n\mathfrak{L},\ \omega \notin n\mathfrak{L}} \theta(\omega, n\mathfrak{L}) \qquad (\exists\zeta \in \mu_d).$$

Proof. These are special forms of the distribution relations due to Ramachandra–Robert (cf. [KL81, p. 43]). □

Now, let us restrict the lattices $\mathfrak{L}$ to those in the form $\mathfrak{L}_\tau = \mathbb{Z}\tau + \mathbb{Z}1$ ($\tau \in \mathfrak{H}$), and write $\sigma(z,\tau) = \sigma(z,\mathfrak{L}_\tau)$ and $\theta(z,\tau) = \theta(z,\mathfrak{L}_\tau)$. The infinite product expansions of the first two holomorphic functions in $q_z = e^{2\pi i z}$, $q_\tau = e^{2\pi i\tau}$ are well known (see e.g. [L87]):

$$\Delta(\mathfrak{L}_\tau) = (2\pi i)^{12} q_\tau \prod_{n=1}^{\infty}(1-q_\tau^n)^{24},$$

$$\sigma(z,\tau) = \frac{e^{\boldsymbol{\eta}(1)z^2/2}}{(2\pi i)}(q_z^{1/2} - q_z^{-1/2}) \prod_{n=1}^{\infty} \frac{(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1})}{(1-q_\tau^n)^2}.$$

As remarked above, the fundamental theta function $\theta(z,\tau)$ is not holomorphic in z, but it is holomorphic in τ. Writing $z = x_1\tau + x_2$ ($x_1, x_2 \in \mathbb{R}$), from the above expansions we obtain

$$\text{(4.1.6)}\qquad \theta(z,\tau) = q_\tau^{6B_2(x_1)} e^{12\pi i x_2(x_1-1)} \Big[(1-q_z)\prod_{n\geq 1}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1})\Big]^{12},$$

where $B_2(T) = T^2 - T + \frac{1}{6}$ is the second Bernoulli polynomial. (Here, we use $\boldsymbol{\eta}(z) = x_1\boldsymbol{\eta}(\tau) + x_2\boldsymbol{\eta}(1)$ and the Legendre relation $\boldsymbol{\eta}(1)\tau - \boldsymbol{\eta}(\tau)1 = 2\pi i$.) Comparing this with the classical expansion of Jacobi's theta function $\vartheta_1(z,\tau)$, we also see that

$$\theta(z,\tau) = e^{12\pi i x_1 z}\left[\frac{\vartheta_1(z,\tau)}{\eta(\tau)}\right]^{12} \qquad (z = x_1\tau + x_2,\ x_1, x_2 \in \mathbb{R}),$$

where $\eta(\tau) := e^{2\pi i\tau/24}\prod_{n=1}^{\infty}(1-q_\tau^n)$ is the Dedekind η-function.

§4.2. Siegel units

In the book [KL81] by D. Kubert and S. Lang, a 12-th power root of $\theta(z,\tau)$ is introduced and intensively studied via the *Klein form*

$$\ell(z;\mathfrak{L}) := e^{-\boldsymbol{\eta}(z,\mathfrak{L})z/2}\sigma(z,\mathfrak{L}) \tag{4.2a}$$

that is defined for a lattice $\mathfrak{L}\subset\mathbb{C}$. Given $x=(x_1,x_2)\in\mathbb{R}^2$, it gives a function on $\tau\in\mathfrak{H}$ (also called the Klein form) defined by

$$\ell_x(\tau) := \ell(x_1\tau+x_2,\mathfrak{L}_\tau) \tag{4.2b}$$

where $\mathfrak{L}_\tau=\mathbb{Z}\tau+\mathbb{Z}$ ($\tau\in\mathfrak{H}$). Note that, in [KL81, p. 29], their "Dedekind η^2" is the $2\pi i$-multiple of our η^2. In fact, since $\ell(z;\mathfrak{L})$ is homogeneous of degree 1 (cf. [KL81, p. 27, (K0)]), we have $2\pi i\ell(z,\mathfrak{L}_\tau)=\ell(2\pi iz,2\pi i\,\mathfrak{L}_\tau)$.

For $x=(x_1,x_2)\in\mathbb{R}^2$, let us define the *Siegel function* $g_x(\tau)$ by

$$g_x(\tau) = 2\pi i\eta(\tau)^2\ell_x(\tau), \tag{4.2c}$$

which, after computation similar to (4.1.6) above, turns out to have the following product form:

$$g_x(\tau) = -q_\tau^{B_2(x_1)/2}e^{\pi ix_2(x_1-1)}\Big[(1-q_z)\prod_{n\geq1}(1-q_\tau^nq_z)(1-q_\tau^nq_z^{-1})\Big] \tag{4.2d}$$

with $z=x_1\tau+x_2$. From this it follows immediately that $g_x(\tau)^{12}=\theta(z,\tau)$. Again, this function has a non-holomorphic factor $q_\tau^{B_2(x_1)/2}e^{\pi ix_2(x_1-1)}$ with respect to the complex variable $z=x_1\tau+x_2$. Observe also that $g_x(\tau)=0$ if and only if $x\in\mathbb{Z}^2$.

Here, we shall collect several properties of Siegel functions for later use. Let $m\geq1$ and assume $x=(r_1/N,r_2/N)$ ($r_1,r_2\in\mathbb{Z},N\geq1$). We consider the condition

$$\mathrm{Q}(x,N,m):\begin{cases}\text{If } N \text{ is odd, then } mr_1^2\equiv mr_2^2\equiv mr_1r_2\equiv0 \bmod N.\\ \text{If } N \text{ is even, then } mr_1^2\equiv mr_2^2\equiv0 \bmod 2N,\ mr_1r_2\equiv0 \bmod N.\end{cases}$$

Proposition 4.2.1. *Notations being as above, the following statements hold:*

(i) *The function $\theta_x(\tau)^m=g_x(\tau)^{12m}$ is modular of level $\Gamma(N)$ if and only if the condition $\mathrm{Q}(x,N,12m)$ holds. In particular, $\theta(x_1\tau+x_2,\tau)$ is modular of level $\Gamma(N^2)$.*

(ii) *When* g.c.d.$(N,12)=3$, *the function $g_x(\tau)^{4m}$ is modular of level $\Gamma(N)$ iff the condition $\mathrm{Q}(x,N,4m)$ holds. In particular, $g_x(\tau)^4$ is modular of level $\Gamma(3N^2)$.*

(iii) *When* g.c.d.$(N,12)=4$, *the function $g_x(\tau)^{3m}$ is modular of level $\Gamma(N)$ iff the condition $\mathrm{Q}(x,N,3m)$ holds. In particular, $g_x(\tau)^3$ is modular of level $\Gamma(4N^2)$.*

Proof. The first claims of (i)–(iii) are only special cases of [KL81, Chap. 3, Ths. 5.2 and 5.3]. To see the latter claim of (i), apply $\mathrm{Q}(x, N^2, 12)$ to $x = (Nr_1/N^2, Nr_2/N^2)$. The latter claims of (ii), (iii) follow similarly by applying $\mathrm{Q}(x, 3N^2, 4)$, $\mathrm{Q}(x, 4N^2, 3)$ respectively. □

Proposition 4.2.2. *For $x = (x_1, x_2) \in \mathbb{R}^2$, put $\theta_x(\tau) := \theta(x_1\tau + x_2, \tau)$. Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then*

$$\theta_x(A\tau) = \theta_{xA}(\tau) \qquad (\tau \in \mathfrak{H}).$$

In particular, $\theta_x(\tau) = \theta_{-x}(\tau)$.

Proof. By [KL81, (K1)], we know $\ell_x(A\tau) = (c\tau + d)^{-1}\ell_{xA}(\tau)$. This together with the well known formula $\Delta(A\tau) = (c\tau + d)^{12}\Delta(\tau)$ proves the desired formula. (In [L87, Chap. 19, §2, (S2)], a similar formula is claimed to hold at the level of g_x. But this is false, as the transformation formula of $\eta(\tau)$ involves another nontrivial "Dedekind sum factor" $\in \mu_{24}$ besides $c\tau + d$.) □

Before stepping forward, let us review similar behaviors to Proposition 4.2.1 for certain powers of the Dedekind η-function $\eta(\tau)$.

Proposition 4.2.3. (i) *$\eta(\tau)^{24}$ is a modular form of weight 12 and level $\Gamma(1)$.*
(ii) *$\eta(\tau)^8$ is a modular form of weight 4 and level $\Gamma(3)$.*
(iii) *$\eta(\tau)^6$ is a modular form of weight 3 and level $\Gamma(4)$.*

Proof. This is essentially included in [KL81, Chap. 3, Lemma 5.1] (where $\Gamma(3)$ should read $\Gamma(4)$). We reproduce the proof for the reader's convenience. The general transformation formula of η is

$$\eta\left(\frac{a\tau + b}{c\tau + d}\right) = \varepsilon(a, b, c, d)\sqrt{\frac{c\tau + d}{i}}\,\eta(\tau) \qquad \left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}),\ c > 0\right),$$

where $\varepsilon(a, b, c, d)$ is a certain 24-th root of 1 given by a precise formula (cf. [Rad73, (74.93)]). (i) follows immediately. For (ii), observe that

$$\varepsilon(a, b, c, d)^8 = \begin{cases} \exp\left(\frac{2}{3}\pi i(bd(1 - c^2) + c(a + d))\right) & (c \text{ odd}), \\ \exp\left(\frac{2}{3}\pi i(ac(1 - d^2) + d(b - c))\right) & (d \text{ odd}), \end{cases}$$

and that in either case $\varepsilon(a, b, c, d)^8 = 1$ when $3 \mid b, c$. For (iii), we also calculate in the case of d odd that

$$\varepsilon(a, b, c, d)^6 = \exp\left(\tfrac{3}{2}\pi id\right)\exp\left(\tfrac{\pi i}{2}(ac(1 - d^2) + d(b - c))\right).$$

Since $8 \mid (1 - d^2)$ for d odd, when $4 \mid b, c$ we have $\varepsilon(a, b, c, d)^6 = \exp\left(\frac{3}{2}\pi id\right)$. Given $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(4)$, if $c > 0$, we may apply the above transformation formula

directly, and then $d \equiv 1$ (4) implies $\varepsilon^6 = i^{-1}$. Hence $\eta(A\tau) = (c\tau+d)^3\eta(\tau)$. If $c < 0$, we apply the formula for $-A$. Then $\varepsilon(-a,-b,-c,-d)^6 = i$. But this time, the factor from $\sqrt{*}$ is $(-c\tau-d)^3/i^3$. Hence, we obtain again $\eta(A\tau) = \eta((-A)\tau) = (c\tau+d)^3\eta(\tau)$ as desired. □

We shall sometimes write $\Delta(\tau)$ for $\eta(\tau)^{24} = \Delta(2\pi i\mathfrak{L}_\tau)$. The following proposition will be applied later in §6.5.

Proposition 4.2.4. *Let* $x = (x_1, x_2) = (r_1/ml, r_2/ml) \in \mathbb{Q}^2$ *for* $m, l \in \mathbb{N}$, $r_1, r_2 \in \mathbb{Z}$.

(i) $\Delta(\tau)\big(\frac{\theta_x(\tau)^{l^2}}{\theta_{lx}(\tau)}\big) = \eta(\tau)^{24}\frac{g_x(\tau)^{12l^2}}{g_{lx}(\tau)^{l^2}}$ *is a modular form of weight* 12 *and level* $\Gamma(lm)$.

(ii) *When* $l = 3$, $\eta(\tau)^8\frac{(g_x(\tau)^4)^9}{g_{3x}(\tau)^4}$ *is a modular form of weight* 4 *and level* $\Gamma(3m)$.

(iii) *When* $l = 2$, $\eta(\tau)^6\frac{(g_x(\tau)^3)^4}{g_{2x}(\tau)^3}$ *is a modular form of weight* 3 *and level* $\Gamma(2m)$.

Proof. The claims on weights are obvious, so only levels should be discussed. We shall intensively make use of [KL81, Chap. 3, Theorem 4.1] by rewriting

$$\Delta\frac{\theta_x^{l^2}}{\theta_{lx}} = (2\pi i)^{12(l^2-1)}\eta^{24l^2}\frac{\ell_x^{12l^2}}{\ell_{lx}^{12}}, \qquad \eta^8\frac{(g_x^4)^9}{g_{3x}^4} = (2\pi i)^{32}\eta^{72}\frac{\ell_x^{36}}{\ell_{3x}^4},$$
$$\eta^6\frac{(g_x^3)^4}{g_{2x}^3} = (2\pi i)^9\eta^{24}\frac{\ell_x^{12}}{\ell_{2x}^3}.$$

It is easy to see that the factors $\ell_x^{12l^2}/\ell_{lx}^{12}$, ℓ_x^{36}/ℓ_{3x}^4 (for $l = 3$) and ℓ_x^{12}/ℓ_{2x}^3 (for $l = 2$) satisfy the Kubert–Lang condition QUAD(ml), QUAD($3m$), QUAD($2m$) of [KL81] respectively (no matter if m, l are even or odd). Since η^{24} is a full level modular form, the proof is complete. □

§4.3. Eisenstein series

Next, we review the Eisenstein series $G_k^{(\mathbf{a} \bmod N)}$ and $E_k^{(\mathbf{x})}$. Our main reference here is [Sch74]. Let $k \geq 2$, $N \geq 1$ be integers and let $\mathbf{a} = (a_1, a_2) \in (\mathbb{Z}/N\mathbb{Z})^2$. We first define

$$G_k^{(\mathbf{a} \bmod N)}(\tau) := \lim_{s\to 0+}\sum_{\mathbf{a} \bmod N}{}' \frac{1}{(m_1\tau+m_2)^k}\frac{1}{|m_1\tau+m_2|^s} \qquad (\tau \in \mathfrak{H}),$$

where the sum is taken over all $(m_1, m_2) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ with $m_1 \equiv a_1$, $m_2 \equiv a_2$ (mod N). Note that, in the above formula, if $k \geq 3$ then we do not need $\lim_s$ and the factor $|\ldots|^s$, because $\sum'_{m_1,m_2} 1/(m_1\tau+m_2)^k$ converges absolutely and uniformly on each compact set. The trick of $\lim_{s\to 0+}$ (Hecke) works essentially

when $k=2$ (and $k=1$). The function $G_2^{(\mathbf{a} \bmod N)}$ is not holomorphic as seen from the following "q-expansion" formula:

$$G_k^{(\mathbf{a} \bmod N)}(\tau) = \begin{cases} \dfrac{-2\pi i}{N^2(\tau-\bar{\tau})} + \displaystyle\sum_{\nu \geq 0} \alpha_\nu(N,2,\mathbf{a}) q_\tau^\nu & (k=2), \\ \displaystyle\sum_{\nu \geq 0} \alpha_\nu(N,k,\mathbf{a}) q_\tau^\nu & (k \geq 3), \end{cases} \tag{4.3.1}$$

where

$$\alpha_\nu(N,k,\mathbf{a}) = \begin{cases} \delta\left(\dfrac{a_1}{N}\right) \displaystyle\sum_{m_2 \equiv a_2\,(N)}{}' \dfrac{1}{m_2^k} & (\nu=0), \\ \dfrac{(-2\pi i)^k}{N^k(k-1)!} \displaystyle\sum_{m \mid \nu,\ \frac{\nu}{m} \equiv a_1\,(N)} m^{k-1} \operatorname{sgn}(m) \zeta_N^{a_2 m} & (\nu \geq 1). \end{cases}$$

For applications, more important are certain linear combinations of the Eisenstein series of the above type: Given a pair $\mathbf{x} = (x_1, x_2) \in (\mathbb{Q}/\mathbb{Z})^2$, choose any (large) N such that $\mathbf{x} \in (\frac{1}{N}\mathbb{Z}/\mathbb{Z})^2$. Then define

$$E_k^{(\mathbf{x})}(\tau) := \frac{(k-1)!}{(2\pi i)^k} \sum_{\bar{a} \in (\mathbb{Z}/N\mathbb{Z})^2} e^{2\pi i(x_1 a_2 - x_2 a_1)} G_k^{(\mathbf{a} \bmod N)}(\tau).$$

It turns out that $E_k^{(\mathbf{x})}(\tau)$ is independent of the choice of N with $\mathbf{x} \in \left(\frac{1}{N}\mathbb{Z}/\mathbb{Z}\right)^2$ and is holomorphic unless $k=2, \mathbf{x}=(0,0)$. We have the following "q-expansion" formula:

$$\begin{aligned} E_k^{(\mathbf{x})}(\tau) = -\frac{P_k(x_1)}{k} &+ \sum_{0 < s \in x_1 + \mathbb{Z}} \sum_{l=1}^{\infty} s^{k-1} e^{2\pi i l(x_2 + s\tau)} \\ &+ \sum_{0 < s \in -x_1 + \mathbb{Z}} \sum_{l=1}^{\infty} s^{k-1} e^{2\pi i l(-x_2 + s\tau)}, \end{aligned} \tag{4.3.2}$$

for $k \geq 3$ or $\mathbf{x} \neq \mathbf{0}$, while in the exceptional case of $k=2$ and $\mathbf{x}=(0,0)$, one should add to the above right hand side the non-holomorphic term $i/(2\pi(\tau-\bar{\tau}))$. Here, $P_k : \mathbb{R}/\mathbb{Z} \to \mathbb{R}$ is the periodic Bernoulli function defined as follows. First, the k-th Bernoulli polynomial $B_k(X) \in \mathbb{Q}[X]$ is defined by the generating function $\sum_k B_k(X) t^k/k! = te^{tX}/(e^t-1)$. Then, using the floor function $\lfloor * \rfloor := \max\{n \in \mathbb{Z} \mid n \leq *\}$, define $P_k(t \bmod \mathbb{Z})$ to be $B_k(t - \lfloor t \rfloor)$ for $k \geq 2$. Note that since $B_k(0) = B_k(1)$ for $k \geq 2$, P_k $(k \geq 2)$ are continuous functions. Meanwhile, P_1 (defined similarly as $t - \lfloor t \rfloor - 1/2$ on $\mathbb{R}/\mathbb{Z} - \{0\}$) is discontinuous at 0 so that we set $P_1(0) = 0$ as the mean of $P_1(0+)$ and $P_1(0-)$. From the definitions of $G_k^{(\mathbf{a} \bmod N)}$

and $E_k^{(\mathbf{x})}$, we get the transformation formulae

$$G_k^{(\mathbf{a}\bmod N)}(A\tau) = (c\tau+d)^k G_k^{(\mathbf{a}A\bmod N)}, \tag{4.3.3}$$
$$E_k^{(\mathbf{x})}(A\tau) = (c\tau+d)^k E_k^{(\mathbf{x}A)}$$

for $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. It then follows that both $G_k^{(\mathbf{a}\bmod N)}$ and $E_k^{(\mathbf{x})}$ are modular forms of weight k of level $\Gamma(N)$. Finally, comparing the q-expansion formula, we may relate the Siegel function $g_x(\tau)$ and the Eisenstein series $E_2^{(\mathbf{x})}(\tau)$ as follows:

$$\frac{d}{d\tau}\log g_x(\tau) = -2\pi i E_2^{(\mathbf{x})}(\tau) \quad (\mathbf{x} = x \bmod \mathbb{Z} \in (\mathbb{Q}/\mathbb{Z})^2,\ x \in \mathbb{Q}^2 \setminus \mathbb{Z}^2). \tag{4.3.4}$$

Indeed, for $x = (x_1, x_2) = (m_1/N, m_2/N) \in \mathbb{Q}^2$, write $z = x_1\tau + x_2$ so that $q_z = \zeta_N^{m_2} q_\tau^{m_1/N}$, and set

$$\Pi := (1-q_z)\prod_{n=1}^{\infty}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}),$$
$$\Pi^+ := \prod_{0<s\in x_1+\mathbb{Z}}(1-e^{2\pi i x_2}e^{2\pi i s\tau})\cdot \prod_{0<s\in -x_1+\mathbb{Z}}(1-e^{-2\pi i x_2}e^{2\pi i s\tau}).$$

Formula (4.3.4) above follows immediately after applying Lemma 4.3.5 below.

Lemma 4.3.5. *For $x = (x_1, x_2) \in \mathbb{R}^2$, we have*

$$\Pi = \Pi^+ \cdot (-1)^{\lfloor x_1\rfloor} e^{-2\pi i x_2 \lfloor x_1\rfloor} e^{\pi i\tau(P_2(x_1)-B_2(x_1))}(1-e^{2\pi i x_2})^{\delta_{x_1\in\mathbb{Z}}},$$

where we understand $\delta_{x_1\in\mathbb{Z}} = \begin{cases} 1 & (x_1\in\mathbb{Z}) \\ 0 & (x_1\notin\mathbb{Z}) \end{cases}$ and $0^0 = 1$.

Proof. When $x \in \mathbb{Z}^2$, we have both $\Pi = 0$ and $(1-e^{2\pi i x_2})^{\delta_{x_1\in\mathbb{Z}}} = 0$, so that the above equation is trivially true. So we shall assume $x \in \mathbb{R}^2 \setminus \mathbb{Z}^2$. If $x_1 = 0$, then $q_z = e^{2\pi i x_2}$, hence $\Pi = (1-q_z)\Pi^+$, which gives us the desired equation. For the case $x_1 \neq 0$, we shall compare factors appearing in Π and Π^+, and apply consecutively $(1-e^{2\pi i\beta}q_\tau^\alpha)/(1-e^{-2\pi i\beta}q_\tau^{-\alpha}) = (-1)e^{2\pi i\beta}q_\tau^\alpha$. Suppose first $x_1 > 0$. Then

$$\begin{aligned}\Pi &= \Pi^+\cdot(1-e^{2\pi i x_2})^{\delta_{x_1\in\mathbb{Z}}}\prod_{i=0}^{\lfloor x_1\rfloor-1}\frac{1-e^{-2\pi i x_2}q_\tau^{-i-\{x_1\}}}{1-e^{2\pi i x_2}q_\tau^{i+\{x_1\}}}\\ &= \Pi^+\cdot(1-e^{2\pi i x_2})^{\delta_{x_1\in\mathbb{Z}}}\prod_{i=0}^{\lfloor x_1\rfloor-1}\left(-e^{2\pi i x_2}q_\tau^{i+\{x_1\}}\right)^{-1}\\ &= \Pi^+\cdot(-1)^{\lfloor x_1\rfloor}\left(e^{2\pi i x_2\lfloor x_1\rfloor}q_\tau^{\frac{1}{2}\lfloor x_1\rfloor(2x_1-\lfloor x_1\rfloor-1)}\right)^{-1}(1-e^{2\pi i x_2})^{\delta_{x_1\in\mathbb{Z}}}.\end{aligned}$$

But since $P_2(x)-B_2(x) = \lfloor x\rfloor(\lfloor x\rfloor+1-2x)$, the RHS is found to be of the desired form. Next, suppose $x_1 < 0$. Then

$$\begin{aligned}\Pi &= \Pi^+ \cdot (1-e^{2\pi i x_2})^{\delta_{x_1\in\mathbb{Z}}} \prod_{i=1}^{\lceil -x_1\rceil} \frac{1-e^{2\pi i x_2} q_\tau^{-i+\{x_1\}}}{1-e^{-2\pi i x_2} q_\tau^{i-\{x_1\}}} \\ &= \Pi^+ \cdot (1-e^{2\pi i x_2})^{\delta_{x_1\in\mathbb{Z}}} \prod_{i=1}^{\lceil -x_1\rceil} \left(-e^{2\pi i x_2} q_\tau^{-i+\{x_1\}}\right) \\ &= \Pi^+ \cdot (-1)^{\lceil -x_1\rceil} e^{2\pi i x_2 \lceil -x_1\rceil} q_\tau^{\frac{1}{2}\lceil -x_1\rceil(2\{x_1\}-\lceil -x_1\rceil-1)} \cdot (1-e^{2\pi i x_2})^{\delta_{x_1\in\mathbb{Z}}} \\ &= \Pi^+ \cdot (-1)^{\lfloor x_1\rfloor} e^{-2\pi i x_2 \lfloor x_1\rfloor} q_\tau^{-\frac{1}{2}\lfloor x_1\rfloor(2x_1-\lfloor x_1\rfloor-1)} \cdot (1-e^{2\pi i x_2})^{\delta_{x_1\in\mathbb{Z}}},\end{aligned}$$

which again turns out to be of the desired form. □

In §7.3, we will discuss a standard lift of the logarithmic derivative equation (4.3.4), which will play a crucial role in our proof of Theorem B stated in the Introduction.

§4.4. Algebraic modular forms

Let $f(\tau)$ be a holomorphic modular form of weight k and level $\Gamma(N)$, and suppose that its $q^{1/N}$-expansion has coefficients in a subring $R \subset \mathbb{C}$. Then it is known (see [K76, 2.1.1 and 2.4.1]) that there is an algebraic modular form F over R which assigns, to each tuple $(E,\, \beta\colon \mathbb{Z}/N\mathbb{Z}\times\mu_N \xrightarrow{\sim} E[N],\, \omega)$ over an R-algebra B (i.e., a $\Gamma(N)^{\mathrm{arith}}$-test object over B in the sense of [K76] consisting of a $\Gamma(1)$-test object (E, O, ω) over B together with a B-isomorphism of group schemes $\beta : \mathbb{Z}/N\mathbb{Z}\times\mu_N \xrightarrow{\sim} E[N]$), a value $F(E,\beta,\omega)\in B$ in such a way that

(1) $F(E,\beta,\omega)$ depends only on the B-isomorphism class of the test object;

(2) $F(E,\beta,\lambda\omega) = \lambda^{-k}F(E,\beta,\omega)$ for each $\lambda\in B^\times$;

(3) if $(E'/B', \beta', \omega')$ is the scalar extension of (E,β,ω) by the R-homomorphism $\phi : B\to B'$, then $\phi(F(E,\beta,\omega)) = F(E',\beta',\omega')$;

(4) for any complex point $s\in \mathrm{Spec}(B)(\mathbb{C})$ given by $\phi_s : B\to\mathbb{C}$ with the fiber $(E_s/\mathbb{C}, \beta_s, \omega_s)$ over s,

$$\phi_s(F(E_s,\beta_s,\omega_s)) = \left(\frac{2\pi i}{\varpi_2}\right)^k f(\tau),$$

where $\tau = \varpi_1/\varpi_2 \in \mathfrak{H}$ is given as the quotient of a $\mathbb{Z}$-basis (ϖ_1,ϖ_2) of the lattice obtained as the collection of period integrals of ω_s along loops on E_s so that $\frac{1}{N}\varpi_1 \bmod \mathfrak{L} = \beta((1,1))$, $\frac{1}{N}\varpi_2 \bmod \mathfrak{L} = \beta((0, e^{2\pi i/N}))$.

Conversely, suppose we are given an algebraic modular form F of weight k and level N over $R\subset\mathbb{C}$. Then the corresponding holomorphic modular form f is given by $f(\tau) = F(\mathbb{C}^\times/(q_{\tau/N})^{N\mathbb{Z}}, \iota, \omega_{\mathrm{can}})$, where $q_{\tau/N} = e^{2\pi i\tau/N}$, ι is the canonical embedding $\mathbb{Z}/N\mathbb{Z}\times\mu_N \hookrightarrow \mathbb{C}^\times/q_\tau^{\mathbb{Z}}$ with $(a, e^{2\pi i b/N}) \mapsto (q_{\tau/N}^a, e^{2\pi i b/N})$, and ω_{can}

is the "canonical differential" coming from dX/X on $\mathbf{G}_m = \operatorname{Spec} \mathbb{Z}[X, X^{-1}]$ (cf. [KM85, (8.8)]). The value of F at the Tate curve $\operatorname{Tate}(q^N)/R(\!(q)\!)$ gives the q $(= e^{2\pi i\tau/N})$-expansion of f.

The above may be applied to the modular units and modular forms of the previous subsections.

We first consider the case of Eisenstein series. If $\mathbf{x} \in \frac{1}{N}\mathbb{Z}^2/\mathbb{Z}^2$ is given, then the Eisenstein series $E_k^{(\mathbf{x})}(\tau)$ is a holomorphic modular form of weight k and level $\Gamma(N)$ unless $k = 2$ and $\mathbf{x} = \mathbf{0}$. The q-expansion given in (4.3.2) has coefficients in $\mathbb{Q}(\mu_N)$. Hence, the corresponding algebraic modular form is defined over $\mathbb{Q}(\mu_N)$. We may apply it to any $\Gamma(N)^{\text{arith}}$-test object $(E/B, \beta, \omega_N)$. Moreover, we shall also regard any $\Gamma(N)$-test object $(E/B, \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N], \omega)$ as a $\Gamma(N)^{\text{arith}}$-test object, defining $\beta : (\mathbb{Z}/N\mathbb{Z}) \times \mu_N \xrightarrow{\sim} E[N]$ by $\beta(a, \zeta_N^b) = \alpha(a, b)$, where $\zeta_N = e_N(\alpha(1,0), \alpha(0,1)) \in B$ (cf. 2.6). Thus, one can speak about

$$E_k^{(\mathbf{x})}(E/B, \alpha \text{ (or } \beta), \omega) \in B[\mu_N] \quad (k \geq 3 \text{ or } \mathbf{x} \neq (0,0)). \tag{4.4.1}$$

In a similar way, since the modular forms $\Delta = \eta^{24}$, η^8, η^6 which appeared in Proposition 4.2.3 have rational q-coefficients, they give algebraic modular forms of the prescribed weight and level over $\mathbb{Q}$.

For example, suppose we are given a $\Gamma(1)$-test object $(E/B, O, \omega)$ with the associated parameter (x, y, g_2, g_3, t) (cf. 2.2). Then one can easily show that

$$\begin{gathered} g_2 = 10E_4^{(0,0)}(E/B, O, \omega), \quad g_3 = \tfrac{7}{6}E_6^{(0,0)}(E/B, O, \omega); \\ g_2^3 - 27g_3^2 = \Delta(E/B, O, \omega). \end{gathered} \tag{4.4.2}$$

Next, we consider modular units. Assume $x = (x_1, x_2) \in \frac{1}{N}\mathbb{Z}^2 \setminus \mathbb{Z}^2$ (hence $N^2 \geq 3$). By Proposition 4.2.1, $\theta_x(\tau) = g_x(\tau)^{12}$ and its inverse are modular functions of level $\Gamma(N^2)$. Observing the q-expansion, we know that there are corresponding algebraic modular forms $\theta_x^{\pm 1}$ of weight 0 and level $\Gamma(N^2)$ defined over $\mathbb{Q}(\mu_{N^2})$. So, we may apply $\theta_x^{\pm 1}$ to $\Gamma(N^2)^{\text{arith}}$-test objects and $\Gamma(N^2)$-test objects. Thus,

$$\theta_x(E/B, \alpha \text{ (or } \beta), \omega) \in B[\mu_{N^2}]^\times \tag{4.4.3}$$

makes sense. In fact, in the case of weight 0, the value is independent of the change of ω (by multiplication by elements of $B^\times$). This means that the value comes from the representative morphism of $\operatorname{Spec}(B)$ to the modular curve $Y(N^2)$ of level $\Gamma(N^2)$ defined over $\mathbb{Q}(\mu_{N^2})$. The space of complex points of $Y(N^2)$ is identified with the Fuchsian model $\mathfrak{H}/\Gamma(N^2)$. Write $\mathcal{O}(\Gamma(N^2))$ for the ring of holomorphic modular functions of level $\Gamma(N^2)$ whose Fourier coefficients with respect to $e^{2\pi i\tau/N^2}$ lie in $\mathbb{Q}(\mu_{N^2})$, so that $Y(N^2) = \operatorname{Spec}(\mathcal{O}(\Gamma(N^2)))$. Then by [Sh71,

Prop. 6.9],

$$\theta_x(\tau) \in \mathcal{O}(\Gamma(N^2))^\times. \tag{4.4.4}$$

The conclusion is that the image of $\theta_x(\tau)$ under the representative homomorphism $\mathcal{O}(\Gamma(N^2)) \to B$ coincides with $\theta_x(E/B, \alpha, \omega)$.

For the other cases of Proposition 4.2.1 where each of g_x^{12m}, g_x^{4m} or g_x^{3m} becomes a modular function of level $\Gamma(N)$ under suitable conditions, one can talk about $g_x^{12m}(E/B, \alpha, \omega) \in B[\mu_N]^\times$ as the image of $g_x^{12m}(\tau) \in \mathcal{O}(\Gamma(N))$ etc. in similar ways.

§4.5. Compatibilities of GL_2-actions

Before closing this section, we review the (left) action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ on the function field $\mathfrak{F}_N$ of the modular curve $Y(N)$ given in [Sh71, §6.2]. Decompose $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as the product of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and $D = \left\{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \mid d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\}$, and define the action on $\mathfrak{F}_N$ of each component as follows. Let $f(\tau) \in \mathfrak{F}_N$ have Fourier expansion in $q_\tau^{1/N}$ with coefficients in $\mathbb{Q}(\mu_N)$. We define the action of $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ by $f \mapsto f|_{{}^t A}$. Identify D with the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ and define its action on $f(\tau)$ by the Galois transformation of the Fourier coefficients. It follows, in particular, that

$$A(\zeta_N) = \zeta_N^{\det(A)} \quad (A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}). \tag{4.5.1}$$

The above action is compatible with the context we developed in §§2.8–2.9 as follows. With each $\sigma \in \pi_1(M_{1,1}, \bar{b})$ are associated the matrix $A = \rho^N(\sigma) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and the automorphism $\mathfrak{a}_\sigma^N \in \mathrm{Aut}(M_{1,1}[N]/M_{1,1})$ together with $\bar{\mathfrak{a}}_\sigma^N \in \mathrm{Aut}(Y(N)/Y(1))$. Our compatibility claim is then as follows.

Claim 4.5.2. *The automorphism $(|_{\bar{\mathfrak{a}}_\sigma^N})$ of $\mathfrak{F}_N$ defined by $(f|_{\bar{\mathfrak{a}}_\sigma^N})(s) = f(\bar{\mathfrak{a}}_\sigma^N(s))$ (where $s : \mathrm{Spec}(\mathbb{C}) \to M_{1,1}[N] \to Y(N)$ is any complex point) coincides with the above action of the matrix $A = {}^t\rho^N(\sigma)$ on $\mathfrak{F}_N$.*

Proof. Indeed, when σ fixes μ_N, the matrix $A = \rho^N(\sigma)$ is in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Then the claim follows from (2.9.3). So, we have only to consider the case where $A = \rho^N(\sigma)$ is of the form $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ ($d \in (\mathbb{Z}/N\mathbb{Z})^\times$). Recall that the $q^{1/N}$-expansion of f is given as the value at the Tate curve $\mathrm{Tate}(q)/\mathbb{Q}(\zeta_N)((q^{1/N}))$ with level N-structure $(1,0) \mapsto q^{1/N}$, $(0,1) \mapsto \zeta_N$ (where $\zeta_N = \exp(2\pi i/N) \in \mathbb{C}$). We can view it as the image of f under the homomorphism $\mathfrak{F}_N \to \mathbb{Q}(\mu_N)((q^{1/N}))$, which corresponds to a representative morphism $\phi : \mathrm{Spec}\big(\mathbb{Q}(\mu_N)((q^{1/N}))\big) \to Y(N)$. By (2.7.3), the value of $f|_{\bar{\mathfrak{a}}_\sigma^N}$ at ϕ is the value of f at $\phi' = \bar{\mathfrak{a}}_\sigma^N \circ \phi$, but (2.8.1) means that this ϕ' is the representative morphism of $\mathrm{Tate}(q)/\mathbb{Q}(\mu_N)((q^{1/N}))$ with the level N-structure

$(1,0) \mapsto q^{1/N}$, $(0,1) \mapsto \zeta_N^d$. The resulting value is thus what is obtained from f by changing all coefficients by the Galois transformation of $\mathbb{Q}(\mu_N)$ with $\zeta_N \mapsto \zeta_N^d$. $\square$

The above sort of compatibility also extends to the context of $\Gamma(1)$-test objects (§2.6) as follows. Suppose that $(E/B, O, \omega)$ is a $\Gamma(1)$-test object as in §2.3 and $\bar{b}$ is a base point on $S = \mathrm{Spec}(B)$. Let $(S^N, \bar{b}^N)$ be as in §2.6. Then there is a natural commutative diagram

$$\begin{array}{ccccc} S^N & \longrightarrow & M_{1,1}[N] & \longrightarrow & Y(N) \\ \downarrow & & \downarrow & & \\ S & \longrightarrow & M_{1,1} & & \end{array}$$

For each $\sigma \in \pi_1(S, \bar{b})$, there is an associated automorphism $\mathfrak{a}_\sigma^N \in \mathrm{Aut}(S^N/S)$ of §2.7. On the other hand, the image σ' of σ in $\pi_1(M_{1,1})$ induces an automorphism $\mathfrak{a}_{\sigma'}^N$ of $M_{1,1}[N]$ as in §2.8. The relation between these $\mathfrak{a}_\sigma^N$ and $\mathfrak{a}_{\sigma'}^N$ is, a priori, just a pointwise one, i.e., they convey $\bar{b}^N$ on S^N and its image on $M_{1,1}[N]$ to those points obtained respectively by monodromy transformations by σ, σ'. But this, together with the fact that S^N/S is a connected component of the pull-back of $M_{1,1}[N]/M_{1,1}$ by $S \to M_{1,1}$ which is preserved by the pull-backs of $\mathfrak{a}_{\sigma'}^N$ ($\sigma \in \pi_1(S, \bar{b})$), ensures the commutativity of

$$\begin{array}{ccc} S^N & \longrightarrow & M_{1,1}[N]V \\ {\scriptstyle \mathfrak{a}_\sigma^N}\downarrow & & \downarrow{\scriptstyle \mathfrak{a}_{\sigma'}^N} \\ S^N & \longrightarrow & M_{1,1}[N] \end{array}$$

Thus, if $\iota : \mathcal{O}(\Gamma(N)) \to B^N$ designates the ring homomorphism of "functions" corresponding to the morphism $S^N \to Y(N)$, we deduce from Claim 4.5.2 that

$$\iota(f)|_{\mathfrak{a}_\sigma^N} = \iota(f|_{{}^t\rho^N(\sigma)}) \quad (\sigma \in \pi_1(S, \bar{b})). \tag{4.5.3}$$

§4.6. GL_2-action on modular units and its refinements

We are particularly interested in a consequence of the above discussion for the modular units θ_x, g_x^4, g_x^3 of level $\Gamma(N^2)$, $\Gamma(3N^2)$, $\Gamma(4N^2)$ respectively. First, from the Fourier expansion of $\theta_x(\tau)$ ($x = (x_1, x_2) \in \frac{1}{N}\mathbb{Z}^2$), we see that the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ ($d \in (\mathbb{Z}/N^2\mathbb{Z})^\times$) maps $\theta_x \mapsto \theta_{(x_1, dx_2)}$. This and Proposition 4.2.2 imply the formula

$$\theta_x|_{{}^tA} = \theta_{x({}^tA)} \quad \big(x \in \tfrac{1}{N}\mathbb{Z}^2,\ A \in \mathrm{GL}_2(\mathbb{Z}/N^2\mathbb{Z})\big). \tag{4.6.1}$$

Note that the lower equation of (4.1.4) implies

$$\theta_x = \theta_y \quad \big(x \equiv y \bmod N;\ x=(x_1,x_2),\ y=(y_1,y_2) \in \big(\tfrac{1}{N}\mathbb{Z}\big)^2\big). \tag{4.6.2}$$

In other words, $\mathrm{GL}_2(\mathbb{Z}/N^2\mathbb{Z})$ has a well defined action on the indices $\big(\frac{1}{N}\mathbb{Z}/N\mathbb{Z}\big)^2$ of modular units θ_x. Then, combining (4.5.3) and (4.6.1) we obtain, for any $\Gamma(N^2)$-test object (E,α,ω),

$$\theta_x(E,\alpha,\omega)|_{\mathfrak{a}_\sigma^{N^2}} = \theta_{x({}^t\rho^{N^2}(\sigma))}(E,\alpha,\omega) \quad \big(x=(x_1,x_2) \in \big(\tfrac{1}{N}\mathbb{Z}\big)^2,\ \sigma \in \pi_1(S,\bar{b})\big). \tag{4.6.3}$$

In exactly the same way, parallel statements to the above for g_x^4, g_x^3 hold after replacing N^2 by $3N^2$, $4N^2$ respectively. But we have to work in a subtler way using the definition of g_x as the product of $2\pi i\eta^2$ and the Klein form $\ell_x(\tau)$. As seen in Propositions 4.2.1 and 4.2.3, the functions g_x^4 and g_x^3 can be defined in the language of lattices with level 3 or 4 basis of torsion points. For Klein forms $\ell_x\big(\begin{smallmatrix}\varpi_1\\ \varpi_2\end{smallmatrix}\big) := \ell(x_1\varpi_1+x_2\varpi_2, \mathbb{Z}\varpi_1+\mathbb{Z}\varpi_2)$, the transformation formulas with respect to $x=(r/N,s/N) \in \big(\frac{1}{N}\mathbb{Z}\big)^2$, $y=(b_1,b_2)\in\mathbb{Z}^2$ and $A=\big(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\big) \in \Gamma(N)$ in [KL81, (K2), (K3), p. 28] read:

$$\begin{cases} \ell_{x+y}\big(\big(\begin{smallmatrix}\varpi_1\\ \varpi_2\end{smallmatrix}\big)\big) = \varepsilon(x,y)\ell_x\big(\big(\begin{smallmatrix}\varpi_1\\ \varpi_2\end{smallmatrix}\big)\big), \\ \ell_x\big(A\big(\begin{smallmatrix}\varpi_1\\ \varpi_2\end{smallmatrix}\big)\big) = \ell_{xA}\big(\big(\begin{smallmatrix}\varpi_1\\ \varpi_2\end{smallmatrix}\big)\big) = \varepsilon_x(A)\ell_x\big(\big(\begin{smallmatrix}\varpi_1\\ \varpi_2\end{smallmatrix}\big)\big), \end{cases} \tag{4.6.4}$$

with

$$\varepsilon(x,y) = (-1)^{b_1b_2+b_1+b_2}e^{-2\pi i\frac{b_1s-b_2r}{2N}}, \tag{K2}$$

$$\varepsilon_x(A) = -(-1)^{\left(\frac{a-1}{N}r+\frac{c}{N}s+1\right)\left(\frac{b}{N}r+\frac{d-1}{N}s+1\right)}e^{2\pi i\frac{br^2+(d-a)rs-cs^2}{2N^2}}. \tag{K3}$$

One can then derive invariance of g_x^4 (resp. g_x^3) for $x \in (\frac{1}{N}\mathbb{Z})^2$ modulo $x \mapsto x+(3N\mathbb{Z})^2$ (resp. $x \mapsto x+(4N\mathbb{Z})^2$), i.e.,

$$g_x^4 = g_y^4 \quad \big(x \equiv y \bmod 3N;\ x=(x_1,x_2),\ y=(y_1,y_2) \in \big(\tfrac{1}{N}\mathbb{Z}\big)^2\big), \tag{4.6.5}$$

$$g_x^3 = g_y^3 \quad \big(x \equiv y \bmod 4N;\ x=(x_1,x_2),\ y=(y_1,y_2) \in \big(\tfrac{1}{N}\mathbb{Z}\big)^2\big). \tag{4.6.6}$$

Concerning the GL_2-action, invariance of type (4.6.1) or Proposition 4.2.2 for g_x^4, g_x^6 is not available, mainly because of the η^2-factor of $g_x = 2\pi i\eta^2\ell_x$. We still find

$$g_x^4|_{{}^tA} = \zeta \cdot g_{x({}^tA)}^4 \quad \big(x \in \tfrac{1}{N}\mathbb{Z}^2,\ A \in \mathrm{GL}_2(\mathbb{Z}/3N^2\mathbb{Z}),\ \zeta \in \mu_3\big), \tag{4.6.7}$$

$$g_x^3|_{{}^tA} = \zeta \cdot g_{x({}^tA)}^3 \quad \big(x \in \tfrac{1}{N}\mathbb{Z}^2,\ A \in \mathrm{GL}_2(\mathbb{Z}/4N^2\mathbb{Z}),\ \zeta \in \mu_4\big). \tag{4.6.8}$$

We also obtain statements corresponding to (4.6.2) by replacing N^2 by $3N^2$ (resp. $4N^2$) for $\Gamma(3N^2)$-(resp. $\Gamma(4N^2)$-)test objects modulo μ_3 (resp. μ_4).

§5. Universal elliptic curve

§5.1. Quick review of Grothendieck–Teichmüller theory

The starting point of Grothendieck–Teichmüller theory was Belyĭ's theorem [B79] which implies, in particular, that the absolute Galois group $G_{\mathbb{Q}}$ is embedded into the (outer) automorphism group of a simplest profinite group $\hat{F}_2 := \pi_1(\mathbf{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\})$. We fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, and take $\mathbf{x}$, $\mathbf{y}$ to be loops as illustrated below:

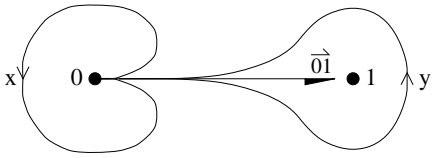


Figure 1

This enables us to parameterize the elements of $G_{\mathbb{Q}}$ in terms of the cyclotomic character $\chi : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^{\times}$ together with a mysterious parameter $f : G_{\mathbb{Q}} \to \hat{F}_2' = [\hat{F}_2, \hat{F}_2]$ $(\sigma \mapsto \mathfrak{f}_\sigma)$ in such a way that a lift of $\sigma \in G_{\mathbb{Q}}$ acts on standard generators $\mathbf{x}$, $\mathbf{y}$ of $\hat{F}_2$ by the formula

$$\sigma(\mathbf{x}) = \mathbf{x}^{\chi(\sigma)}, \qquad \sigma(\mathbf{y}) = \mathfrak{f}_\sigma^{-1}\mathbf{y}^{\chi(\sigma)}\mathfrak{f}_\sigma. \tag{5.1.1}$$

The above standard lift (Belyĭ's lift of $G_{\mathbb{Q}}$ into $\mathrm{Aut}(\hat{F}_2)$) is understood geometrically via the notion of tangential base point $\overrightarrow{01}$ introduced by Deligne [De89].

The collection $\{(\chi(\sigma), \mathfrak{f}_\sigma) \in \hat{\mathbb{Z}}^{\times} \times \hat{F}_2' \mid \sigma \in G_{\mathbb{Q}}\}$ is thus a copy of $G_{\mathbb{Q}}$ mapped into the "concrete set" $\hat{\mathbb{Z}}^{\times} \times \hat{F}_2'$. One important open problem is to characterize the copied image. In this direction, the (profinite) Grothendieck–Teichmüller group $\widehat{GT}$ was introduced by Drinfeld [Dr90] and Ihara [Ih90], and some of its refined versions/variants have been studied by several authors (cf., e.g., [LS06], [F10]).

Besides the fundamental property $G_{\mathbb{Q}} \hookrightarrow \widehat{GT}$, important is the reason why it is called $\widehat{GT}$, namely, as expected by Grothendieck [G84], that it should act on (a tower of) the profinite Teichmüller groups $\pi_1(M_{g,n})$ $(2 - 2g - n < 0)$ in a certain consistent way in view of "cutting and pasting of Riemann surfaces". This second feature has been, to a certain extent, established in [NS00]–[N99-02] by introducing a group $\mathbb{\Gamma}$ intermediate between $G_{\mathbb{Q}}$ and $\widehat{GT}$.

Thus, theoretically one can write down the action of $G_{\mathbb{Q}}$ on those $\pi_1(M_{g,n})$ $(2 - 2g - n < 0)$ in terms of the two parameters $\chi(\sigma)$ and $\mathfrak{f}_\sigma$ $(\sigma \in G_{\mathbb{Q}})$. One interesting problem is to find information on the mysterious parameter $\mathfrak{f}_\sigma$ from the actions on various subgroups or quotients of $\pi_1(M_{g,n})$. Even in the most primitive case of $M_{0,4} = \mathbf{P}^1 - \{0, 1, \infty\}$, deep arithmetic nature was found in a series of works

by Y. Ihara and his colleagues [Ih86a], [Ih86b], [IKY87], [A89], [C89], [Ih99-00], [Ih02], [MS03]. Some other studies in this direction have also been performed, e.g., in a series of works [NT03-06], [NTY10].

§5.2. Tate elliptic curve

The Weierstrass equation of the Tate elliptic curve $\mathrm{Tate}(q)$ over $\mathbb{Q}((q))$ is given by

$$\mathrm{Tate}(q) : Y^2 = 4X^3 - g_2(q)X - g_3(q),$$

where

$$g_2(q) = 20\left(-\frac{B_4}{8} + \sum_{n\geq 1}\sigma_3(n)q^n\right), \tag{5.2.1}$$

$$g_3(q) = \frac{7}{3}\left(-\frac{B_6}{12} + \sum_{n\geq 1}\sigma_5(n)q^n\right). \tag{5.2.2}$$

($B_4 = -1/30$, $B_6 = 1/42$ are the Bernoulli numbers, and $\sigma_d(n)$ denotes the sum of the d-powers of the positive divisors of n.) Let $\bar{q}$ be the generic geometric point over $S_q := \mathrm{Spec}\big(\mathbb{Q}((q))\big)$ valued in the Puiseux power series field $\overline{\mathbb{Q}}\{\{q\}\}$, or more economically in

$$\Omega = \bigcup_{n=1}^{\infty}\ \bigcup_{[K:\mathbb{Q}]<\infty} K((q^{1/n})),$$

and let $\overrightarrow{\mathfrak{w}}_{\bar{q}}$ be the Weierstrass tangential base point on $\mathrm{Tate}(q)\setminus\{O\}$. The fundamental group $\pi_1(S_q,\bar{q})$ is canonically split as the semidirect product $G_{\mathbb{Q}} \ltimes \hat{\mathbb{Z}}(1)$ where $G_{\mathbb{Q}}$ acts on Ω via the coefficients of each Puiseux series. Therefore, the pro-$\mathcal{C}$ monodromy representation (§2.5) has the form

$$\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}_{\bar{q}}} : \pi_1(S_q,\bar{q}) = G_{\mathbb{Q}} \ltimes \hat{\mathbb{Z}}(1) \to \mathrm{Aut}\big(\pi_1(\mathrm{Tate}(q)\otimes\Omega\setminus\{O\}, \overrightarrow{\mathfrak{w}}_{\bar{q}})\big). \tag{5.2.3}$$

Based on the technique studied in [IN97], in [N99] we studied the restriction of $\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}_{\bar{q}}}$ to the $G_{\mathbb{Q}}$-part. Using the formal patching of $\pi_1(\mathbf{P}^1 - \{0,1,\infty\})$ along Néron polygons of Deligne–Rapoport type, we introduced suitable generators $\mathbf{x}_1, \mathbf{x}_2, \mathbf{z}$ of $\Pi_{1,1} := \pi_1((\mathrm{Tate}(q)\otimes\Omega\setminus\{O\}, \overrightarrow{\mathfrak{w}}_{\bar{q}})$ with $[\mathbf{x}_1,\mathbf{x}_2]\mathbf{z} = 1$ so that $\mathbf{z}$ gives the generator of the inertia group rotating once anticlockwise, and showed

Theorem 5.2.4 ([N99, Th. 3.4]). *The Galois representation $\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}_{\bar{q}}}|_{G_{\mathbb{Q}}}$ is expressed by the following formulae in terms of $(\chi(\sigma), \mathfrak{f}_\sigma) \in \widehat{GT}$:*

$$\begin{cases} \mathbf{x}_1 \mapsto \mathbf{z}^{(1-\chi(\sigma))/2}\mathfrak{f}_\sigma(\mathbf{x}_1\mathbf{x}_2\mathbf{x}_1^{-1},\mathbf{z})\mathbf{x}_1\mathfrak{f}_\sigma(\mathbf{x}_2^{-1},\mathbf{z})^{-1}, \\ \mathbf{x}_2 \mapsto \mathfrak{f}_\sigma(\mathbf{x}_2^{-1},\mathbf{z})\mathbf{x}_2^{\chi(\sigma)}\mathfrak{f}_\sigma(\mathbf{x}_2^{-1},\mathbf{z})^{-1}, \\ \mathbf{z} \mapsto \mathbf{z}^{\chi(\sigma)}. \end{cases} \tag{5.2.5}$$

□

(This theorem was shown for $\mathcal{C} = \{\text{all finite groups}\}$, hence holds for an arbitrary full class $\mathcal{C}$ of finite groups.) The choice of generators was given in a precise way using van Kampen type amalgamation of groups devised in a previous paper [N99-02, Part I]. Naively, those chosen generators may be illustrated as in the following picture, where $\mathbf{x}_2$ represents a vanishing cycle. In [N99], we gave an explicit description of $\mathcal{E}_\sigma^{\mathcal{C}}$ for the Tate curve with $\mathcal{C} = (p)$ the class of all finite p-groups and σ in the congruence kernel $G_{\mathbb{Q}}(\mu_{p^\infty})$. Note that in this case $\mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]]$ is isomorphic to the power series ring $\mathbb{Z}_p[[T_1, T_2]]$ with $T_i = \bar{\mathbf{x}}_i - 1$ $(i = 1, 2)$.

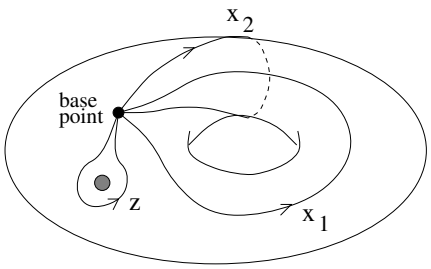


Figure 2

Theorem 5.2.6 ([N99, Ths. 3.3 and 3.5]). *Consider* $\mathcal{E}_\sigma^{(p)} \in \mathbb{Z}_p[[T_1, T_2]]$ *for the Tate curve* $\mathrm{Tate}(q)$ *over* $\mathbb{Q}((q))$. *Let* $U_i = \log(1+T_i)$ $(i=1,2)$. *Then, in* $\mathbb{Q}_p[[U_1, U_2]]$, *we have*

$$\mathcal{E}_\sigma^{(p)}(T_1, T_2) = \sum_{\substack{m \geq 2 \\ even}} \frac{\chi_{m+1}(\sigma)}{1 - p^m} \frac{U_2^m}{m!} \qquad (\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}).$$

Here $\chi_m : G_{\mathbb{Q}(\mu_{p^\infty})} \to \mathbb{Z}_p(m)$ *is the* m*-th Soulé character defined by the properties*

$$\Big(\prod_{\substack{1 \leq a < p^n \\ p \nmid a}} (1 - \zeta_{p^n}^a)^{a^{m-1}} \Big)^{\frac{1}{p^n}(\sigma - 1)} = \zeta_{p^n}^{\chi_m(\sigma)} \qquad (\forall n \geq 1). \qquad \square$$

In fact, in [N99] we gave two proofs; one using the explicit formula given in [N95], and one using the formula of Magnus–Gassner type to reduce the proof to the explicit formula for Ihara's power series (cf. [N99, (3.3); (3.5)–(3.6)]). In the next section, we shall generalize the explicit formula for finite level $\mathbb{E}_m^{\mathcal{C}}$ $(m \in |\mathcal{C}|)$.

§5.3. Mordell transformation on $M_{1,2}^\omega$

The universal once punctured elliptic curve $\mathcal{E} \setminus \{O\}$ over $M_{1,1}^\omega$ (§2.2) has a profile as $M_{1,2}^\omega$ which is by definition the fiber product of $M_{1,2}$ and $M_{1,1}^\omega$ over $M_{1,1}$. It is the representative scheme for the moduli problem of the $\Gamma(1)$-test objects $(E/B, O, \omega)$ with an extra section $P : B \to E$ disjoint from O.

It is also often useful to consider $M^{\omega}_{1,2}$ as the moduli space of quartic models of elliptic curves $Y^2 = f(X) = X^4 + bX^2 + cX + d$ with distinguished two infinities (∞_+, ∞_-), where $\infty_\pm$ corresponds respectively to $(\xi, \eta) = (0, \pm 1)$ after the change of variables $\xi = X^{-1}$, $\eta = YX^{-2}$. In [NTY10], we introduced the Mordell transformation $\mathfrak{M}$ which transforms this quartic model $Y^2 = f(X) = X^4 + bX^2 + cX + d$ to the Weierstrass cubic model

$$y^2 = 4x^3 - \left(\tfrac{4}{3}b^2 + 16d\right)x - \left(-\tfrac{8}{27}b^3 + \tfrac{32}{3}bd - 4c^2\right) \tag{5.3.1}$$

by the variable transformation

$$\begin{cases} X = \dfrac{-3y - 6c}{12x + 8b}, \\ Y = -x/2 + b/6 + X^2, \end{cases} \qquad \begin{cases} x = 2X^2 - 2Y + b/3, \\ y = 8X(Y - X^2 - b/2) - 2c. \end{cases} \tag{5.3.2}$$

The two marked points $\infty_\pm$ on the quartic model $Y^2 = f(X)$ are mapped to the points on E_f by

$$\begin{cases} \infty_+ \mapsto P_f := (-2b/3, 2c), \\ \infty_- \mapsto O. \end{cases} \tag{5.3.3}$$

Conversely, given an elliptic curve with Weierstrass equation $E : y^2 = 4x^3 - g_2x - g_3$ with a finite point $P = (x_0, y_0)$ on it, we can recover the quartic model

$$Y^2 = (\mathfrak{M}^{-1}(E, P))(X) := X^4 + \left(-\tfrac{3}{2}x_0\right)X^2 + \left(\tfrac{1}{2}y_0\right)X + \tfrac{1}{16}(g_2 - 3x_0^2). \tag{5.3.4}$$

We call this latter mapping $\mathfrak{M}^{-1}$ from (E, P) to the above quartic the *inverse Mordell transformation*.

An illustration of usefulness of these transformations was given in [NTY10], where a modified version of $\mathfrak{M}$ (written $\mathcal{M}$ there) is used, normalized to provide monic cubic models of elliptic curves. (Cf. also arguments in [N99-02, §7.8].)

§5.4. Cardano–Ferrari mapping of braid configuration space

We are now at the stage of considering braid configuration spaces. Let $\mathbf{A}^n_u \setminus D$ denote the space of monic polynomials of degree n in variable u with no multiple roots (here D is understood to be the discriminant locus), and let $(\mathbf{A}^n_u \setminus D)_0$ denote its subspace of those with second highest coefficient vanishing.

In [NTY10, (2.10)], we introduced the (Cardano–)Ferrari morphism

$$\mathcal{F}_0 : (\mathbf{A}^4_u \setminus D)_0 \to (\mathbf{A}^3_u \setminus D)_0$$

which assigns to a quartic its resolvent cubic in the following way:

$$\mathcal{F}_0(u^4 + bu^2 + cu + d) = u^3 - \left(\tfrac{1}{3}b^2 + 4d\right)u - \left(\tfrac{2}{27}b^3 - \tfrac{8}{3}bd + c^2\right).$$

(In our normalization, if T_1, T_2, T_3, T_4 are the zeros of a given quartic $u^4 + bu^2 + cu + d$, then the resolvent cubic $\mathcal{F}_0(u^4 + bu^2 + cu + d)$ has zeros $U_i = S_i + \frac{2}{3}b$ $(i = 1, 2, 3)$ with S_i is given by $S_1 = -(T_1+T_4)(T_2+T_3)$, $S_2 = -(T_1+T_3)(T_2+T_4)$, $S_3 = -(T_1 + T_2)(T_3 + T_4)$. (The term "$+\frac{2}{3}b$" is just for parallel transport to have $U_1 + U_2 + U_3 = 0$.) The solutions of the original quartic equation are given by those $\frac{1}{2}(\sqrt{S_1} + \sqrt{S_2} + \sqrt{S_3})$ with four choices of signs of $\sqrt{S_i}$'s satisfying $\sqrt{S_1}\sqrt{S_2}\sqrt{S_3} = -c$. (See also loc. cit., (2.6)). Let us now define

$$4\iota : (\mathbf{A}^3 \setminus D)_0 \to M^{\omega}_{1,1}, \qquad \gamma(u) \mapsto y^2 = -4\gamma(-x),$$

namely, if $\gamma(u) = u^3 - \gamma_2 u + \gamma_3$, then $4\iota(\gamma)$ gives an elliptic curve defined by $y^2 = 4x^3 - 4\gamma_2 x - 4\gamma_3$. Then we obtain the commutative diagram

$$\begin{array}{ccc} (\mathbf{A}^4_u \setminus D)_0 & \xrightarrow{\mathfrak{M}} & M^{\omega}_{1,2}V \\ {\scriptstyle \mathcal{F}_0}\downarrow & & \downarrow{\scriptstyle \text{proj.}} \\ (\mathbf{A}^3_u \setminus D)_0 & \xrightarrow{4\iota} & M^{\omega}_{1,1} \end{array} \tag{5.4.1}$$

where the horizontal arrows give isomorphisms of schemes.

Since there is a well known deformation retraction of Tschirnhaus type between the spaces $\mathbf{A}^n \setminus D$ and $(\mathbf{A}^n_u \setminus D)_0$, their etale homotopy types do not need to be distinguished. We shall write "$\mathcal{F}$" to designate any one of the morphisms $\mathbf{A}^4_u \setminus D \to \mathbf{A}^3_u \setminus D$ which are parallel transforms of $\mathcal{F}_0$ (dropping the "zero sum" condition) giving the same homomorphism on fundamental groups.

On $\mathbf{A}^n_u \setminus D$, Ihara–Matsumoto [IM95] introduced a standard tangential base point $\bar{b}_n$. Let us briefly recall their construction: Let $\mathbf{A}^n_v \setminus \Delta$ be the affine n-space with distinct coordinates $v = (v_1, \ldots, v_n)$ and consider the etale covering map $(\mathbf{A}^n_v \setminus \Delta) \to (\mathbf{A}^n_u \setminus D)$ which maps each point $v \in \mathbf{A}^n_v \setminus \Delta$ to the monic in $\mathbf{A}^n_u \setminus D$ which has v as ordered zeros. Then $\bar{b}_n$ is defined as the image of the tangential base point $v = (0, t^{n-1}, \ldots, t^2, t)$ valued in $\overline{\mathbb{Q}}\{\{t\}\}$. The geometric fundamental group $\pi_1((\mathbf{A}^n \setminus D) \otimes \overline{\mathbb{Q}}, \bar{b}_n)$ can then be presented as the profinite completion of the Artin braid group B_n which has standard generators $\tau_1, \ldots, \tau_{n-1}$ with braid relations $\tau_i\tau_j = \tau_j\tau_i$, $\tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}$ $(i = 1, \ldots, n-1,\ i+1 < j)$, and each τ_i gives a specific element "interchanging marked points v_i and v_j positively". The base point $\bar{b}_n$ supplies a splitting $\pi_1(\mathbf{A}^n_u \setminus D, \bar{b}_n) = G_{\mathbb{Q}} \ltimes \hat{B}_n$ with Galois action in the form of Drinfeld's formula in terms of $(\chi(\sigma), \mathfrak{f}_\sigma) \in \widehat{GT}$ for $\sigma \in G_{\mathbb{Q}}$:

$$\begin{cases} \sigma(\tau_1) = \tau_1^{\chi(\sigma)}, \\ \sigma(\tau_2) = \mathfrak{f}_\sigma(\tau_1^2, \tau_2^2)^{-1}\tau_2^{\chi(\sigma)}\mathfrak{f}_\sigma(\tau_1^2, \tau_2^2), \\ \sigma(\tau_i) = \mathfrak{f}_\sigma(\omega_i, \tau_i^2)^{-1}\tau_i^{\chi(\sigma)}\mathfrak{f}_\sigma(\omega_i, \tau_i^2) \quad (i \geq 3), \end{cases} \tag{5.4.2}$$

where $\omega_i = (\tau_1 \cdots \tau_{i-1})^i$.

NB. The construction of $\bar{b}_n$ and the above formula have been generalized to higher genus mapping class groups first in [N97], and then extended fully in [NS00], [N99-02].

Dropping the (superfluous) "zero sum" condition, we calculate the image of $\bar{b}_4$ represented under $(0, t^3, t^2, t)$ by the Ferrari morphism as $(S_1, S_2, S_3) = (-t^4-t^3, -t^5-t^3, -t^4-t^5)$, which is equivalent to $(0, t^4-t^5, t^3-t^5) \sim (0, t^4, t^3) \sim \bar{b}_3$. Here, $\sim$ means "preserving principal coefficients", which does not alter coefficientwise $G_{\mathbb{Q}}$-actions on Puiseux power series; we may identify the tangential base points $\mathcal{F}(\bar{b}_4)$ and $\bar{b}_3$ (written $\mathcal{F}(\bar{b}_4) \approx \bar{b}_3$) from the Galois-theoretic point of view (cf. [N99-02, Part II, §5.9]). Thus we obtain a $G_{\mathbb{Q}}$-compatible homomorphism

$$\pi_1(\mathcal{F}) : \pi_1(\mathbf{A}^4_u \setminus D, \bar{b}_4) \to \pi_1(\mathbf{A}^3_u \setminus D, \bar{b}_3) \tag{5.4.3}$$

as remarked in [NTY10, (2.8)]. It is easy to see that the geometric part of this homomorphism is nothing but the surjection $\hat{B}_4 \to \hat{B}_3$ given by $\tau_1, \tau_3 \mapsto \tau_1$, $\tau_2 \mapsto \tau_2$. We call $\ker(\pi_1(\mathcal{F}))$ the *Ferrari kernel*, which is a free profinite group of rank 2 generated by

$$\begin{aligned} \mathbf{x}_1 &:= \tau_1^{-1}\tau_3\tau_2\tau_1\tau_3^{-1}\tau_2^{-1}, \\ \mathbf{x}_2 &:= \tau_1\tau_3^{-1}, \\ \mathbf{z} &:= (\tau_1\tau_2)^6(\tau_1\tau_2\tau_3)^{-4} \end{aligned} \tag{5.4.4}$$

with $[\mathbf{x}_1, \mathbf{x}_2]\mathbf{z} = 1$. We will see that these generators correspond naturally to the standard generators of the fundamental group of the Tate elliptic curve over $\mathbb{Q}((q))$ given in Theorem 5.2.4.

NB. The above choice of generators follows [N99] and differs from [NTY10, (2.9)], [NT03-06, II, (4.2.2)], [N99-02, I, §4] by a '90°-rotation'.

§5.5. Analytic resolution of $\mathfrak{M}^{-1}(E, P)$

In this subsection, we shall construct the solutions of the quartic equation of the inverse Mordell transformation $\mathfrak{M}^{-1}(E, P)$ explicitly in any complex model. Suppose that E is a complex elliptic curve $\mathbb{C}/(\mathbb{Z}\varpi_1 + \mathbb{Z}\varpi_2)$ and P is a point $(\wp(z), \wp'(z))$, where $\wp$ is the Weierstrass $\wp$-function with respect to the lattice $\mathbb{Z}\varpi_1 + \mathbb{Z}\varpi_2$ with $\tau := \varpi_1/\varpi_2 \in \mathfrak{H}$. Set $e_1 := \wp(\varpi_1/2)$, $e_2 := \wp(\varpi_2/2)$ and $e_3 := \wp((\varpi_1 + \varpi_2)/2)$. It is known that there is a canonical choice of square root of $e_2 - e_1$ given by

$$\sqrt{e_2 - e_1} = \frac{\pi}{\varpi_2} \prod_{n=1}^{\infty} (1 - q^{2n})^2 (1 + q^{2n-1})^4 \quad (q = q_\tau^{1/2} = e^{\pi i \tau}). \tag{5.5.1}$$

See [Fr16, p. 406]. Let $\mathrm{sn}(z)$, $\mathrm{cn}(z)$, $\mathrm{dn}(z)$ denote the Jacobian elliptic functions with fundamental parallelogram given by $2K = \varpi_2\sqrt{e_2-e_1}$, $2iK' = \varpi_1\sqrt{e_2-e_1}$.

Proposition 5.5.2. *Notations being as above, set $w = \sqrt{e_2-e_1}\cdot z$. Then the four zeros of the quartic given as the inverse Mordell transformation $\mathfrak{M}^{-1}(E,P)$ are:*

$$T_1 = \frac{\sqrt{e_2-e_1}}{2}\left(\frac{1+\mathrm{cn}(w)+\mathrm{dn}(w)}{\mathrm{sn}(w)}\right),$$
$$T_2 = \frac{\sqrt{e_2-e_1}}{2}\left(\frac{\mathrm{cn}(w)-1-\mathrm{dn}(w)}{\mathrm{sn}(w)}\right),$$
$$T_3 = \frac{\sqrt{e_2-e_1}}{2}\left(\frac{\mathrm{dn}(w)-1-\mathrm{cn}(w)}{\mathrm{sn}(w)}\right),$$
$$T_4 = \frac{\sqrt{e_2-e_1}}{2}\left(\frac{1-\mathrm{cn}(w)-\mathrm{dn}(w)}{\mathrm{sn}(w)}\right).$$

Proof. We make use of the "Mordell–Ferrari" commutative diagram (5.4.1). Tracing the lower layer, we find that the Ferrari resolvents of the quartic $\mathfrak{M}^{-1}(E,P)$ should be given by $\iota^{-1}(E) = \{-e_1,-e_2,-e_3\}$. Then, if $\mathfrak{M}^{-1}(E,P)$ is of the form u^4+bu^2+cu+d, the classical formula of Cardano–Ferrari tells us that the resulting four solutions are obtained as $\frac{1}{2}(\sqrt{S_1}+\sqrt{S_2}+\sqrt{S_3})$ for any choice of square roots of $S_i := -e_i - \frac{2}{3}b$ $(i=1,2,3)$ such that $\sqrt{S_1}\sqrt{S_2}\sqrt{S_3} = -c$. But now $b = -\frac{3}{2}\wp(z)$ and $c = \frac{1}{2}\wp'(z)$, and hence $S_i = \wp(z) - e_i$ $(i=1,2,3)$. On the other hand, it is also known (from [Fr16, p. 389]) for $w = \sqrt{e_2-e_1}z$ that

$$\mathrm{sn}(w) = \frac{\sqrt{e_2-e_1}}{\sqrt{\wp(z)-e_1}}, \qquad \mathrm{cn}(w) = \frac{\sqrt{\wp(z)-e_2}}{\sqrt{\wp(z)-e_1}}, \qquad \mathrm{dn}(w) = \frac{\sqrt{\wp(z)-e_3}}{\sqrt{\wp(z)-e_1}},$$

from which it turns out that they give a correct choice of $\sqrt{S_i} = \sqrt{\wp(z)-e_i}$'s for Cardano–Ferrari solutions. Our proposition follows from these equations immediately after expressing the $\sqrt{S_i}$ by Jacobian elliptic functions and $\sqrt{e_2-e_1}$. □

§5.6. Connection between the Tate–Weierstrass point and $\bar{b}_4$

Let us fit the Tate elliptic curve $\mathrm{Tate}(q)/\mathbb{Q}((q))$ in $M^{\omega}_{1,2} \to M^{\omega}_{1,1}$ to obtain a pair of tangential points $(\overrightarrow{\mathfrak{w}}_{\bar{q}}, \bar{q})$ on $(M^{\omega}_{1,2}, M^{\omega}_{1,1})$ respectively. We shall connect the inverse Mordell transformation of $\overrightarrow{\mathfrak{w}}_{\bar{q}}$ to the standard base point $\bar{b}_4$ on $\mathbf{A}^4_u \setminus D$ by using Proposition 5.5.2. Observe that the defining coefficients $g_2(q)$, $g_3(q)$ of $\mathrm{Tate}(q)$ in (5.2.1)–(5.2.2) are those $g_2(\varpi_1,\varpi_2)$, $g_3(\varpi_1,\varpi_2)$ applied to the lattice generated by $\varpi_1 = (2\pi i)\tau$, $\varpi_2 = (2\pi i)$. In this case, $\sqrt{e_2-e_1} = \frac{1}{2i} + O(q)$. We look at the point (T_4,T_3,T_2,T_1) of Proposition 5.5.2 on $\mathbf{A}^4_v \setminus \Delta$, which, by parallel

transportation, gives an equivalent tangential base point defined by

$$(0, T_3 - T_4, T_2 - T_4, T_1 - T_4)$$
$$= \frac{\sqrt{e_2 - e_1}}{2}\left(0, \frac{2(\mathrm{dn}(w) - 1)}{\mathrm{sn}(w)}, \frac{2(\mathrm{cn}(w) - 1)}{\mathrm{sn}(w)}, \frac{2(\mathrm{cn}(w) + \mathrm{dn}(w))}{\mathrm{sn}(w)}\right).$$

Recalling that the Weierstrass tangential base point (in the analytic case) is defined by the local coordinate $t = -2x/y = -2\wp(z)/\wp'(z) = z + O(z^2)$, we shall evaluate the inverse image of the tangential base point $\mathfrak{M}^{-1}(\overrightarrow{\mathfrak{w}}_{\bar{q}})$ on $\mathbf{A}^4_v \setminus \Delta$, by expanding the above coordinates near $(q, t) = (0, 0)$. Indeed, the well known Taylor expansions (cf. [Fr16, p. 399])

$$\mathrm{sn}(w) = w - (1 + k^2)\frac{w^3}{3!} + \cdots, \qquad \mathrm{cn}(w) = 1 - \frac{w^2}{2} + \cdots,$$
$$\mathrm{dn}(w) = 1 - k^2\frac{w^2}{2} + \cdots$$

with

$$k^2 = \lambda = 16q\prod_{n=1}^{\infty}\left(\frac{1 + q^{2n}}{1 + q^{2n-1}}\right)^8 \qquad (q = q_\tau^{1/2} = e^{\pi i \tau}) \tag{5.6.1}$$

provide the principal terms of the components of $(0, T_3 - T_4, T_2 - T_4, T_1 - T_4)$ above as Laurent series in 'k, z' or 'q, t' (denoted $\sim$):

$$(0, T_3 - T_4, T_2 - T_4, T_1 - T_4) \sim \left(0, \frac{k^2 z}{8}, \frac{z}{8}, \frac{2}{z}\right) \sim \left(0, 2tq, \frac{t}{8}, \frac{2}{t}\right).$$

Now, the tangential base point $\bar{b}_4$ can be defined by the following homomorphism of the coordinate ring of $\mathbf{A}^4_v - \Delta$ into a Puiseux ring:

$$\mathbb{Q}[v_1, v_2, v_3, v_4]\left[\frac{1}{v_i - v_j}\right]_{1 \le i \ne j \le 4} \to \bigcup_{k=1}^{\infty} \overline{\mathbb{Q}}[[t_1^{1/k}, t_2^{1/k}, t_3^{1/k}]]\left[\frac{1}{t_1}, \frac{1}{t_2}, \frac{1}{t_3}\right]$$

where $t_1, t_2 \in \mathbf{A}^1 - \{0, 1\}$ and $t_3 \in \mathbf{A}^1 - \{0\}$ are the Ihara–Matsumoto coordinates (cf. [IM95]) introduced by $(v_2 - v_1, v_3 - v_1, v_4 - v_1) = (t_1 t_2 t_3, t_2 t_3, t_3)$. To connect $\bar{b}_4$ to $\mathfrak{M}^{-1}(\overrightarrow{\mathfrak{w}}_{\bar{q}})$, factorize the above homomorphism through an intermediate ring

$$\tilde{R} := \left(\bigcup_{k=1}^{\infty} \overline{\mathbb{Q}}[[t_1^{1/k}, t_2^{1/k}]]\left[\frac{1}{t_1}, \frac{1}{t_2}\right]\right)\left[t_3, \frac{1}{t_3}\right],$$

and put

$$(0, t_1 t_2 t_3, t_2 t_3, t_3) := (0, T_3 - T_4, T_2 - T_4, T_1 - T_4) \sim \left(0, 2tq, \frac{t}{8}, \frac{2}{t}\right) \tag{5.6.2}$$

so that $t_1 \sim 16q$, $t_2 \sim \frac{t^2}{16}$, $t_3 \sim \frac{2}{t}$. The induced $(\bigcup_{k=1}^{\infty} \overline{\mathbb{Q}}[[t^{1/k}, q^{1/k}]][1/t, 1/q])$-valued point on $\mathrm{Spec}(\tilde{R})$ defines (a lift of) the tangential base point $\mathfrak{M}^{-1}(\overrightarrow{\mathfrak{w}}_{\bar{q}})$. Arriving at this stage, one can now introduce a triple of natural paths $\varepsilon_1 : \overrightarrow{01}_{t_1} \rightsquigarrow \frac{1}{16}\overrightarrow{01}_{t_1} = \overrightarrow{01}_q$, $\varepsilon_2 : \overrightarrow{01}_{t_2} \rightsquigarrow 16 \cdot \overrightarrow{01}_{t_2} = \overrightarrow{01}_{t^2}$, and $\varepsilon_3 : \overrightarrow{01}_{t_3} \rightsquigarrow \frac{1}{2}\overrightarrow{01}_{t_3} = \overrightarrow{\infty 1}_t \rightsquigarrow \overrightarrow{01}_t$ on $\mathrm{Spec}(\tilde{R})$ along the positive power roots of 2 (and of 16). (Note here that ε_1, ε_2 are infinitesimal paths near 0 on $\mathbf{A}^1 - \{0, 1\}$ while ε_3 is a global path on $\mathbf{A}^1 - \{0\}$.) Then, taking the projection image of $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$, we obtain a path $\varepsilon : \bar{b}_4 \rightsquigarrow \mathfrak{M}^{-1}(\overrightarrow{\mathfrak{w}}_{\bar{q}})$ on $\mathbf{A}^4_u \setminus D$. By construction, we have

$$\text{(5.6.3)} \qquad \begin{cases} \sigma(\varepsilon_1) = (\tau_1^2)^{4\rho_2(\sigma)} \cdot \varepsilon_1, \\ \sigma(\varepsilon_2) = ((\tau_1\tau_2)^3)^{-4\rho_2(\sigma)} \cdot \varepsilon_2, \\ \sigma(\varepsilon_3) = ((\tau_1\tau_2\tau_3)^4)^{\rho_2(\sigma)} \cdot \varepsilon_3 \end{cases}$$

for $\sigma \in G_{\mathbb{Q}}$, where $\rho_2 : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}$ is the Kummer 1-cocycle defined by $\zeta_n^{\rho_2(\sigma)} = \sigma(\sqrt[n]{2})/\sqrt[n]{2}$ $(n \geq 1)$.

Let us also calculate the image $\mathcal{F}(\mathfrak{M}^{-1}(\overrightarrow{\mathfrak{w}}_{\bar{q}}))$ on $\mathbf{A}^3_u \setminus D$. Using the above (5.6.2), one obtains a triple of Ferrari resolvents (S_1, S_2, S_3) on $\mathbf{A}^3_v \setminus \Delta$ having lower degree terms in t, q as $(S_1, S_2, S_3) = (-1/4 - 4q + \cdots, -1/4 - t^2q/4 + \cdots, -4q - t^2q/4 + \cdots)$. By parallel transportation, its Ihara–Matsumoto coordinates s_1, s_2 can be characterized by

$$\text{(5.6.4)} \qquad (0, s_1s_2, s_2) := (0, S_2 - S_1, S_3 - S_1) \sim (0, 4q, 1/4)$$

so that $s_1 \sim 16q$, $s_2 \sim 1/4$, where $\sim$ indicates principal terms as Laurent series in 'q, t'. We observe that the image $\mathcal{F}(\varepsilon)$ looks like an infinitesimal segment path

$$\overrightarrow{01}_{s_1} (= 16 \cdot \overrightarrow{01}_q) \rightsquigarrow \frac{1}{16}\overrightarrow{01}_{s_1} (= \overrightarrow{01}_q)$$

on the s_1-line. The appearance of $\frac{1}{16}$ in this manner in Grothendieck–Teichmüller theory has been observed first in [N99-02, §4.10], and this feature has continuously appeared in our works [N97], [NS00] etc.

§5.7. Standard splittings of $\pi_1(M^{\omega}_{1,2})$

Below, we shall switch our working place to the $M^{\omega}_{1,2}$-side of the Mordell transformation (5.4.1). We denote by the same symbols the images of the base point $\bar{b}_4$ and of the above path ε on $\mathbf{A}^4_u \setminus D$ on $M^{\omega}_{1,2}$ under $\mathfrak{M}$. Let $\beta_1(\sigma) \in \pi_1(M^{\omega}_{1,2}, \bar{b}_4)$, $\mathfrak{s}_1(\sigma) \in \pi_1(M^{\omega}_{1,2}, \overrightarrow{\mathfrak{w}}_{\bar{q}})$ denote the elements corresponding to $\sigma \in G_{\mathbb{Q}}$. Also we represent the images under $\mathfrak{M}$ of generator elements of $\hat{B}_4$ by the same symbols, which are in the first sense loops based at $\bar{b}_4$ but may also be regarded as loops based at $\overrightarrow{\mathfrak{w}}_{\bar{q}}$ by conjugation by ε. Under this abuse of notation, we may rephrase

the above formula (5.6.3) as

$$\begin{aligned}(5.7.1)\qquad \beta_1(\sigma)\,\varepsilon\,\mathfrak{s}_1(\sigma)^{-1} &= \varepsilon\cdot(\tau_1^2)^{4\rho_2(\sigma)}((\tau_1\tau_2)^3)^{-4\rho_2(\sigma)}((\tau_1\tau_2\tau_3)^4)^{\rho_2(\sigma)}\\ &= (\tau_1^2)^{4\rho_2(\sigma)}((\tau_1\tau_2)^3)^{-4\rho_2(\sigma)}((\tau_1\tau_2\tau_3)^4)^{\rho_2(\sigma)}\cdot\varepsilon.\end{aligned}$$

Drawing back Drinfeld's formula (5.4.2) by ε, we obtain Galois actions on τ_1,τ_2,τ_3 at the Tate–Weierstrass base point $\overrightarrow{\mathfrak{w}}_{\bar q}$ as follows:

$$(5.7.2)\qquad \begin{cases}\mathfrak{s}_1(\sigma)\,\tau_1\,\mathfrak{s}_1(\sigma)^{-1} = \tau_1^{\chi(\sigma)},\\ \mathfrak{s}_1(\sigma)\,\tau_2\,\mathfrak{s}_1(\sigma)^{-1} = \omega_2^{-4\rho_2(\sigma)}\mathfrak{f}_\sigma(\tau_1^2,\tau_2^2)^{-1}\tau_2^{\chi(\sigma)}\mathfrak{f}_\sigma(\tau_1^2,\tau_2^2)\omega_2^{4\rho_2(\sigma)},\\ \mathfrak{s}_1(\sigma)\,\tau_3\,\mathfrak{s}_1(\sigma)^{-1} = \omega_3^{4\rho_2(\sigma)}\mathfrak{f}_\sigma(\omega_3,\tau_3^2)^{-1}\tau_3^{\chi(\sigma)}\mathfrak{f}_\sigma(\omega_3,\tau_3^2)\omega_3^{-4\rho_2(\sigma)},\end{cases}$$

where $\omega_2=\tau_1^2$, $\omega_3=(\tau_1\tau_2)^3$.

Next we shall look at the kernel of the projection $\pi_1(M^\omega_{1,2},\overrightarrow{\mathfrak{w}}_{\bar q})\to\pi_1(M^\omega_{1,1},\bar q)$ which is identified with the Ferrari kernel $\ker(\pi_1(\mathcal{F}))$ (5.4.3). In [N99-02, §4], we considered $\pi_1(M_{1,2})=\pi_1(M^\omega_{1,2})/\langle\omega_4\rangle$ as the topological mapping class group of a torus with two marked points. The images of τ_1,τ_2,τ_3 were then understood to be the Dehn twists along certain simple closed curves on it. From this discussion, one could introduce generators $\mathbf{x}_1,\mathbf{x}_2,\mathbf{z}$ given by combination of Dehn twists as in (5.4.4). Since the Ferrari kernel has isomorphic image in $\pi_1(M_{1,2})$, we see that the $G_{\mathbb{Q}}$-action on these generators $\mathbf{x}_1,\mathbf{x}_2,\mathbf{z}$ of $\pi_1(\mathrm{Tate}(q)\setminus\{O\})$ in Theorem 5.2.4 exactly gives the $G_{\mathbb{Q}}$-action on the Ferrari kernel even in $\pi_1(M^\omega_{1,2},\overrightarrow{\mathfrak{w}}_{\bar q})$.

At this stage, it is probably appropriate to show how the above formula (5.7.2) can consistently imply a key formula of Theorem 5.2.4, namely, the fact that $\mathfrak{s}_1(\sigma)$ acts on $\mathbf{x}_2$ by conjugation in the following form:

$$(*)\qquad \mathbf{x}_2\mapsto\mathfrak{f}_\sigma(\mathbf{x}_2^{-1},\mathbf{z})\mathbf{x}_2^{\chi(\sigma)}\mathfrak{f}_\sigma(\mathbf{x}_2^{-1},\mathbf{z})^{-1}.$$

In fact, our substantial ingredient for connecting (5.7.2) to $(*)$ is what is called "relation (IV)" satisfied by the image of $G_{\mathbb{Q}}\hookrightarrow\widehat{GT}$, which was found in [N99-02, Theorem 4.16]. It (equivalently) implies (cf. also [NS00, p. 543]) the equation

$$\text{(IV)}\qquad \mathfrak{f}_\sigma(\tau_3^2,\omega_3)=\omega_3^{-4\rho_2(\sigma)}\mathfrak{f}_\sigma(\tau_3,\omega_3^2)(\tau_3\omega_3)^{4\rho_2(\sigma)}\tau_3^{-4\rho_2(\sigma)}\qquad(\sigma\in G_{\mathbb{Q}}).$$

Proof that (5.7.2) *and* (IV) *imply* $(*)$. As $\mathbf{x}_2=\tau_1\tau_3^{-1}$, one easily sees from (5.7.2) that the conjugate action by $\mathfrak{s}_1(\sigma)$ gives the mapping

$$\mathbf{x}_2\mapsto\omega_3^{4\rho_2(\sigma)}\mathfrak{f}_\sigma(\tau_3^2,\omega_3)\mathbf{x}_2^{\chi(\sigma)}\mathfrak{f}_\sigma(\tau_3^2,\omega_3)^{-1}\omega_3^{-4\rho_2(\sigma)}.$$

Applying relation (IV) here and noting that τ_3, ω_3 commute with $\mathbf{x}_2$, the above expression is equivalent to

$$\mathbf{x}_2\mapsto\mathfrak{f}_\sigma(\tau_3,\omega_3^2)\mathbf{x}_2^{\chi(\sigma)}\mathfrak{f}_\sigma(\tau_3,\omega_3^2)^{-1}.$$

Since $\mathfrak{f}_\sigma$ is in $[\hat{F}_2, \hat{F}_2]$, and since the pair $\{\tau_1, \omega_4 = (\tau_1\tau_2\tau_3)^4\}$ elementwise commutes with the pair $\{\tau_3 = \mathbf{x}_2^{-1}\tau_1, \omega_3^2 = \mathbf{z}\omega_4\}$, it follows that $\mathfrak{f}_\sigma(\tau_3, \omega_3^2) = \mathfrak{f}_\sigma(\mathbf{x}_2^{-1}, \mathbf{z})$. Thus, we conclude that the above $(*)$ is derived from (5.7.2) and (IV). □

Before closing this subsection, we give a statement on how the Weierstrass tangential section (§2.4) gives a complement of the Ferrari kernel, i.e., a splitting of $\pi_1(M^\omega_{1,2}, \overrightarrow{\mathfrak{w}}_{\bar{q}})$ with it:

Proposition 5.7.3. *The image of the Weierstrass section*

$$s_{\overrightarrow{\mathfrak{w}}} : \pi_1(M^\omega_{1,1}, \bar{q}) \to \pi_1(M^\omega_{1,2}, \overrightarrow{\mathfrak{w}}_{\bar{q}})$$

coincides with the subgroup $\langle \tau_1, \tau_2 \rangle \rtimes \mathfrak{s}_1(G_{\mathbb{Q}})$ *so that* $s_{\overrightarrow{\mathfrak{w}}}(\tau_i) = \tau_i$ $(i = 1, 2)$. *Consequently, the conjugate action on the Ferrari kernel* $\ker(\pi_1(\mathcal{F})) = \langle \mathbf{x}_1, \mathbf{x}_2 \rangle$ *via* $s_{\overrightarrow{\mathfrak{w}}}$ *of each split component of* $\pi_1(M^\omega_{1,1}, \bar{q}) = \hat{B}_3 \rtimes \mathfrak{s}_0(G_{\mathbb{Q}})$ *at* $\bar{q}$ *is given by*

$$\mathrm{Int}(\mathfrak{s}_{\overrightarrow{\mathfrak{w}}}(\tau_1)) : \begin{cases} \mathbf{x}_1 \mapsto \mathbf{x}_1\mathbf{x}_2^{-1}, \\ \mathbf{x}_2 \mapsto \mathbf{x}_2, \end{cases} \qquad \mathrm{Int}(\mathfrak{s}_{\overrightarrow{\mathfrak{w}}}(\tau_2)) : \begin{cases} \mathbf{x}_1 \mapsto \mathbf{x}_1, \\ \mathbf{x}_2 \mapsto \mathbf{x}_2\mathbf{x}_1, \end{cases}$$

on $\hat{B}_3$ *and by Theorem* 5.2.4 *on* $\mathfrak{s}_0(G_{\mathbb{Q}})$.

We will give the proof of this proposition at the end of §6.

§5.8. Lifting modular forms

As observed in §2.2, the moduli space $M^\omega_{1,1}$ and the universal elliptic curve $M^\omega_{1,2}$ over it are themselves affine schemes. Let $\mathcal{O}^\omega_{1,1}$ denote the former structure ring $\mathbb{Q}[g_2, g_3, (g_2^3 - 27g_3^2)^{-1}]$, and let $\mathcal{O}^\omega_{1,2}$ denote the latter structure ring which can be written as $\mathcal{O}^\omega_{1,1}[x, y]/(4x^3 - g_2x - g_3 - y^2)$. We shall fix a maximal pro-etale cover (i.e., universal cover) $\widetilde{M^\omega_{1,2}} = \mathrm{Spec}(\widetilde{\mathcal{O}^\omega_{1,2}})$ of $M^\omega_{1,2}$, and a base point $\tilde{\mathfrak{w}}_{\bar{q}}$ on it that lifts $\overrightarrow{\mathfrak{w}}_{\bar{q}}$. Note that this determines, at the same time, the universal cover $\widetilde{M^\omega_{1,1}} = \mathrm{Spec}(\widetilde{\mathcal{O}^\omega_{1,1}})$ of $M^\omega_{1,1}$ together with its base point $\tilde{q}$ as the pointed subobject under $(\widetilde{M^\omega_{1,2}}, \tilde{\mathfrak{w}}_{\bar{q}})$. For any pointed Galois etale covers $f : (Y, \bar{y}) \to (X, \bar{x})$ dominated by $(\widetilde{M^\omega_{1,2}}, \tilde{\mathfrak{w}}_{\bar{q}})$, we shall write $\mathfrak{a}_{Y/X} : \pi_1(X, \bar{x}) \to \mathrm{Aut}(Y/X)$ for the natural surjective anti-homomorphism determined by $\mathfrak{a}_{Y/X}(\sigma)(\bar{y}) = \sigma(\bar{y})$.

In §5.1, we selected a system of (an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and) standard generators $\mathbf{x}_1, \mathbf{x}_2, \mathbf{z}$ of $\pi_1(\mathrm{Tate}(q)_{\bar{q}} \setminus \{O\}, \bar{q})$ which determines the matrix representation $\rho^N : \pi_1(M^\omega_{1,1}, \bar{q}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

As in §2.6, we obtain a system of etale coverings $M^\omega_{1,1}[N] \to M^\omega_{1,1}$ which corresponds to the kernels of ρ^N $(N \geq 1)$. Also we pick a system of base points $\bar{q}^N$ on $M^\omega_{1,1}[N]$ in multiplicatively compatible way with respect to $N \geq 1$. Regard then the associated $\Gamma(N)$-test object $(E^N/\mathcal{O}^{\omega}_{1,1}{}^N, \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E^N[N], \omega_N)$

with the pair of base points $(\overrightarrow{\mathfrak{w}}_{\bar{q}^N}, \bar{q}^N)$ as a pointed subobject of $(\widetilde{M^{\omega}_{1,2}}, \tilde{\mathfrak{w}}_{\bar{q}})$, so that the structure rings of both E^N and $\mathcal{O}^{\omega}_{1,1}{}^N$ become subrings of $\widetilde{\mathcal{O}^{\omega}_{1,2}}$ and of $\widetilde{\mathcal{O}^{\omega}_{1,1}}$ respectively. Note also that the Weil pairing gives a compatible system of primitive roots of unity $\{\zeta_N\}$ in $\widetilde{\mathcal{O}^{\omega}_{1,1}}$. It turns out that $\zeta_N = \exp(2\pi i/N)$ under our choice of $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$.

Now, we see how modular units, eta-function and Eisenstein series introduced in §4 can be lifted to certain elements of $\widetilde{\mathcal{O}^{\omega}_{1,1}}$. In fact, by Proposition 4.2.1, the Siegel function g_x ($x \in (\frac{1}{N}\mathbb{Z}/\mathbb{Z})^2$) is a modular function of level $\Gamma(12N^2)$ with $q^{1/N}$-expansion with coefficients in $\mathbb{Q}(\mu_{2N^2})$. By Proposition 4.2.3, the square η^2 of the eta function is a modular form of weight 1 and level $\Gamma(12)$ which has $\mathbb{Q}$-rational $q^{1/12}$-expansion. By (4.3.2), the Eisenstein series $E_k^{(\mathbf{x})}$ ($\mathbf{x} \in (\frac{1}{N}\mathbb{Z}/\mathbb{Z})^2$) for $k \geq 3$ or $\mathbf{x} \neq 0$ is a modular form of weight k of level $\Gamma(N)$ with $q^{1/N}$-expansion with coefficients in $\mathbb{Q}(\mu_N)$. Thus, forming algebraic modular forms corresponding to them over suitably large cyclotomic fields ($\subset \mathbb{C}$) (§4.4), we obtain their values at $(E^N/\mathcal{O}^{\omega}_{1,1}{}^N, \alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E^N[N], \omega_N)$ in $\widetilde{\mathcal{O}^{\omega}_{1,1}}$. Note that an algebraic form of level N may also be of level MN, which, however, still gives the same element in $\widetilde{\mathcal{O}^{\omega}_{1,1}}$. We shall use the same symbols as modular forms to designate the corresponding elements in $\widetilde{\mathcal{O}^{\omega}_{1,1}}$. For example, we have $\Delta = (\eta^2)^{12}$, $\theta_x = g_x^{12}$ as elements of $\widetilde{\mathcal{O}^{\omega}_{1,1}}$. Moreover, their $q^{1/N}$-expansions can be recovered as the values at the Tate tangential base point, i.e., as the Puiseux power series images under $\widetilde{\mathcal{O}^{\omega}_{1,1}} \to \Omega \subset \overline{\mathbb{Q}}\{\{q\}\}$ at $\bar{q}$.

§5.9. Kummer characters, power roots of Δ

Monodromy characters along power roots of various fundamental quantities play important roles in our study. Besides the cyclotomic character $\chi : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^{\times}$ coming from the roots of unity, the most basic character is the Kummer character (1-cocycle)

$$\rho_a : G_{\mathbb{Q}} \to \hat{\mathbb{Z}} = \hat{\mathbb{Z}}(1)$$

for a positive rational number a, which is defined with the positive power roots $\sqrt[n]{a}$ ($n \geq 1$) by

$$\zeta_n^{\rho_a(\sigma)} = \sigma(\sqrt[n]{a})/\sqrt[n]{a} \quad (n \geq 1,\ \sigma \in G_{\mathbb{Q}}).$$

Note that although the cyclotomic character $\chi : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^{\times}$ does not depend on the choice of either $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ or primitive n-th roots of unity ζ_n, the Kummer character $\rho_a : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}$ does depend on either choice specified by the properties $\sqrt[n]{a} \in \mathbb{R} \cap \overline{\mathbb{Q}}$ and $\zeta_n = \exp(2\pi i/n)$ ($n \geq 1$). As obvious extension of notations, for any algebraic variety $S = \mathrm{Spec}(B)$ with base point $\bar{b} : \mathrm{Spec}(\Omega) \to S$ (given by $\mathbb{Q} \subset B \to \Omega$), we shall write

$$\chi : \pi_1(S, \bar{b}) \to \hat{\mathbb{Z}}^{\times}, \quad \chi_a : \pi_1(S, \bar{b}) \to \hat{\mathbb{Z}}$$

to designate the composition of the natural projection $\pi_1(S,\bar{b}) \to G_{\mathbb{Q}}$ with the above χ, ρ_a $(a \in \mathbb{Q}_{>0})$ respectively.

Next, we shall introduce a standard monodromy character along power roots of the modular function Δ. Since η^2 is a unit of $\widetilde{\mathcal{O}^{\omega}_{1,1}}$, its power roots $(\eta^2)^{1/N}$ also lie in $\widetilde{\mathcal{O}^{\omega}_{1,1}}$. The choice of their branches can be determined by specifying their images in $\overline{\mathbb{Q}}\{\{q\}\}$, or more simply by specifying the principal coefficients as Puiseux power series in q. Since $\eta^2 = q^{1/12}\prod(1-q^n)^2$, we simply set $(\eta^2)^{1/N}$ to have leading term $q^{1/12N}$. Put also $\Delta^{1/N} := ((\eta^2)^{1/N})^{12}$.

The Kummer character

$$\rho_{\Delta} : \pi_1(M^{\omega}_{1,1},\bar{q}) \to \hat{\mathbb{Z}}$$

is defined by

$$\frac{\Delta^{1/N}|_{\mathfrak{a}_\sigma}}{\Delta^{1/N}} = \zeta_N^{\rho_\Delta(\sigma)} \qquad (N \geq 1,\ \sigma \in \pi_1(M^{\omega}_{1,1},\bar{q})).$$

The following gives a complete description of ρ_Δ:

Lemma 5.9.1. *Let $\pi_1(M_{1,1},\bar{q}) = \mathfrak{s}_0(G_{\mathbb{Q}}) \ltimes \hat{B}_3$ be the standard splitting of the fundamental group of $M^{\omega}_{1,1}$ at the Tate tangential base point $\bar{q}$. On $\mathfrak{s}_0(G_{\mathbb{Q}})$, ρ_Δ vanishes. On $\hat{B}_3$, ρ_Δ is determined by $\rho_\Delta(\tau_1) = \rho_\Delta(\tau_2) = -1$. Consequently,*

$$\rho_{\Delta} : \pi_1(M^{\omega}_{1,1},\bar{q}) \to \hat{\mathbb{Z}} \qquad (\tau_1,\tau_2 \mapsto -1,\ \mathfrak{s}_0(\sigma) \mapsto 0\ (\sigma \in G_{\mathbb{Q}})).$$

Proof. The action from $\mathfrak{s}_0(G_{\mathbb{Q}})$ is defined by coefficientwise Galois action on the Puiseux series in q. Our choice is given by setting the principal coefficient to be 1, so ρ_Δ vanishes. On the discrete geometric fundamental group B_3, we interpret ρ_Δ as the winding number of the function $\Delta = g_2^3 - 27g_3^2 = 16(e_1-e_2)^2(e_1-e_3)^2(e_2-e_3)^2$ along the motion of three points e_1,e_2,e_3 according to braids. The minus sign comes from our convention of path composition. □

§5.10. Power roots of Siegel units

For g_x $(x = (r_1/m, r_2/m))$, recall that the principal term of the $q^{1/12m^2}$-expansion reads by definition (see §4.2)

$$\begin{cases} -e^{\pi i x_2(x_1-1)} & (m \nmid r_1), \\ -e^{\pi i x_2(x_1-1)}(1-\zeta_m^{r_2}) & (m \mid r_1). \end{cases}$$

In view of this, to determine the standard N-th root of g_x (written $g_x^{1/N}$), it suffices to choose the standard N-th roots of those individual factors. Set

$$(-1)^{1/N} = \zeta_{2N}, \qquad (e^{\pi i x_2(x_1-1)})^{1/N} = \zeta_{2Nm^2}^{r_2(r_1-m)}$$

and let $(1-\zeta_m^{r_2})^{1/N}$ be the principal branch having the least argument as the complex number. Certainly, we shall define $g_x^{1/N}$ for particular $x=(r_1/m, r_2/m)$ with $(r_1,r_2)\in[0,m)^2-\{\mathbf{0}\}$ so that the principal coefficient of $q^{1/12m^2N}$ is $\zeta_{2N}\zeta_{2Nm^2}^{r_2(r_1-m)}$, multiplied by $(1-\zeta_m^{r_2})^{1/N}$ when $r_1=0$. However, for general $x\in\mathbb{Q}^2\setminus\mathbb{Z}^2$, we take a slightly more careful process via the real analytic continuity of g_x $(\neq 0)$ in $x\in\mathbb{R}^2\setminus\mathbb{Z}^2$: We consier the complex analytic model discussed in §2.9, where the universal elliptic curve with level m structure was given as a quotient of $\mathbb{C}\times\mathfrak{H}$ by $\mathbb{Z}^2\rtimes\Gamma(m)$. To specify $g_x^{1/N}$ it suffices to choose its image as an analytic function on the upper half-plane $\mathfrak{H}$. Observe now that the Siegel function g_x $(x\in\mathbb{R}^2)$ varies real analytically with respect to x, and is zero for $x\in\mathbb{Z}^2$ while non-zero for $x\in\mathbb{R}^2\setminus\mathbb{Z}^2$. For $x=(x_1,x_2)\in[0,1)^2$ $(x\neq 0)$, we define $g_x^{1/N}$ to be the root whose Fourier expansion at $i\infty$ has principal coefficient $e^{\pi i(1+x_2(x_1-1))/N}$, multiplied by $(1-e^{2\pi i x_2})^{1/N}$ when $x_1=0$. For general $(x_1,x_2)=(r_1/m,r_2/m)\in\mathbb{Q}^2\setminus\mathbb{Z}^2$, pick a sufficiently small real number $\varepsilon/m>0$, and trace the branch of $g_\xi^{1/N}$ from $\xi=(\varepsilon,\varepsilon)$ in the already considered region $[0,1)^2-\{0\}$ along the piecewise line path $\xi=(\varepsilon,\varepsilon)\to(\varepsilon,\varepsilon+x_2)\to(\varepsilon+x_1,\varepsilon+x_2)$, and then take the limit $\varepsilon\to 0$: the process may be summarized as

$$g_x^{1/N}:=\lim_{\varepsilon\to 0}\ \underset{t_1:0\rightsquigarrow 1}{\mathrm{Move}}\ \underset{t_2:0\rightsquigarrow 1}{\mathrm{Move}}\ \big(g_{\xi((x_1t_1,0)+(0,x_2t_2)+(\varepsilon,\varepsilon))}^{1/N}\big). \tag{5.10.1}$$

Since the path does not meet a lattice point in $\mathbb{Z}^2$, the real analytic continuity of g_x with respect to $x\in\mathbb{R}^2$ determines a well defined branch of $g_x^{1/N}$. Obviously, $g_x^{1/N}$ forms a power root system with respect to N, that is, $(g_x^{1/MN})^N=g_x^{1/M}$ for $M,N\in\mathbb{N}$. We also define $\theta_x^{1/N}:=(g_x^{1/N})^{12}$.

Before closing this section, we shall introduce certain Kummer type quantities. These will be crucial in our main Theorem A on approximating the $\mathbb{E}_m^{\mathcal{C}}(\sigma)$-invariant, which we will discuss in detail in the next section.

Definition 5.10.2. Let $\mathcal{C}$ be a full class of finite groups. Define

$$e_{\mathcal{C}}:=\prod_{l\,\text{prime}\in|\mathcal{C}|}e_l$$

where $e_l=1,3,4$ according as $l\geq 5$, $=3$, $=2$ respectively.

Let $\rho^{\mathcal{C}}:\pi_1(M_{1,1}^{\omega},\bar{q})\to\mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}})$ be the standard representation on the abelianization of $\Pi_{1,1}$, let $m\geq 1$ and pick any $\sigma\in\pi_1(M_{1,1}^{\omega},\bar{q})$.

Definition 5.10.3. If two pairs of rational integers $\mathbf{r}=(r_1,r_2)$, $\mathbf{s}=(s_1,s_2)\in\mathbb{Z}^2$ satisfy

$$\begin{pmatrix}s_1\\ s_2\end{pmatrix}\equiv\rho^{\mathcal{C}}(\sigma)\begin{pmatrix}r_1\\ r_2\end{pmatrix}\bmod m^2Me_{\mathcal{C}}$$

for some $M \in |\mathcal{C}|$, then the move of pairs

$$x = \left(\frac{r_1}{m}, \frac{r_2}{m}\right) \to y = \left(\frac{s_1}{m}, \frac{s_2}{m}\right) \in \left(\frac{1}{m}\mathbb{Z}\right)^2$$

is called $\rho^{\mathcal{C}}(\sigma)$-*admissible at level* m modulo m^2M. (Here $\rho^{\mathcal{C}}(\sigma)$ is considered as acting on $(\mathbb{Z}/(m^2Me_{\mathcal{C}})\mathbb{Z})^2$ through $\rho^{m^2Me_{\mathcal{C}}}$ (§2.6).)

Note that, in this case, as noted in (4.6.2), (4.6.7)-(4.6.8), $(g_x)^{c_l}|_{\mathfrak{a}_\sigma} = \zeta \cdot (g_y)^{c_l}$ ($\zeta \in \mu_{e_l}$), where $c_l = 12, 4, 3$ (resp. $e_l = 1, 3, 4$) according as $l \geq 5, = 3, = 2$.

Definition 5.10.4. Notations being as above, let $x \to y$ be a move of pairs of rational numbers which is $\rho^{\mathcal{C}}(\sigma)$-admissible at level m modulo m^2M. (In this case, by assumption $x, y \notin \mathbb{Z}^2$.) Define then the value

$$\kappa^{m,m^2M}_{x\to y,\mathcal{C}}(\sigma) = \left(\kappa^{m,m^2M}_{x\to y,l}(\sigma)\right)_{l:\,\text{prime}\in|\mathcal{C}|} \in \mathbb{Z}_{\mathcal{C}}$$

by

$$\left(\frac{(g_x^{c_l})^{1/l^n}|_{\mathfrak{a}_\sigma}}{(g_y^{c_l})^{1/l^n}}\right) = \zeta_{e_l l^n}^{\kappa^{m,m^2M}_{x\to y,l}(\sigma)} \qquad (l^n \in |\mathcal{C}|,\ l \text{ prime}).$$

An easy observation: Each l-component of $\kappa^{m,m^2M}_{x\to y,\mathcal{C}}(\sigma)$ for prime $l \in |\mathcal{C}|$ can be interpreted as $\kappa^{m,m^2M}_{x\to y,(l)}(\sigma)$, i.e., as obtained by replacing $\mathcal{C}$ by the full class of l-groups (denoted (l)). Note here that $\rho^{\mathcal{C}}(\sigma)$-admissibility implies $\rho^{(l)}(\sigma)$-admissibility.

One more crucial remark should be added here: Our move of pairs $x \to y$ is chosen after $\sigma \in \pi_1(M^\omega_{1,1}, \bar{q})$ is given. Therefore $\kappa^{m,m^2M}_{x\to y,\mathcal{C}}$ does not form a single function $\pi_1(M^\omega_{1,1}, \bar{q}) \to \mathbb{Z}_{\mathcal{C}}$. What we have obtained is, in general, only a "collection of quantities", which, however, still turn out to have certain coherence as we will see in the next section.

In particular, if we restrict the range of σ to the pro-$\mathcal{C}$ congruence kernel where $\rho^{\mathcal{C}}(\sigma) = 1$, then we may fix $x = y$ for all of them, and $\kappa^{m,m^2M}_{x\to x,\mathcal{C}}$ gives an additive character (even independent of M). We will discuss this in more detail in §6.10.

§6. Modular unit formula

§6.1. Set up

Let $\mathcal{C}$ be a full class of finite groups. Suppose we are given a $\Gamma(1)$-test object (E, O, ω) defined over a regular domain B ($\supset \mathbb{Q}$) whose connected spectrum $S = \mathrm{Spec}(B)$ has a fixed base point $\bar{b} : \mathrm{Spec}(\Omega) \to S$. We have a unique representative morphism $r : S \to M^\omega_{1,1}$ together with $r_E : E \setminus \{O\} \to M^\omega_{1,2}$. Pick any path γ

from $r(\bar{b})$ to the standard base point $\bar{q}$ on $M_{1,1}$ introduced in the previous section. Then, through the Weierstrass tangential section (§2.4), we obtain a path $\tilde{\gamma}$ from $r_E(\overrightarrow{\mathfrak{w}}_{\bar{b}})$ to $\overrightarrow{\mathfrak{w}}_{\bar{q}}$ on $M^{\omega}_{1,2}$ lifting γ. Note that this uniquely determines a lift $r_E(\overrightarrow{\mathfrak{w}}_{\bar{b}})^{\sim}$ on $\widetilde{M^{\omega}_{1,2}}$ connecting to $\tilde{\mathfrak{w}}_{\bar{q}}$ selected in §5.8.

Let (x, y, g_2, g_3, t) be the associated parameter for $(E/B, O, \omega)$ and let $\mathcal{O}_E$ denote the structure ring $H^0(E \setminus \{O\}, \mathcal{O}) = B[x, y]/(y^2 = 4x^3 - g_2x - g_3)$ of the affine scheme $E \setminus \{O\}$. Fix a maximal etale extension $\widetilde{\mathcal{O}}_E$ whose spectrum $\widetilde{E \setminus \{O\}} := \mathrm{Spec}(\widetilde{\mathcal{O}}_E)$ serves as an etale universal cover of $E \setminus \{O\}$ over B. We also pick and fix a lift $\tilde{\mathfrak{w}}_{\bar{b}} : \mathrm{Spec}(\Omega\{\{t\}\}) \to \widetilde{E \setminus \{O\}}$ of the Weierstrass base point $\overrightarrow{\mathfrak{w}}_{\bar{b}}$.

The fiber product P of $\widetilde{M^{\omega}_{1,2}}$ and $E \setminus \{O\}$ over $M^{\omega}_{1,2}$ is, in general, not connected. But since there is a canonical bijection between the fiber set $\widetilde{M^{\omega}_{1,2}}(r_E(\overrightarrow{\mathfrak{w}}_{\bar{b}}))$ and the fiber set $P(\overrightarrow{\mathfrak{w}}_{\bar{b}})$, we have a canonical point p_0 in the latter set corresponding to $r_E(\overrightarrow{\mathfrak{w}}_{\bar{b}})^{\sim}$. This determines the morphism of pointed schemes

$$\widetilde{r_E} : (\widetilde{E \setminus \{O\}}, \tilde{\mathfrak{w}}_{\bar{b}}) \to (P, p_0) \to (\widetilde{M^{\omega}_{1,2}}, r_E(\overrightarrow{\mathfrak{w}}_{\bar{b}})^{\sim})$$

which actually factors through the connected component of P carrying the p_0. Correspondingly, we have a canonical ring homomorphism

$$\widetilde{r_E}^* : \widetilde{\mathcal{O}^{\omega}_{1,2}} \to \widetilde{\mathcal{O}}_E.$$

For any connected pointed etale Galois cover $f : (Y, \bar{y}) \to (X, \bar{x})$ dominated by $(\widetilde{E \setminus \{O\}}, \tilde{\mathfrak{w}}_{\bar{b}})$, we write $\mathfrak{a}_{Y/X} : \pi_1(X, \bar{x}) \to \mathrm{Aut}(Y/X)$ for the natural surjective anti-homomorphism determined by $\mathfrak{a}_{Y/X}(\sigma)(\bar{y}) = \sigma(\bar{y})$ for $\sigma \in \pi_1(X, \bar{x})$ (which has monodromy action on $\bar{y} \in Y(\bar{x}) = Y \otimes_X \bar{x}$ on the RHS). In terms of the corresponding rings $\mathcal{O}_X \subset \mathcal{O}_Y \subset \widetilde{\mathcal{O}}_E$, it induces a canonical left action of $\pi_1(X, \bar{x})$ on the functions in $\mathcal{O}_Y$ (written $f \mapsto f|_{\mathfrak{a}_\sigma}$) characterized by the property

$$f(\mathfrak{a}_\sigma(\phi)) = (f|_{\mathfrak{a}_\sigma})(\phi) \quad (\phi \in Y(R) = \mathrm{Hom}(\mathcal{O}_Y, R),\ f \in \mathcal{O}_Y,\ \mathfrak{a}_\sigma = \mathfrak{a}_{Y/X}(\sigma))$$

for variable rings R. (Note that this use of notation $\mathfrak{a}_\sigma$ is compatible with that in §2.7.)

Let B^{ur} be the maximal unramified subextension of B inside the above $\widetilde{\mathcal{O}}_E$. One observes that then $S^{\mathrm{ur}} = \mathrm{Spec}(B^{\mathrm{ur}})$ is naturally pointed by $\bar{b}$, the image of $\tilde{\mathfrak{w}}_{\bar{b}}$. Thus, each of the spectra of the rings in the inclusion series

$$B \subset B^N \subset B^{\mathcal{C}} = \bigcup_{N \in |\mathcal{C}|} B^N \subset B^{\mathrm{ur}}$$

has a standard base point valued in Ω which we will write $\bar{b}$, $\bar{b}^N$, $\bar{b}^{\mathcal{C}}$, $\bar{b}^{\mathrm{ur}}$ respectively. From the anti-isomorphism $\mathfrak{a}_{S^{\mathrm{ur}}/S} : \pi_1(S, \bar{b}) \to \mathrm{Aut}(S^{\mathrm{ur}}/S)$, we have a standard isomorphism $\pi_1(S, \bar{b}) \xrightarrow{\sim} \mathrm{Aut}(B^{\mathrm{ur}}/B)$ written $\sigma \mapsto (*|\mathfrak{a}_\sigma)$. The above

homomorphism $\widetilde{r_E}^*$ induces by restriction a ring homomorphism $\widetilde{\mathcal{O}^{\omega}_{1,1}} \to B^{\mathrm{ur}}$. This enables us to consider the images in B^{ur} of algebraic modular forms or of selected power roots of Δ and Siegel units in the last section (§§5.8–5.10). Accordingly, ρ_{Δ}, $\kappa^{m,m^2M,\mathcal{C}}_{x\to y}$ make sense on $\pi_1(S,\bar{b})$ and factor through $\pi_1(M^{\omega}_{1,1},\bar{q})$ via the representative morphism $r : S \to M^{\omega}_{1,1}$ and the selected path $\gamma : r(\bar{b}) \rightsquigarrow \bar{q}$.

§6.2. Main approximation theorem

In this subsection, we state our main approximation theorem. The proof will be given in the last part of this section.

By taking conjugation via the above r_E and $\tilde{\gamma}$, we can also pull back the standard generators $\mathbf{x}_1, \mathbf{x}_2$ of $\Pi_{1,1} = \pi_1(\mathrm{Tate}_{\bar{q}}\backslash\{O\}, \overrightarrow{\mathfrak{w}}_{\bar{q}})$ (§5.2) to $\pi_1(E_{\bar{b}}\backslash\{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ (denoted by the same symbols) so that $\mathbf{z} = [\mathbf{x}_1, \mathbf{x}_2]^{-1}$ generates an inertia subgroup over the missing point O on $E_{\bar{b}}\backslash\{O\}$. *Throughout this section, we keep the symbols* $\mathbf{x}_1, \mathbf{x}_2, \mathbf{z}$ *to denote these specified generators of* $\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ and their images in the maximal pro-$\mathcal{C}$ quotient:

$$\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})(\mathcal{C}) = \langle \mathbf{x}_1, \mathbf{x}_2, \mathbf{z} \mid [\mathbf{x}_1, \mathbf{x}_2]\mathbf{z} = 1 \rangle_{\text{pro-}\mathcal{C}}.$$

Plugging this into the setting of §3, we obtain, for $m \in |\mathcal{C}|$, the monodromy invariants (of Eisenstein type) $\mathbb{E}^{\mathcal{C}}_m : \pi_1(S,\bar{b}) \times \mathbb{Z}^2_{\mathcal{C}} \to \mathbb{Z}_{\mathcal{C}}$ (Definition 3.4.1).

Theorem 6.2.1 (Modular unit formula). *Let* $\sigma \in \pi_1(S,\bar{b})$. *For any* $M \in |\mathcal{C}|$ *and* $(u,v) \in \mathbb{Z}^2_{\mathcal{C}} \setminus (m\mathbb{Z}_{\mathcal{C}})^2$, *pick two pairs of rational integers* $\mathbf{r} = (r_1, r_2)$, $\mathbf{s} = (s_1, s_2)$ *such that* $\mathbf{r} \equiv (u,v) \bmod mM^2 2^{\varepsilon}$ (*where* $\varepsilon = 0, 1$ *according as* $2 \nmid M$, $2|M$ *respectively*) *and* $x = (r_1/m, r_2/m) \to y = (s_1/m, s_2/m)$ *is* $\rho^{\mathcal{C}}(\sigma)$*-admissible at level* m *modulo* m^2M^2. *Then*

$$\mathbb{E}^{\mathcal{C}}_m(\sigma; u, v) \equiv \tfrac{1}{12}\big(\kappa^{m,m^2M^2}_{x\to y,\mathcal{C}}(\sigma) - \rho_{\Delta}(\sigma)\big) + \rho_m(\sigma) \bmod M^2.$$

Here, ρ_m is the Kummer character along positive power roots of m in the sense of §5.9. Since $\Delta(E, m\omega) = m^{-12}\Delta(E,\omega)$, the above right hand side can be written in the form of Theorem A of the Introduction. We also note that by definition $\mathbb{E}_m(\sigma; 0, 0) = 0$, and recall from Proposition 3.4.8 that $\mathbb{E}_m(\sigma; u, v)$ for $(u,v) \in (m\mathbb{Z}_{\mathcal{C}})^2$ can be evaluated from $\mathbb{E}_m(\sigma; u+1, v)$, $\mathbb{E}_m(\sigma; 1, 0)$ and an elementary term.

For the proof of the above theorem, observe first that, without loss of generality, *we may assume* $\mathcal{C}$ *is the full class of all finite groups* (cf. Remark 3.6.5). By the Chinese Remainder Theorem, *we may also assume* $M = l^n$ *for a prime* l. Below, we shall start the proof with these assumptions being supposed. In particular, we drop $\mathcal{C}$ from the notation $\kappa^{m,m^2M^2}_{x\to y,\mathcal{C}}(\sigma)$, which means $\mathcal{C}$ is supposed to be the class of all finite groups till the end of §6.9.

§6.3. Geometrically abelian coverings

Let N be an integer in $|\mathcal{C}|$. The isogeny $E \overset{N}{\to} E$ by multiplication by N gives an etale B-cover of degree N^2. Let us write this covering as $E_B^N \to E$ to distinguish the copy E_B^N from E/B. We have specified differential forms both on E/B and E_B^N, which will be written ω and ω_N respectively. The pull-back of ω to E_B^N is then $N\omega_N$. The associated parameter of E_B^N is of the form $(g_2, g_3, x_N, y_N, t_N)$, where the last three parameters x_N, y_N, t_N can be explicitly written from the original ones for E/B by classical well known N-division formulas for elliptic functions. In particular, t_N can be expanded in a power series of the form $\frac{t}{N}(1 + tB[[t]])$.

The above isogeny by multiplication by N also induces the etale cover

$$E_0^N := E_B^N \setminus E^N[N] \to E_0 := E \setminus \{O\}.$$

The etale neighborhoods of the zero sections O in both E_0^N and E_0 are canonically isomorphic, i.e., $\mathrm{Rev}^O((E_B^N/O)^\wedge) \approx \mathrm{Rev}^O((E/O)^\wedge)$. From this we obtain a unique tangential base point $\overrightarrow{\mathfrak{w}}_N$ valued in $\Omega\{\{t\}\}$ near the zero section of E_0^N that lifts the Weierstrass base point $\overrightarrow{\mathfrak{w}}_{\bar{b}}$ on E_0. Note that the Weierstrass base point $\overrightarrow{\mathfrak{w}}_{\bar{b}}^N$ of E_0^N valued in $\Omega\{\{t_N\}\}$ itself has to be distinguished from $\overrightarrow{\mathfrak{w}}_N$. But since $t_N \sim t/N$ and since we have a standard power root system $\{\sqrt[n]{N} > 0\}$, we can fix an isomorphism of Puiseux power series

$$\Omega\{\{t_N\}\} \xrightarrow{\sim} \Omega\{\{t\}\} \quad (t_N^{1/n} \mapsto t^{1/n}/\sqrt[n]{N},\ n = 1, 2, \dots)$$

which defines a standard path from $\overrightarrow{\mathfrak{w}}_N$ to $\overrightarrow{\mathfrak{w}}_{\bar{b}}^N$. Through this path $\overrightarrow{\mathfrak{w}}_N \rightsquigarrow \overrightarrow{\mathfrak{w}}_{\bar{b}}^N$, the fundamental group $\pi_1(E_0^N, \overrightarrow{\mathfrak{w}}_N)$, which is a subgroup of $\pi_1(E_0, \overrightarrow{\mathfrak{w}}_{\bar{b}})$, is isomorphic to $\pi_1(E_0^N, \overrightarrow{\mathfrak{w}}_{\bar{b}}^N)$.

§6.4. Geometrically meta-abelian coverings

Suppose $N = ml$ with l a prime factor of N. We shall construct a sequence of etale covers of E_0^N of degrees l^n $(n = 1, 2, \dots)$ whose geometric fibers form connected cyclic covers of $(E_0^N)_{\bar{b}}$. As in the previous subsection, let $N\omega_N$ on E_B^N be the pull-back of ω and let $(g_2, g_3, X_N, Y_N, t_N)$ be the associated parameter of (E_B^N, O, ω_N) (§2.2). Define then

$$\Theta_{l,N} = \begin{cases} \dfrac{\Delta(E_B^N, O, \omega_N)^{l^2}}{l^{12}} \displaystyle\prod_{P \in E[l] \setminus \{O\}} \frac{1}{(X_N - X_N(P))^6} & (l \geq 5), \\ \dfrac{\Delta(E_B^N, O, \omega_N)^3}{3^4} \displaystyle\prod_{P \in E[3] \setminus \{O\}} \frac{1}{(X_N - X_N(P))^2} & (l = 3), \\ \dfrac{\Delta(E_B^N, O, \omega_N)}{(-Y_N)^3} & (l = 2). \end{cases} \tag{6.4.1}$$

Note here that $\Delta(E_B^N, O, \omega_N) \in B^\times$. Also, each $P \in E[l]$ $(\subset E_B^N[N] \otimes B^l)$ means a section $S^l \to E_B^N \otimes B^l$ and $x_N(P)$ gives an element of B^l $(\subset B^N)$. Although each factor $x_N - x_N(P)$ is a function on $E_0^N \otimes B^l$, the product is easily seen to lie in the structure ring $\mathcal{O}_{E_B^N}$ of E_0^N over B. The associated divisor $\mathrm{div}(\Theta_{l,N})$ of $\Theta_{l,N}$ is given by

$$\mathrm{div}(\Theta_{l,N}) = \begin{cases} 12(l^2-1)\cdot[O] - 12\cdot(E_B^N[l] \setminus \{O\}) & (l \geq 5), \\ 4\cdot 8\cdot[O] - 4\cdot(E_B^N[3] \setminus \{O\}) & (l = 3), \\ 3\cdot 3\cdot[O] - 3\cdot(E_B^N[2] \setminus \{O\}) & (l = 2). \end{cases} \tag{6.4.2}$$

Now, consider the function $\Theta_{l,N} = \Theta_{l,ml}$ as a B-morphism of $E_B^N \setminus E_B^N[ml]$ to $\mathbf{G}_\mathrm{m} = \mathrm{Spec}\, B[T, 1/T]$ (via $T \mapsto \Theta_{l,ml}$). And further take the pull-back Y^{ml,l^k} by the l^k-isogeny of $\mathbf{G}_\mathrm{m} = \mathrm{Spec}\, B[U, 1/U] \to \mathbf{G}_\mathrm{m} = \mathrm{Spec}\, B[T, 1/T]$ $(T \mapsto U^{l^k})$. Then we have the commutative diagram

$$\begin{array}{ccccccc}
\mathbf{G}_\mathrm{m} & \xleftarrow{\Theta_{l,ml}^{1/l^k}} & Y^{ml,l^k} & \longleftarrow & Y_{\bar{b}}^{ml,l^k} & \xleftarrow{\overrightarrow{\mathfrak{w}}_Y} & \mathrm{Spec}(\Omega\{\{t\}\}) \\
{\scriptstyle l^k}\downarrow & & \downarrow & & \downarrow & & \downarrow{\scriptstyle (\ )^{l^k}} \\
\mathbf{G}_\mathrm{m} & \xleftarrow{\Theta_{l,ml}} & E_B^{ml} \setminus E_B^{ml}[ml] & \longleftarrow & E_{\bar{b}}^{ml} \setminus E_{\bar{b}}^{ml}[ml] & \xleftarrow{\overrightarrow{\mathfrak{w}}_{ml}} & \mathrm{Spec}(\Omega\{\{t\}\}) \\
 & & \downarrow & & \downarrow & & \| \\
 & & E_0 = E \setminus \{O\} & \longleftarrow & E_{\bar{b}} \setminus \{O\} & \xleftarrow{\overrightarrow{\mathfrak{w}}_{\bar{b}}} & \mathrm{Spec}(\Omega\{\{t\}\}) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & S & \longleftarrow & \bar{b} & = & \mathrm{Spec}(\Omega)
\end{array} \tag{6.4.3}$$

where $\overrightarrow{\mathfrak{w}}_Y$ is the induced base point on $Y_{\bar{b}}^{ml,l^k}$. Since the degrees of $\mathrm{div}(\Theta_{l,ml})$ at irreducible divisors in $E[l]$ are prime to l, the pull-backed scheme Y^{ml,l^k} is geometrically connected over S. One can regard $\pi_1(Y^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$ naturally as a subgroup of $\pi_1(E_0^{ml}, \overrightarrow{\mathfrak{w}}_{ml})$. Moreover, regarding the toroidal type transformation $t \mapsto t^{1/l^k}$ of $\Omega\{\{t\}\}$ as equivalence of base points, we see that a unique etale morphism $(\widetilde{E \setminus \{O\}}, \tilde{\mathfrak{w}}_{\bar{b}}) \to (Y^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$ is determined as a pointed cover. In this way, $\Theta_{l,ml}^{1/l^k} \in \mathcal{O}(Y^{ml,l^k})^\times$ is considered as a specific element of $\mathcal{O}_E^\times$.

§6.5. Inertia classes and theta values

We inherit the notations of the previous section. If we extend the base scheme S to $S^N = \mathrm{Spec}(B^N)$ which corresponds to the kernel of the monodromy representation $\rho^N : \pi_1(S, \bar{b}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ (§2.6), the divisor $E[N] \otimes B^N$ $(\subset E_B^N \otimes_B B^N)$ is a

union of N^2 copies of S^N indexed by the level structure $\alpha^N : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E^N[N]$. The geometric fiber $(E_0^N)_{\bar{b}} = E_{\bar{b}}^N \setminus E_{\bar{b}}^N[N]$ is an abelian etale cover of $(E_0)_{\bar{b}} = E_{\bar{b}} \setminus \{O\}$ with Galois group $(\mathbb{Z}/N\mathbb{Z})^2$. The puncture of $(E_0^N)_{\bar{b}}$ corresponding to $\alpha^N(\mathbf{a})$ will be denoted by $P_{\mathbf{a}}$.

Let $\alpha^{ml} : (\mathbb{Z}/ml\mathbb{Z})^2 \xrightarrow{\sim} E^{ml}[ml]$ be the level ml-structure induced from our choice of generators $\mathbf{x}_1, \mathbf{x}_2$ of $\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ in §6.2 (cf. §2.6). For convenience, we shall use the notation

$$(\mathbb{Z}/ml\mathbb{Z})_0^2 := \big\{\mathbf{a} = (a_1, a_2) \in (\mathbb{Z}/ml\mathbb{Z})^2 \mid l\mathbf{a} \neq \mathbf{0}\big\}.$$

For $\mathbf{a} \in (\mathbb{Z}/ml\mathbb{Z})_0^2$, since the image of the section $\alpha^{ml}(\mathbf{a}) : S^{ml} \to E^{ml}$ does not intersect the support of $\mathrm{div}(\Theta_{l,ml})$, the value $\Theta_{l,ml}(\alpha^{ml}(\mathbf{a}))$ lies in $(B^{ml})^\times$. In fact, the classical formula (cf. [KL81, §10, Th. 2.2]; see also [Fr16, pp. 383–384] for the case $l = 2$) gives

$$\Theta_{l,ml}(\mathbf{a}) = \Theta_{l,ml}(\alpha^{ml}(\mathbf{a})) = \begin{cases} \Delta \cdot (\theta_x)^{l^2}/\theta_{lx} & (l \geq 5), \\ \eta^8 \cdot (g_x^9)^4/g_{3x}^4 & (l = 3), \\ \eta^6 \cdot (g_x^4)^3/g_{2x}^3 & (l = 2), \end{cases} \tag{6.5.1}$$

for $\mathbf{a} \in (\mathbb{Z}/ml\mathbb{Z})_0^2$, where $x = (r_1/ml, r_2/ml) \in \mathbb{Q}^2$ is such that $r_i \in [0, ml]$ $(i = 1, 2)$ are integers with $a_i = r_i \bmod ml$. The right hand side of (6.5.1) is in total an algebraic modular form of level $\Gamma(ml)$ (Prop. 4.2.4), and can be evaluated at the $\Gamma(ml)$-test object $(E^{ml}/B^{ml}, \alpha^{ml}, \omega_{ml})$ with value in $(B^{ml})^\times$. However, in fact, we may evaluate the RHS at our compatible sequence of $\Gamma(N)$-test objects $(E^N/B^N, \alpha^N, \omega_N)$ as long as $ml \,|\, N$ to obtain a well defined value in $\bigcup_{N=1}^{\infty}(B^N)^\times \subset (B^{\mathrm{ur}})^\times$. This observation is crucial to our subsequent arguments in which, by Proposition 4.2.1, the numerator and denominator of the RHS of (6.5.1) individually make sense as elements of $(B^{12m^2l^2})^\times$, or more simply, just as elements of $(B^{\mathrm{ur}})^\times$.

Now, we shall consider distributions of inertia subsets in $\pi_1(Y_{\bar{b}}^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$. Since the support of the divisor of $\Theta_{l,ml}$ is in $E^{ml}[l]$, in the (completion of the) cyclic cover of curves $Y_{\bar{b}}^{ml,l^k} \to E_{\bar{b}}^{ml} \setminus E_{\bar{b}}^{ml}[ml]$, each $P_{\mathbf{a}} \in E_{\bar{b}}^{ml}[l]$ $(\mathbf{a} \in (m\mathbb{Z}/ml\mathbb{Z})^2)$ is ramified, while each $P_{\mathbf{a}} \in E_{\bar{b}}^{ml}[ml] \setminus E_{\bar{b}}^{ml}[l]$ $(\mathbf{a} \in (\mathbb{Z}/ml\mathbb{Z})_0^2)$ is unramified and splits into l^k points on the cover. In particular, if $(u, v) \in (\hat{\mathbb{Z}})^2 \setminus (m\hat{\mathbb{Z}})^2$, then the inertia group generated by

$$\mathbf{z}_{uv} := (\mathbf{x}_2^{-v}\mathbf{x}_1^{-u})\mathbf{z}(\mathbf{x}_1^u\mathbf{x}_2^v)$$

still lies inside $\pi_1(Y_{\bar{b}}^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$ $(\subset \pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}}))$. Here, notice that $\mathbf{x}_1, \mathbf{x}_2$ denote the prescribed generators of $\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ and that $\mathbf{z}_{uv}$ is in general not conjugate to $\mathbf{z}$ in the subgroup $\pi_1(Y_{\bar{b}}^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$: As remarked above, the inertia

groups over $P_{\mathbf{a}}$ ($\mathbf{a} \in (\mathbb{Z}/ml\mathbb{Z})_0^2$) split into a union of l^k conjugacy classes of inertia subgroups in $\pi_1(Y_{\bar{b}}^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$.

Definition 6.5.2. For $(u,v) \in (\hat{\mathbb{Z}})^2 \setminus (m\hat{\mathbb{Z}})^2$, define the missing point $Q_{u,v}^{ml,l^k}$ on $Y_{\bar{b}}^{ml,l^k}$ to be the one determined by the inertia group $\langle \mathbf{z}_{uv} \rangle$. Let X^{ml,l^k} be the integral closure of $E_B^{ml} \setminus E_B^{ml}[l]$ in Y^{ml,l^k}. The specific element $\Theta_{l,ml}^{1/l^k}$ is considered as a unit of the structure ring of X^{ml,l^k}. Moreover, the above point $Q_{u,v}^{ml,l^k}$ determines a B^{ur}-point of $X^{ml,l^k}/B$, which we shall write $\beta_{u,v}^{ml,l^k} : S^{\mathrm{ur}} \to X^{ml,l^k}$. Composing these two, one obtains a unit of B^{ur} which will be written as

$$\Theta_{l,ml}^{1/l^k}(u,v) := \Theta_{l,ml}^{1/l^k}(\beta_{u,v}^{ml,l^k}(S^{\mathrm{ur}})) \in (B^{\mathrm{ur}})^{\times}. \tag{6.5.3}$$

On the other hand, the B^{ur}-point $\beta_{u,v}^{ml,l^k} : S^{\mathrm{ur}} \to X^{ml,l^k}$ of $X^{ml,l^k}/B$ lies over the B^{ml}-point of $E_B^{ml} \setminus E_B^{ml}[l]$ induced from the section $\alpha^{ml}(\mathbf{a}) : S^{ml} \to E^{ml}$ for $\mathbf{a} = (a_1, a_2) \in (\mathbb{Z}/ml\mathbb{Z})_0^2$ representing the residue class of (u,v) modulo ml.

Lemma 6.5.4. *Let $c_l = 12, 4, 3$ according as $l \geq 5, = 3, = 2$ respectively. For $(r_1, r_2) \in \mathbb{Z}^2 \setminus (m\mathbb{Z})^2$, set $x = (r_1/ml, r_2/ml) \in \mathbb{Q}^2$. Then*

$$\Theta_{l,ml}^{1/l^k}(r_1, r_2) = (\eta^{2c_l})^{1/l^k} \cdot \frac{((g_x^{c_l})^{1/l^k})^{l^2}}{(g_{lx}^{c_l})^{1/l^k}},$$

where $(\eta^2)^{1/l^k}$, g_*^{1/l^k} are the pull-backs by $S^{\mathrm{ur}} \to (M_{1,1}^{\omega})^{\mathrm{ur}}$ of the corresponding elements introduced respectively in §5.9 and §5.10.

Proof. Put $N = ml$. By functoriality of the construction, it suffices to work in the complex analytic model of Tate form: $E^N = \mathbb{C}/N\mathfrak{L}_\tau \to E = \mathbb{C}/\mathfrak{L}_\tau$ ($\mathfrak{L}_\tau = \mathbb{Z}\tau + \mathbb{Z}$, $\tau \in \mathfrak{H}$) so that, say, $\Delta(E^N, O, 2\pi i dz_N) = \Delta(\mathbb{C}/N\mathfrak{L}_\tau, O, 2\pi i \frac{dz}{N}) = \Delta(2\pi i \mathfrak{L}_\tau) = \Delta(\mathbb{C}/\mathfrak{L}_\tau, O, 2\pi i dz)$, which coincides with $\eta(\tau)^{24}$. Express the elliptic curve E^N as $Y_N^2 = 4x_N^3 - g_2 X_N - g_3$ with

$$\begin{aligned}
X_N &= \wp(2\pi i z_N, 2\pi i N\mathfrak{L}_N) = \frac{1}{(2\pi i)^2}\wp(z_N, N\mathfrak{L}_N),\\
Y_N &= \wp'(2\pi i z_N, 2\pi i N\mathfrak{L}_N) = \frac{1}{(2\pi i)^3}\wp'(z_N, N\mathfrak{L}_N),\\
g_2 &= g_2(2\pi i\mathfrak{L}_\tau) = \frac{1}{12}\Big(1 + 240\sum_{n\geq 1}\sigma_3(n)q_\tau^n\Big),\\
g_3 &= g_3(2\pi i\mathfrak{L}_\tau) = -\frac{1}{216}\Big(1 - 504\sum_{n\geq 1}\sigma_5(n)q_\tau^n\Big).
\end{aligned}$$

Then the fundamental local coordinate at $O \in E^N$ is given by $t_N = -2x_N/y_N = 2\pi i z_N(1 + O(z_N))$. First, we shall see that one of the inertia groups over $P_{\mathbf{a}}$ is

generated by $\mathbf{z}_{uv}$ with $(u,v) \in \hat{\mathbb{Z}}^2$ satisfying $(u,v) \equiv \mathbf{a} \bmod N$. The starting inertia element $\mathbf{z} = \mathbf{z}_{00}$ determines the origin puncture $O = P_{\mathbf{0}}$ on $E^N \setminus E^N[N]$ which is the anchor point of the tangential base point $\overrightarrow{\mathfrak{w}}^N$ represented by (the image of) a real analytic small segment $\{z_N \mid 0 < t_N < \varepsilon\}$. Note that, for any $u, v \in \mathbb{Z}$ with $(u,v) \equiv \mathbf{a} \bmod m$, the puncture $P_{\mathbf{a}}$ is the anchor point of $\mathbf{x}_1^u \mathbf{x}_2^v(\overrightarrow{\mathfrak{w}}^N)$ which is obtained by continuously tracing the paths $\mathbf{x}_1^u \mathbf{x}_2^v$ from $\overrightarrow{\mathfrak{w}}^N$. The automorphism $\mathfrak{a}_{\mathbf{x}_1^u \mathbf{x}_2^v} \in \mathrm{Aut}(E^N \setminus E^N[N])$ is determined by $\mathbf{x}_1^u \mathbf{x}_2^v(\overrightarrow{\mathfrak{w}}^N) = \mathfrak{a}_{\mathbf{x}_1^u \mathbf{x}_2^v}(\overrightarrow{\mathfrak{w}}^N) = \mathfrak{a}_{\mathbf{x}_2}^v \mathfrak{a}_{\mathbf{x}_1}^u(\overrightarrow{\mathfrak{w}}^N)$. Extend $\mathfrak{a}_\gamma \in \mathrm{Aut}(E^N \setminus E^N[N])$ to a unique automorphism $\overline{\mathfrak{a}_\gamma}$ of E^N. Observing

$$\overline{\mathfrak{a}_{\mathbf{x}_2^{-v}\mathbf{x}_1^{-u}\mathbf{z}\mathbf{x}_1^u\mathbf{x}_2^v}}\,\overline{\mathfrak{a}_{\mathbf{x}_1^u\mathbf{x}_2^v}}(O) = \overline{\mathfrak{a}_{\mathbf{x}_2^v}}\,\overline{\mathfrak{a}_{\mathbf{x}_1^u}}\,\overline{\mathfrak{a}_{\mathbf{z}}}\,\overline{\mathfrak{a}_{\mathbf{x}_1^{-u}}}\,\overline{\mathfrak{a}_{\mathbf{x}_2^{-v}}}(\overline{\mathfrak{a}_{\mathbf{x}_2^v}}\,\overline{\mathfrak{a}_{\mathbf{x}_1^u}}(O)),$$

we see that the element $\mathbf{z}_{uv} := \mathbf{x}_2^{-v}\mathbf{x}_1^{-u}\mathbf{z}\mathbf{x}_1^u\mathbf{x}_2^v$ ($(u,v) \equiv \mathbf{a} \bmod N$) generates an inertia subgroup over $P_{\mathbf{a}} = \overline{\mathfrak{a}_{\mathbf{x}_1^u\mathbf{x}_2^v}}(O) = \overline{\mathfrak{a}_{\mathbf{x}_2^v}}\,\overline{\mathfrak{a}_{\mathbf{x}_1^u}}(O)$ in $\pi_1(E^N \setminus E^N[N], \overrightarrow{\mathfrak{w}}^N)$.

Next, recalling $N = ml$, we consider the Kummer cover $Y^{ml,l^k} \to E^{ml} \setminus E^{ml}[ml]$ by $\Theta_{l,ml}^{1/l^k}$ and its partial compactification $X^{ml,l^k} \to E^{ml} \setminus E^{ml}[l]$. Observe first that the following quotient of Siegel functions with $z_N = x_1\tau + x_2$ ($x = (x_1, x_2) \in \mathbb{R}^2$):

$$\begin{aligned}
&(6.5.5)\qquad \frac{g_x^{l^2}}{g_{lx}} \\
&= \frac{(-1)^{l^2}}{-1} \cdot \frac{q_\tau^{B_2(x_1)l^2/2}}{q_\tau^{B_2(lx_1)/2}} \cdot \frac{e^{\pi i x_2(x_1-1)l^2}}{e^{\pi i l x_2(lx_1-1)}} \cdot \frac{(1-q_{z_N})^{l^2}}{1-q_{z_N}^l} \prod_{n\geq 1} \frac{(1-q_\tau^n q_{z_N})^{l^2}(1-q_\tau^n q_{z_N}^{-1})^{l^2}}{(1-q_\tau^n q_{z_N}^l)(1-q_\tau^n q_{z_N}^{-l})} \\
&= \big((-1)^{l^2-1} q_{z_N}^{\frac{l-l^2}{2}} q_\tau^{\frac{l^2-1}{12}}\big) \frac{(1-q_{z_N})^{l^2}}{1-q_{z_N}^l} \prod_{n\geq 1} \frac{(1-q_\tau^n q_{z_N})^{l^2}(1-q_\tau^n q_{z_N}^{-1})^{l^2}}{(1-q_\tau^n q_{z_N}^l)(1-q_\tau^n q_{z_N}^{-l})}
\end{aligned}$$

turns out to be holomorphic in z_N (non-holomorphic factors are canceled) and that the infinite product factor has an expansion in z_N with principal coefficient $(q_\tau^{-1/24}\eta(\tau))^{2l^2-2}$. Since $\frac{(1-q_{z_N})^{l^2}}{1-q_{z_N}^l} = \frac{(-2\pi i z)^{l^2-1}}{l}(1 + O(z_N))$, it follows that $\Theta_{l,ml}(z_N)$ may be expressed as

$$(6.5.6)\quad \Theta_{l,N}(z_N) = \begin{cases} \Delta(\tau)\left(\dfrac{g_x^{l^2}}{g_{lx}}\right)^{12} = \dfrac{\Delta^{l^2}}{l^{12}}(2\pi i z_N)^{12(l^2-1)}(1 + O(z_N)) & (l \geq 5), \\ \eta(\tau)^8\left(\dfrac{g_x^9}{g_{3x}}\right)^4 = \dfrac{\Delta^3}{3^4}(2\pi i z_N)^{32}(1 + O(z_N)) & (l = 3), \\ \eta(\tau)^6\left(\dfrac{g_x^4}{g_{2x}}\right)^3 = \dfrac{\Delta}{2^3}(2\pi i z_N)^9(1 + O(z_N)) & (l = 2). \end{cases}$$

Our task is to look closely into a specific branch of $\Theta_{l,ml}^{1/l^k}$ and to evaluate it at

$z_N = \frac{z}{N} = \frac{r_1}{ml}\tau + \frac{r_2}{ml}$ when $(r_1, r_2) \in \mathbb{Z}^2 \setminus (m\mathbb{Z})^2$. (Note that $\Theta_{l,ml} = 0, \infty$ according as $(r_1, r_2) \in (ml\mathbb{Z})^2$ or $\in (m\mathbb{Z})^2 \setminus (ml\mathbb{Z})^2$ respectively.) To identify the branch of $\Theta_{l,ml}^{1/l^k}$, it suffices to specify l^k-th roots of all factors of (6.5.5) on the infinitesimally small segment $0 < z_N \ll 1$, i.e., $x_1 = 0$ and $0 < x_2 \ll 1$. For those factors other than $\frac{(-1)^{l^2}}{-1}$, $\frac{(1-q_{z_N})^{l^2}}{1-q_{z_N}^l}$, we shall take canonical (principal branch) l^k-th roots on the segment. For the remaining two factors (that contribute to the principal coordinate $2\pi i z_N$), we employ the following argument. By our definition of $\overrightarrow{\mathfrak{w}}_Y$ lifting $\overrightarrow{\mathfrak{w}}^{ml}$ (cf. (6.4.3)), the branch $\Theta_{l,ml}^{1/l^k}$ should be taken so that the l^k-th root of the segment $0 < t_N < \varepsilon$ in $\mathbf{G}_{\mathrm{m}}$ be kept positive real under the pull-back by the isogeny $\mathbf{G}_{\mathrm{m}} \to \mathbf{G}_{\mathrm{m}}$ of degree l^k. Since $t_N = 2\pi i z_N(1 + O(z_N))$, this means that the real infinitesimal segment $0 < z_N \ll 1$ attached to $\overrightarrow{\mathfrak{w}}^N$ on $E^N \setminus E^N[l]$ should be lifted to a real infinitesimal segment determined by $\mathrm{Arg}((2\pi i z_N)^{1/l^k}) = \frac{\pi}{2l^k}$ attached to $\overrightarrow{\mathfrak{w}}_Y$ on Y^{ml,l^k}. This latter condition is equivalent to choosing $(-1)^{1/l^k} := e^{\pi i/l^k}$ and $(1-q_x)^{1/l^k}$ to be the principal branch for $0 < x \ll 1$ so that $\mathrm{Arg}((-1)^{1/l^k}) = \frac{\pi}{2l^k}$, $\mathrm{Arg}((1-q_x)^{1/l^k}) = -\frac{\pi}{4l^k}$ and hence $(-1)^{1/l^k} \cdot (1-q_{z_N})^{1/l^k} = (2\pi i z_N)^{1/l^k}(1 + O(z_N))$, $(-1)^{1/l^k} \cdot (1 - q_{z_N}^l)^{1/l^k} = (2\pi i l z_N)^{1/l^k}(1 + O(z_N))$ on $0 < z_N \ll 1$.

Now, for $(r_1, r_2) \in \mathbb{Z}^2 \setminus (m\mathbb{Z})^2$, we shall figure out the place Q_{r_1,r_2}^{ml,l^k} determined by the inertia element $\mathbf{z}_{\mathbf{r}} = (\mathbf{x}_2^{-r_2}\mathbf{x}_1^{-r_1})\mathbf{z}(\mathbf{x}_1^{r_1}\mathbf{x}_2^{r_2})$. It must be obtained as a unique puncture on Y^{ml,l^k} anchoring the tangential base point $\mathbf{x}_1^{r_1}\mathbf{x}_2^{r_2}(\overrightarrow{\mathfrak{w}}_Y)$ whose location is detected by tracing the continuous move of the tangential base point $\overrightarrow{\mathfrak{w}}_Y$ (represented by the above infinitesimal segment on Y^{ml,l^k}) along the (lifts of) paths $\mathbf{x}_2^{r_2}$ first and $\mathbf{x}_1^{r_1}$ afterwards. As observed above, our selection of l^k-th power roots of (6.5.5) is given factor by factor, hence it can be separated to l^k-th power roots of its numerator $g_x^{l^2}$ and denominator g_{lx} real analytically, each of which can move continuously along the path $\mathbf{x}_1^{r_1}\mathbf{x}_2^{r_2}$ so as to keep our choice of branch of power roots of Siegel units (§5.10) from the start $\overrightarrow{\mathfrak{w}}_Y$. During the trip, the non-zero continuity of both $(g_x^{l^2})^{1/l^k}$ and $(g_{lx})^{1/l^k}$ in $x = (x_1, x_2)$ along the path keeps correct determination of l^k-th root branches, and hence, upon arrival at the goal $\mathbf{x}_1^{r_1}\mathbf{x}_2^{r_2}(\overrightarrow{\mathfrak{w}}_Y)$ anchored at Q_{r_1,r_2}^{ml,l^k}, we obtain the desired value as stated in the lemma. □

§6.6. Estimating difference of sections

We now work in the extension of the profinite groups

$$1 \to \pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}}) = \Pi_{1,1} \to \pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}}) \to \pi_1(S, \bar{b}) \to 1$$

with the Weierstrass tangential section $s_{\overrightarrow{\mathfrak{w}}} : \pi_1(S, \bar{b}) \to \pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$. Write $\bar{\sigma} := s_{\overrightarrow{\mathfrak{w}}}(\sigma)$ for each $\sigma \in \pi_1(S, \bar{b})$.

Since $\Theta_{l,ml}$ is defined over B and has zeros of order prime to l, the etale cover $Y^{ml,l^k} \to E_B^{ml} \setminus E_B^{ml}[ml]$ is connected, defined over B and total ramified over O. Taking $k \to \infty$, we can consider the subgroup $\pi_1(Y^{ml,l^\infty}, \overrightarrow{\mathfrak{w}}_Y)$ of $\pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ surjectively mapped onto $\pi_1(S, \bar{b})$. The above totally-ramifiedness of $Y^{ml,l^k} \to E_B^{ml} \setminus E_B^{ml}[ml]$ at O implies triviality of the intersection of the inertia subgroup $\langle \mathsf{z} \rangle \subset \pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ with $\pi_1(Y^{ml,l^\infty}, \overrightarrow{\mathfrak{w}}_Y)$, i.e., $\pi_1(Y^{ml,l^\infty}, \overrightarrow{\mathfrak{w}}_Y) \cap \langle \mathsf{z} \rangle = \{1\}$. Therefore, for each $\sigma \in \pi_1(S, \bar{b})$, there exists a unique $\sigma_m \in \pi_1(Y^{ml,l^\infty}, \overrightarrow{\mathfrak{w}}_Y)$ which normalizes $\langle \mathsf{z} \rangle$ and is mapped to σ. Let us compare $\bar{\sigma}$ and σ_m. Note that $\bar{\sigma}$ is also contained in the normalizer of $\langle \mathsf{z} \rangle$, and $\pi_1(E_B^{ml} \setminus E_B^{ml}[ml], \overrightarrow{\mathfrak{w}}_{ml})$ contains this normalizer. The difference $\bar{\sigma}\sigma_m^{-1}$ thus belongs to $\pi_1(E_{\bar{b}}^{ml} \setminus E_{\bar{b}}^{ml}[ml], \overrightarrow{\mathfrak{w}}_{ml})$. Since $\pi_1(E_{\bar{b}}^{ml} \setminus E_{\bar{b}}^{ml}[ml], \overrightarrow{\mathfrak{w}}_{ml})/\pi_1(Y_{\bar{b}}^{lm,l^\infty}, \overrightarrow{\mathfrak{w}}_Y)$ is generated by the image of z, it follows that there exists a unique l-adic integer $\xi_m(\sigma)$ such that $\mathsf{z}^{\xi_m(\sigma)}\bar{\sigma}$ is contained in $\pi_1(Y^{lm,l^\infty}, \overrightarrow{\mathfrak{w}}_Y)$. So, without loss of generality we may take σ_m in the form $\sigma_m = \mathsf{z}^{\xi_m(\sigma)}\bar{\sigma}$ for a unique $\xi_m(\sigma) \in \mathbb{Z}_l$.

Lemma 6.6.1. *We have*

$$\xi_m(\sigma) = \frac{l^2}{12(l^2-1)}\rho_\Delta(\sigma) - \frac{1}{l^2-1}\rho_l(\sigma) - \rho_{ml}(\sigma) \quad (\sigma \in \pi_1(S, \bar{b})),$$

where ρ_l and ρ_{ml} are the Kummer characters along positive roots of l, ml respectively (§5.9).

Proof. Let t_{ml} be the associated parameter "t" for the cover $E^{ml} \setminus E^{ml}[ml]$ (§2.2). Then, near $t_{ml} = 0$, we have

$$\Theta_{l,ml} \sim \begin{cases} \dfrac{\Delta^{l^2}}{l^{12}}(t_{ml}^{12})^{l^2-1} & (l \geq 5), \\ \dfrac{(\eta^8)^9}{3^4}(t_{ml}^4)^8 = \dfrac{\Delta^3}{3^4}(t_{ml}^4)^8 & (l = 3), \\ \dfrac{(\eta^6)^4}{2^3}(t_{ml}^3)^3 = \dfrac{\Delta}{2^3}(t_{ml}^3)^3 & (l = 2), \end{cases} \tag{6.6.2}$$

where $\sim$ means equality 'up to a factor of $1 + O(t_{ml})$'. Since $t_{ml} \sim t/ml$, we may also understand $\sim$ to designate 'up to a factor of $1 + O(t)$' and get

$$\Theta_{l,ml} \sim \frac{\Delta^{l^2} t^{12(l^2-1)}}{l^{12}(ml)^{12(l^2-1)}}, \ \frac{\Delta^3 t^{32}}{3^4(3m)^{32}}, \ \frac{\Delta t^9}{2^3(2m)^9}$$

in the respective cases $l \geq 5, = 3, = 2$. By definition, σ_m keeps $\Theta_{l,ml}^{1/l^k}$ invariant, while $\bar{\sigma}$ acts on its coefficients in the fractional powers of t. Noticing that $t^{1/l^k}|_{\mathfrak{a}_z} = \zeta_{l^k}^{-1} t^{1/l^k}$ in our convention, we obtain when $l \geq 5$,

$$\zeta_{l^k}^{-12(l^2-1)\rho_{ml}(\sigma) - 12\rho_l(\sigma) + l^2\rho_\Delta(\sigma)} \cdot \zeta_{l^k}^{-12(l^2-1)\xi_m} = 1.$$

From this the desired formula follows. By similar arguments for the cases $l = 3, 2$, we also see

$$\xi_m(\sigma) = \begin{cases} \frac{3}{32}\rho_\Delta(\sigma) - \frac{1}{8}\rho_3(\sigma) - \rho_{3m}(\sigma) & (l = 3), \\ \frac{1}{9}\rho_\Delta(\sigma) - \frac{1}{3}\rho_2(\sigma) - \rho_{2m}(\sigma) & (l = 2), \end{cases}$$

both cases of which fit into the same formula as the case $l \geq 5$. □

§6.7. Monodromy permutations of inertia subsets

As explained above, since our $\Theta_{l,ml}$ gives an S-morphism $E_B^{ml} \setminus E_B^{ml}[l] \to \mathbf{G}_{\mathrm{m}}$, the pull-backed scheme Y^{ml,l^k} still has a canonical model over S. In particular, we have an exact sequence

$$1 \to \pi_1(Y_{\bar{b}}^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y) \to \pi_1(Y^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y) \to \pi_1(S, \bar{b}) \to 1 \tag{6.7.1}$$

which is our main working place in this subsection.

We shall consider the set of conjugacy unions of inertia subgroups in $\pi_1(Y_{\bar{b}}^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$ over the missing points $\mathfrak{Q}^{ml,l^k}$ of $Y_{\bar{b}}^{ml,l^k}$ lying on the integral closure X^{ml,l^k} of $E_B^{ml} \setminus E_B^{ml}[l]$ in Y^{ml,l^k} (Definition 6.5.2). Denote, for each $Q \in \mathfrak{Q}^{ml,l^k}$, by $\mathfrak{I}_Q$ the conjugacy union of the inertia subgroups over Q in $\pi_1(Y^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$. We now realize the following twofold actions.

On one hand, the standard generator $\mathbf{z} \in \Pi_{1,1} = \pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ lies in $\pi_1(E_B^{ml} \setminus E_B^{ml}[ml], \overrightarrow{\mathfrak{w}}_{ml})$, which contains $\pi_1(Y_{\bar{b}}^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$ as a normal subgroup. Conjugation by $\mathbf{z}$ induces a permutation of $\bigcup_Q \mathfrak{I}_Q$, hence of $\mathfrak{Q}^{ml,l^k}$.

On the other hand, we also have the conjugate action by a preimage σ_m of σ under the natural surjection $\pi_1(Y^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y) \to \pi_1(S, \bar{b})$. Recall that we have already specified a particular choice of σ_m in §6.6. (However, the induced action on the set $\mathfrak{Q}^{ml,l^k}$ does not depend on the choice of σ_m, as long as it is chosen up to the kernel $\pi_1(Y_{\bar{b}}^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$.)

Note that the point $Q_{u,v}^{ml,l^k}$ determined by the inertia element $\mathbf{z}_{uv}$ (Definition 6.5.2) also lies in $\mathfrak{Q}^{ml,l^k}$. In the following proposition, we examine the above twofold conjugate actions on those inertia subsets including those $\mathbf{z}_{uv}$ with numerical quantities to evaluate distances of permuted points.

Suppose we are given an element $\sigma \in \pi_1(S, \bar{b})$ with $\rho(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ and two pairs of integers $\mathbf{r} = (r_1, r_2)$ and $\mathbf{s} = (s_1, s_2)$ in $\mathbb{Z}^2 \setminus (m\mathbb{Z})^2$ so that $\mathbf{s} \equiv (ar_1 + cr_2, br_1 + dr_2) \bmod m^2 l^k$.

Proposition 6.7.2. *Notations being as above, there is a unique $\nu = \nu_{\mathbf{r},\mathbf{s}}^{ml,l^k} \in \mathbb{Z}_l$ determined modulo l^k by any of the following equivalent conditions:*

(1) *$\sigma_m \mathbf{z}_{\mathbf{r}} \sigma_m^{-1}$ is conjugate to $\mathbf{z}^{-\nu} \mathbf{z}_{\mathbf{s}}^{\chi(\sigma)} \mathbf{z}^{\nu}$ in $\pi_1(Y_{\bar{b}}^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$.*

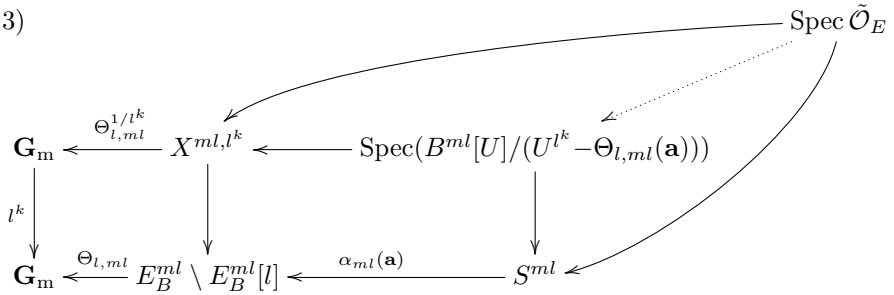
(2) $\dfrac{(\Theta_{l,ml}^{1/l^k}(r_1,r_2))|_{\mathfrak{a}_\sigma}}{\Theta_{l,ml}^{1/l^k}(s_1,s_2)} = \zeta_{l^k}^{-c_l(l^2-1)\nu}$, *where* $c_l = 12, 4, 3$ *according as* $l \geq 5, = 3, = 2$ *respectively.*

(3) $\zeta_{e_l l^k}^{\rho_\Delta(\sigma)} \left(\dfrac{(g_x^{1/l^k})^{c_l l^2}}{(g_{lx}^{1/l^k})^{c_l}} \right)\Big|_{\mathfrak{a}_\sigma} = \zeta_{l^k}^{-c_l(l^2-1)\nu} \left(\dfrac{(g_y^{1/l^k})^{c_l l^2}}{(g_{ly}^{1/l^k})^{c_l}} \right)$, *where* $x = (r_1/ml, r_2/ml)$, $y = (s_1/ml, s_2/ml) \in \mathbb{Q}^2$, c_l *is as above and* $e_l = 12/c_l$.

The remaining part of this subsection is devoted to the proof of this proposition. Recall from §6.5 that we write $P_{\mathbf{a}}$ for the point in $E_B^{ml}[ml] \setminus E_B^{ml}[l]$ lying on the component $\alpha^{ml}(S^{ml})$ over $\bar{b}$. The set $\mathfrak{Q}^{ml,l^k}$ is naturally mapped onto the set $\mathfrak{P}^{ml} := \{P_{\mathbf{a}} \mid \mathbf{a} \in (\mathbb{Z}/ml\mathbb{Z})_0^2\}$. Since the cover $(Y^{ml,l^k} \to E_B^{ml} \setminus \{O\})_{\bar{b}}$ is totally ramified in $\langle \mathbf{z} \rangle$, the conjugate action by $\mathbf{z}$ gives a transitive orbit in $\mathfrak{Q}^{ml,l^k}$ as the fiber set at each $P_{\mathbf{a}}$. Since the action of $\pi_1(S, \bar{b})$ on $\mathfrak{P}^{ml}$ is given by the matrix ρ^{ml} on the index set, the existence of ν and its uniqueness modulo l^k as in (1) is easy to see. To see the coincidence of ν given by the conditions (1) and (2) needs more arguments.

Before going further, it is convenient for us to introduce a labeling of the set $\mathfrak{Q}^{ml,l^k}$. Recall first that X^{ml,l^k} is the integral closure of $E_B^{ml} \setminus E_B^{ml}[l]$ in Y^{ml,l^k} (Definition 6.5.2). The structure ring of X^{ml,l^k} is a subring of that of Y^{ml,l^k}; both are dominated by $\mathrm{Spec}(\tilde{\mathcal{O}}_E) = \widetilde{E_0}$. The partial compactifications $E_B^{ml} \setminus E_B^{ml}[l] \supset E_0^{ml} = E_B^{ml} \setminus E_B^{ml}[ml]$ and $X^{ml,l^k} \supset Y^{ml,l^k}$ give rise to the sequence $\mathrm{Spec}(\tilde{\mathcal{O}}_E) = \widetilde{E_0} \to Y^{ml,l^k} \hookrightarrow X^{ml,l^k} \to E_B^{ml} \setminus E_B^{ml}[l] \to S^{ml}$ equipped with the set of sections $\alpha_{ml}(\mathbf{a}) : S^{ml} \to E_B^{ml} \setminus E_B^{ml}[l]$ ($\mathbf{a} \in (\mathbb{Z}/ml\mathbb{Z})_0^2$). Each section $\alpha_{ml}(\mathbf{a})$ fits in the following cartesian diagram yielding a canonical morphism $\mathrm{Spec}(\tilde{\mathcal{O}}_E) \to S^{ml}(\Theta_{l,ml}^{1/l^k}(\mathbf{a}))$:

(6.7.3)



Namely, we have a specific element $\Theta_{l,ml}^{1/l^k}(\mathbf{a}) \in (B^{\mathrm{ur}})^\times$ as the image of U in $B^{\mathrm{ur}} \subset \tilde{\mathcal{O}}_E$. Now, the carriers of the points $\mathfrak{Q}^{ml,l^k}$ as schemes over $S^{\mathrm{ur}} = \mathrm{Spec}(B^{\mathrm{ur}})$ are of the form

$$(6.7.4)\qquad (X^{ml,l^k}-Y^{ml,l^k})\otimes_B B^{\mathrm{ur}} = \bigsqcup_{\mathbf{a}\in(\mathbb{Z}/ml\mathbb{Z})_0^2} \mathrm{Spec}(B^{\mathrm{ur}}[U]/(U^{l^k}-\Theta_l(\mathbf{a}))) = \bigsqcup_{\mathbf{a}\in(\mathbb{Z}/ml\mathbb{Z})_0^2}\ \bigsqcup_{b=0}^{l^k-1} \mathrm{Spec}(B^{\mathrm{ur}}[U]/(U-\zeta_{l^k}^b\Theta_l(\mathbf{a})^{1/l^k})).$$

Each (physical) component $\mathrm{Spec}(B^{\mathrm{ur}}[U]/(U-\zeta_{l^k}^b\Theta_l(\mathbf{a})^{1/l^k}))$ carries a unique missing point $Q_{\mathbf{a},b}$ ($\mathbf{a}\in(\mathbb{Z}/ml\mathbb{Z})_0^2$, $b\in[0,l^k-1]$) on the algebraic curve $X_{\bar b}^{ml,l^k}$. Thus, we have obtained natural labelings of our sets:

$$(6.7.5)\qquad \begin{array}{ccccc} \mathfrak{Q}^{ml,l^k} & = & (X^{ml,l^k}-Y^{ml,l^k})_{\bar b} & = & \{Q_{\mathbf{a},b}\mid \mathbf{a}\in(\mathbb{Z}/ml\mathbb{Z})_0^2,\ b\in[0,l^k-1]\} \\ \downarrow & & \downarrow & & \downarrow \\ \mathfrak{P}^{ml} & = & (E_B^{ml}[ml]-E_B^{ml}[l])_{\bar b} & = & \{P_{\mathbf{a}}\mid \mathbf{a}\in(\mathbb{Z}/ml\mathbb{Z})_0^2\} \end{array}$$

Remark 6.7.6. From a real analytic argument similar to the proof of Lemma 6.5.4, one would also see that $\Theta_{l,ml}^{1/l^k}(r_1,r_2)=\Theta_{l,ml}^{1/l^k}(\mathbf{a})$ in $(S^{\mathrm{ur}})^\times$ at least for $(r_1,r_2)\in[0,m)^2$. This observation, however, will not be used in our proof of Theorem 6.2.1.

Now, we shall interpret the above two group-theoretic conjugate actions by $\mathbf{z}\in\Pi_{1,1}$ and $\sigma_m\in\pi_1(S,\bar b)$ on $\mathfrak{Q}^{ml,l^k}$ in geometric terms.

On one hand, the standard generator $\mathbf{z}\in\Pi_{1,1}=\pi_1(E\setminus\{O\},\overrightarrow{\mathfrak{w}}_{\bar b})$ lies in $\pi_1(E_B^{ml}\setminus E_B^{ml}[ml],\overrightarrow{\mathfrak{w}}_{ml})$ and also induces an automorphism $\mathfrak{a}_{\mathbf{z}}$ of $Y^{ml,l^k}\otimes_B B^{\mathrm{ur}}$, which extends naturally to an automorphism $\overline{\mathfrak{a}_{\mathbf{z}}}$ of $X^{ml,l^k}\otimes_B B^{\mathrm{ur}}$. Denote by the same symbol $\overline{\mathfrak{a}_{\mathbf{z}}}$ the induced permutations of the points $\mathfrak{Q}^{ml,l^k}:=(X^{ml,l^k}-Y^{ml,l^k})_{\bar b}$.

On the other hand, $\mathfrak{Q}^{ml,l^k}$ is also regarded as a set of B^{ur}-rational points on $(X^{ml,l^k}-Y^{ml,l^k})/B$ on which there is a natural monodromy action of $\pi_1(S,\bar b)$. We simply write it $\sigma_m(*)$, as it corresponds to a preimage σ_m of σ under the natural surjection $\pi_1(Y^{ml,l^k},\overrightarrow{\mathfrak{w}}_Y)\to\pi_1(S,\bar b)$. In view of diagram (6.7.4), this action is given by the left action $(*)|_{\mathfrak{a}_\sigma}$ in the value ring B^{ur} on the images of U from the carrier schemes for points in $\mathfrak{Q}^{ml,l^k}$.

Thus, the coincidence of the quantity ν of (1) and (2) amounts to the following

Lemma 6.7.7. *For each $Q\in\mathfrak{Q}^{ml,l^k}$, $\mathfrak{I}_{\overline{\mathfrak{a}_{\mathbf{z}}}^{\nu}(Q)}=\mathbf{z}^{-\nu}\mathfrak{I}_Q\mathbf{z}^{\nu}$.*

Proof. This is only a general theory (but needs a careful treatment of conventions on path compositions). Consider the pointed universal etale cover $\tilde Y$ of $E_{\bar b}^{ml}\setminus E_{\bar b}^{ml}[ml]$ dominating $Y_{\bar b}^{ml,l^k}$ and partial compactification $\tilde X$ as the projective limit of the integral closures of finite layers over $E_{\bar b}^{ml}\setminus E_{\bar b}^{ml}[l]$. The profinite set $\tilde\Omega:=\tilde X-\tilde Y$ is regarded as the set of cusps. Then, for each $\gamma\in\pi_1(E_{\bar b}^{ml}\setminus E_{\bar b}^{ml}[ml],\overrightarrow{\mathfrak{w}}_{ml})$,

let $\overline{\mathfrak{a}_\gamma}$ denote the restriction to $\tilde{\Omega}$ of the naturally extended action on $\tilde{X}$ from $\mathfrak{a}_\gamma \in \mathrm{Aut}(\tilde{Y})$. If γ is contained in the inertia group for $Q \in \tilde{\Omega}$, i.e., $\overline{\mathfrak{a}_\gamma}(Q) = Q$, then it follows from our convention (cf. (2.7.1)) that

$$\overline{\mathfrak{a}_{\mathbf{z}^{-1}\gamma\mathbf{z}}}(\overline{\mathfrak{a}_\mathbf{z}}(Q)) = \overline{\mathfrak{a}_{\mathbf{z}\cdot\mathbf{z}^{-1}\gamma\mathbf{z}}}(Q) = \overline{\mathfrak{a}_{\gamma\mathbf{z}}}(Q) = \overline{\mathfrak{a}_\mathbf{z}}(\overline{\mathfrak{a}_\gamma}(Q)) = \overline{\mathfrak{a}_\mathbf{z}}(Q).$$

The statement is only a reflection of this computation. □

Thus, we established the existence of $\nu = \nu^{ml,l^k}_{\mathbf{r},\mathbf{s}}$ and their coincidence in the conditions (1) and (2). The condition (3) is only a restatement of (2) in view of Lemma 6.5.4 and the Kummer property

$$(\eta^{2c_l})^{1/l^k}|_{\mathfrak{a}_\sigma} = (\eta^{2c_l})^{1/l^k} \cdot \zeta_{e_l\, l^k}^{\rho_\Delta(\sigma)}. \tag{6.7.8}$$

Thus, the proof of Proposition 6.7.2 is complete. □

§6.8. Count character for winding numbers

Now, recalling that $Y_{\bar{b}}^{ml,l^\infty}$ is given as the Kummer cover over $E_{\bar{b}}^{ml} \setminus E_{\bar{b}}^{ml}[ml]$, we have the exact sequence

$$1 \to \pi_1(Y_{\bar{b}}^{ml,l^\infty}, \overrightarrow{\mathfrak{w}}_Y) \to \pi_1(E_{\bar{b}}^{ml} \setminus E_{\bar{b}}^{ml}[ml], \overrightarrow{\mathfrak{w}}_{ml}) \xrightarrow{\vartheta_{ml}} \mathbb{Z}_l \to 1,$$

where $c_l \cdot \vartheta_{ml} : \pi_1(E_{\bar{b}}^{ml} \setminus E_{\bar{b}}^{ml}[ml], \overrightarrow{\mathfrak{w}}_{ml}) \to \mathbb{Z}_l$ (with $c_l = 12, 4, 3$ according to $l \geq 5, = 3, = 2$ respectively) counts winding numbers of the images of paths by $\Theta_{l,ml}$ around zero. Now, the fundamental group $\pi_1(E_{\bar{b}}^{ml} \setminus E_{\bar{b}}^{ml}[ml], \overrightarrow{\mathfrak{w}}_{ml})$ is normally generated by $\mathbf{x}_1^{ml}$, $\mathbf{x}_2^{ml}$ and the $\mathbf{z}_\mathbf{r}$ ($\mathbf{r} \in [0, ml)^2$) as a subgroup of $\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}) = \langle \mathbf{x}_1, \mathbf{x}_2, \mathbf{z} \mid [\mathbf{x}_1, \mathbf{x}_2]\mathbf{z} = 1 \rangle$. Indeed, as observed in [N95, (2.6)], we may characterize ϑ_{ml} as follows:

Lemma 6.8.1. *The above homomorphism ϑ_{ml} is given by*

(i) $$\vartheta_{ml}(\mathbf{x}_1^{ml}) = -l(l-1)/2,$$

(ii) $$\vartheta_{ml}(\mathbf{x}_2^{ml}) = l(l-1)/2,$$

(iii) $$\vartheta_{ml}(\mathbf{z}_\mathbf{r}) = \begin{cases} (l^2-1), & \mathbf{r} \in ml\mathbb{Z}^2, \\ -1, & \mathbf{r} \in m\mathbb{Z}^2 \setminus ml\mathbb{Z}^2, \\ 0, & \textit{otherwise}. \end{cases}$$

Proof. It suffices to show the lemma for a complex elliptic curve $E(\mathbb{C}) = \mathbb{C}/\mathfrak{L}$ given by a lattice $\mathfrak{L} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ ($\tau = \omega_1/\omega_2 \in \mathfrak{H}$) with a tangential base point of $E \setminus \{O\}$ represented by (the image of) a small arrow $\overrightarrow{\mathfrak{w}} = \overrightarrow{(0, \varepsilon\omega_2)} \subset \mathbb{C}$ ($0 < \varepsilon \ll 1$). We take the generators $\mathbf{x}_1, \mathbf{x}_2, \mathbf{z}$ based at $\overrightarrow{\mathfrak{w}}$ to be (the images in $\mathbb{C}/\mathfrak{L}$ of) certain standard paths (along $\mathbb{R}\omega_1 \cup \mathbb{R}\omega_2 \cup \{\omega + e^{2\pi i t}\overrightarrow{\mathfrak{w}} | \omega \in \mathfrak{L}, 0 \leq t \leq 1\}$)

illustrated by: $\mathbf{x}_1 : \overrightarrow{\mathfrak{w}} \to \overrightarrow{\mathfrak{w}} - \omega_1$, $\mathbf{x}_2 : e^{\pi i t}\overrightarrow{\mathfrak{w}}(t : 0 \to 1) \to \overrightarrow{\mathfrak{w}} - \omega_2$ and $\mathbf{z} : e^{2\pi i t}\overrightarrow{\mathfrak{w}}$ $(t : 0 \to 1)$ respectively (and their shifts by the elements of $\mathfrak{L}$). Observe then that the composition $\mathbf{x}_1\mathbf{x}_2\mathbf{x}_1^{-1}\mathbf{x}_2^{-1}\mathbf{z}$ is contractible on $\mathbb{C} \setminus \mathfrak{L}$, hence gives the standard relation $[\mathbf{x}_1, \mathbf{x}_2]\mathbf{z} = 1$ in $\pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}})$. Now, the function

$$f(z) = \prod_{P \in (m\mathfrak{L}/ml\mathfrak{L}) - \{O\}} \frac{1}{(\wp(z, ml\mathfrak{L}) - \wp(P, ml\mathfrak{L}))^6}$$

is a constant multiple of $\Theta_{l,ml}^{12/c_l}$ whose winding number is given by $12\vartheta_{ml}(\gamma) = \frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}dz$ for any path γ connecting two points in $\mathfrak{L} + \overrightarrow{\mathfrak{w}}$.

(iii) follows immediately from the fact that $f(z)$ has only zeros of order $12(l^2-1)$ at the points in $ml\mathfrak{L}$ and only poles of order 12 at the points in $m\mathfrak{L} \setminus ml\mathfrak{L}$.

To show (i), (ii), we shall consider integration surrounding a side of the ml-magnified fundamental parallelogram. Let δ denote the semicircle path $e^{\pi i t}\overrightarrow{\mathfrak{w}}$ $(t : 0 \to 1)$ and its shifts with $\mathfrak{L}$, and consider the loop $\mathbf{x}_1^{ml}\delta(-\mathbf{x}_1)^{ml}\delta^{-1}$ which negatively surrounds one zero and $l-1$ poles. Since $f(z) = f(-z)$, the integral of $f'(z)/f(z)$ along $\mathbf{x}_1$ is the same as that along $-\mathbf{x}_1$, while the periodicity of $f(z)$ implies the integral along δ and that along δ^{-1} $(= \delta^{-1}$ at $-ml\omega_1)$ cancel with each other. Hence, $12(l^2-1) - 12(l-1) = -2 \cdot 12\vartheta(\mathbf{x}_1^{ml})$, which implies (i). Similarly, we obtain (ii) by considering integration of $f'(z)/f(z)$ along $\mathbf{x}_2^{ml}\delta(-\mathbf{x}_2)^{ml}\delta^{-1}$ which positively surrounds one zero and $l-1$ poles. □

Before proceeding with the proof of Theorem 6.2.1, we shall present an immediate application of ϑ_{ml} concerning the points on Y^{ml,l^k} determined by the inertia elements $\mathbf{z}_{uv} = (\mathbf{x}_1^u\mathbf{x}_2^v)^{-1}\mathbf{z}(\mathbf{x}_1^u\mathbf{x}_2^v)$ $((u,v) \in \hat{\mathbb{Z}}^2)$.

We note that this abelian quotient of $\pi_1(E_{\bar{b}}^{ml} \setminus E_{\bar{b}}^{ml}[ml], \overrightarrow{\mathfrak{w}}_{ml})$ is generally not invariant under the conjugate action of $\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$, in particular we do not expect a formula like $\vartheta_{ml}(x\mathbf{z}x^{-1}) = \vartheta_{ml}(\mathbf{z})$.

If $(u,v), (u',v') \in \hat{\mathbb{Z}}^2$ satisfy the congruence $(u,v) \equiv (u',v') \bmod ml$, then the quotient of $\mathbf{x}_1^u\mathbf{x}_2^v$ by $\mathbf{x}_1^{u'}\mathbf{x}_2^{v'}$ lies in $\pi_1(E_{\bar{b}}^{ml} \setminus E_{\bar{b}}^{ml}[ml], \overrightarrow{\mathfrak{w}}_{ml})$. The following lemma gives an estimate of its value via ϑ_{ml}.

Lemma 6.8.2. *If $(u,v), (u',v') \in \hat{\mathbb{Z}}^2$ satisfy $(u,v) \equiv (u',v') \bmod ml^{k+1}$, then $\vartheta_{ml}((\mathbf{x}_1^{u'}\mathbf{x}_2^{v'})^{-1}(\mathbf{x}_1^u\mathbf{x}_2^v))$ and $\vartheta_{ml}((\mathbf{x}_1^{u'}\mathbf{x}_2^{v'})(\mathbf{x}_1^u\mathbf{x}_2^v)^{-1})$ are divisible by l^k. If moreover $l \geq 3$, then the assumption may be replaced by $(u,v) \equiv (u',v') \bmod ml^k$.*

Proof. By assumption, we may write $u' = u + \varepsilon$, $v' = v + \delta$ with $\varepsilon = ml^{k+1}\alpha$, $\delta = ml^{k+1}\beta$ for some $\alpha, \beta \in \hat{\mathbb{Z}}$. We shall first prove

$$\vartheta_{ml}(\mathbf{x}_2^{-v'}\mathbf{x}_1^{-u'}\mathbf{x}_1^u\mathbf{x}_2^v) = \vartheta_{ml}((\mathbf{x}_2^{-\delta}\mathbf{x}_1^{-\varepsilon}) \cdot (\mathbf{x}_1^{\varepsilon}\mathbf{x}_2^{-v}\mathbf{x}_1^{-\varepsilon}\mathbf{x}_2^v)) \equiv 0 \bmod l^k.$$

One immediately sees that $\vartheta_{ml}(\mathbf{x}_2^{-\delta}) = \beta l^{k+1}\frac{1-l}{2}$, $\vartheta_{ml}(\mathbf{x}_1^{-\varepsilon}) = \alpha l^{k+1}\frac{l-1}{2}$, each of which vanishes modulo l^k. ($(*)$: When $l \geq 3$, even modulo l^{k+1}.) For the second factor, using free differential calculus, we have in $\Pi'_{1,1}/\Pi''_{1,1}$,

$$\mathbf{x}_1^{\varepsilon}\mathbf{x}_2^{-v}\mathbf{x}_1^{-\varepsilon}\mathbf{x}_2^{v} \equiv -\left(\frac{\bar{\mathbf{x}}_1^{\varepsilon}-1}{\bar{\mathbf{x}}_1-1}\cdot\frac{\bar{\mathbf{x}}_2^{-v}-1}{\bar{\mathbf{x}}_2-1}\right)\cdot\mathbf{z}.$$

Write the RHS as $\mu\cdot\mathbf{z}$ ($\mu \in \hat{\mathbb{Z}}[[\Pi_{1,1}^{\mathrm{ab}}]]$), and consider μ as a measure on $\hat{\mathbb{Z}}^2$ of separate variable type; we may then compute

$$\begin{aligned}\vartheta_{ml}(\mathbf{x}_1^{\varepsilon}\mathbf{x}_2^{-v}\mathbf{x}_1^{-\varepsilon}\mathbf{x}_2^{v}) = &\int_{m\hat{\mathbb{Z}}} d\left(\frac{\bar{\mathbf{x}}_1^{\varepsilon}-1}{\bar{\mathbf{x}}_1-1}\right)\int_{m\hat{\mathbb{Z}}} d\left(\frac{\bar{\mathbf{x}}_2^{-v}-1}{\bar{\mathbf{x}}_2-1}\right)\\ &- l^2\int_{ml\hat{\mathbb{Z}}} d\left(\frac{\bar{\mathbf{x}}_1^{\varepsilon}-1}{\bar{\mathbf{x}}_1-1}\right)\int_{ml\hat{\mathbb{Z}}} d\left(\frac{\bar{\mathbf{x}}_2^{-v}-1}{\bar{\mathbf{x}}_2-1}\right).\end{aligned}$$

Then, taking into account that $\varepsilon = ml^{k+1}\alpha$, we see that the first factors of the above two terms vanish modulo l^{k+1}, $l^2\cdot l^k$ respectively. When $l \geq 3$, the above remark $(*)$ gives the refined implication as in the statement.

As for $\vartheta_{ml}((\mathbf{x}_1^{u'}\mathbf{x}_2^{v'})(\mathbf{x}_1^{u}\mathbf{x}_2^{v})^{-1}) = \vartheta_{ml}(\mathbf{x}_1^{\varepsilon}\mathbf{x}_2^{\delta}) + \vartheta_{ml}(\mathbf{x}_2^{-\delta}\mathbf{x}_1^{u}\mathbf{x}_2^{\delta}\mathbf{x}_1^{-u})$, we may argue in a similar way. This completes the proof. □

Corollary 6.8.3. *If $(u,v),(u',v') \in \hat{\mathbb{Z}}^2 \setminus (m\hat{\mathbb{Z}})^2$ satisfy the congruence $(u,v) \equiv (u',v') \bmod ml^{k+1}$, then $\mathbf{z}_{uv}$ and $\mathbf{z}_{u'v'}$ determine the same cusp on Y^{ml,l^k}. If $l \geq 3$, then the assumption may be replaced by $(u,v) \equiv (u',v') \bmod ml^k$.*

Proof. To prove the proposition in this case, it suffices to show that the difference of conjugating factors for $\mathbf{z}_{uv}$ and $\mathbf{z}_{u'v'}$ to $\mathbf{z}$ is mapped to $l^k\mathbb{Z}_l$ by ϑ_{ml}. This is nothing but the statement of the above lemma. □

Consider the above corollary when $l \geq 3$ and $k = 1$. Then all inertia elements $\mathbf{z}_{uv}$ with a fixed residue class of (u,v) modulo ml give the same cusp in $\mathfrak{Q}^{ml,l}$. From this remark, one should notice in particular that the points of the form Q_{uv}^{ml,l^k} with $(u,v) \in \hat{\mathbb{Z}}^2 \setminus (m\hat{\mathbb{Z}})^2$ do not exhaust all cusps in $\mathfrak{Q}^{ml,l^k}$.

§6.9. End of the proof of Theorem 6.2.1

Given a pair $(u,v) \in (\hat{\mathbb{Z}})^2 \setminus (m\hat{\mathbb{Z}})^2$, pick $(r_1,r_2) \in \mathbb{Z}^2 \setminus (m\mathbb{Z})^2$ such that $(r_1,r_2) \equiv (u,v) \bmod ml^{2n+1}$. Then, by Lemma 6.8.2, the cusps determined by $\mathbf{z}_{uv}$ and $\mathbf{z}_{\mathbf{r}}$ are the same on $Y^{ml,l^{2n}}$. Set $x = (r_1/m, r_2/m)$, $y = (s_1/m, s_2/m)$, so that $x \to y$ is $\rho(\sigma)$-admissible at level m modulo m^2l^{2n} (Def. 5.10.3). Then $l^{-1}x \to l^{-1}y$ is $\rho(\sigma)$-admissible at level ml modulo m^2l^{2n-2} (in fact, still modulo m^2l^{2n}). Proposition 6.7.2(3) then implies

Corollary 6.9.1. *Notations being as above, in particular e_l designating $1, 3, 4$ according as $l \geq 5, =3, =2$ respectively, we have*

$$12(l^2-1)\nu_{\mathbf{r},\mathbf{s}}^{ml,l^{2n}}(\sigma) \equiv \kappa_{x\to y}^{m,m^2l^{2n}}(\sigma) - l^2\kappa_{l^{-1}x\to l^{-1}y}^{ml,m^2l^{2n-2}}(\sigma) - \rho_\Delta(\sigma) \bmod e_l \cdot l^{2n}.$$

Therefore, the following congruence holds with a uniquely determined congruence class on the right hand side:

$$\nu_{\mathbf{r},\mathbf{s}}^{ml,l^{2n}}(\sigma) \equiv \frac{\kappa_{x\to y}^{m,m^2l^{2n}}(\sigma) - l^2\kappa_{l^{-1}x\to l^{-1}y}^{ml,m^2l^{2n-2}}(\sigma) - \rho_\Delta(\sigma)}{12(l^2-1)} \bmod l^{2n}. \qquad \square$$

We now enter the heart of our proof of Theorem 6.2.1. Let $\mathbf{t} = (t_1, t_2) \in \hat{\mathbb{Z}}^2$ be such that $t_1 = a(\sigma)r_1 + c(\sigma)r_2$, $t_2 = b(\sigma)r_1 + d(\sigma)r_2$ so that $\mathbf{t} \equiv \mathbf{s} \bmod m^2l^{2n}e_l$, and put $\mathbf{x}_\mathbf{t} = \mathbf{x}_2^{-t_2}\mathbf{x}_1^{-t_1}$, $\mathbf{x}_\mathbf{s} = \mathbf{x}_2^{-s_2}\mathbf{x}_1^{-s_1}$ so that $\mathbf{z}_\mathbf{t} = \mathbf{x}_\mathbf{t}\mathbf{z}\mathbf{x}_\mathbf{t}^{-1}$, $\mathbf{z}_\mathbf{s} = \mathbf{x}_\mathbf{s}\mathbf{z}\mathbf{x}_\mathbf{s}^{-1}$. Then we calculate

$$\begin{aligned}(6.9.2)\qquad \sigma_m\mathbf{z}_\mathbf{r}\sigma_m^{-1} &= \mathbf{z}^{\xi_m(\sigma)}\bar{\sigma}\mathbf{z}_\mathbf{r}\bar{\sigma}^{-1}\mathbf{z}^{-\xi_m(\sigma)}\\ &= \mathbf{z}^{\xi_m(\sigma)}\mathcal{S}_\mathbf{r}(\sigma)(\mathbf{x}_\mathbf{t}\mathbf{x}_\mathbf{s}^{-1})\mathbf{z}_\mathbf{s}^{\chi(\sigma)}(\mathbf{x}_\mathbf{t}\mathbf{x}_{\mathbf{s}^{-1}})^{-1}\mathcal{S}_\mathbf{r}(\sigma)^{-1}\mathbf{z}^{-\xi_m(\sigma)}\\ &= \mathbf{z}^{\xi_m(\sigma)}w\{G_\mathbf{r}(\sigma)\cdot\mathbf{z}\}(\mathbf{x}_\mathbf{t}\mathbf{x}_\mathbf{s}^{-1})\mathbf{z}_\mathbf{s}^{\chi(\sigma)}(\mathbf{x}_\mathbf{s}\mathbf{x}_\mathbf{t}^{-1})^{-1}\{G_\mathbf{r}(\sigma)\cdot\mathbf{z}\}^{-1}w^{-1}\mathbf{z}^{-\xi_m(\sigma)}\end{aligned}$$

for some $w \in \Pi''_{1,1}$. By Corollary 6.8.3, the inertia elements $\mathbf{z}_\mathbf{t}$ and $\mathbf{z}_\mathbf{s}$ determine the same cusp in $Y_{\bar{b}}^{ml^{2n}}$. Therefore, by Proposition 6.7.2(1), there exists some $h \in \pi_1(Y_{\bar{b}}^{ml,l^{2n}}, \overrightarrow{\mathfrak{w}}_Y)$ such that $\sigma_m\mathbf{z}_\mathbf{r}\sigma_m^{-1}$ is of the form $h\mathbf{z}^{-\nu}\mathbf{z}_\mathbf{s}^{\chi(\sigma)}\mathbf{z}^\nu h^{-1}$ with $\nu = \nu_{\mathbf{r},\mathbf{s}}^{ml,l^{2n}}(\sigma)$. Since $\langle\mathbf{z}_\mathbf{r}\rangle$ is self-centralizing in $\pi_1(E_{\bar{b}}\setminus\{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ and since $\pi_1(Y_{\bar{b}}^{ml,l^\infty}, \overrightarrow{\mathfrak{w}}_Y) \supset \langle\mathbf{z}_\mathbf{r}, \Pi''_{1,1}\rangle$, we see that $\nu = \nu_{\mathbf{r},\mathbf{s}}^{ml,l^{2n}}(\sigma)$ satisfies

$$(6.9.3)\qquad \mathbf{z}^{-\nu} \equiv \mathbf{z}^{\xi_m(\sigma)}\{G_\mathbf{r}(\sigma)\cdot\mathbf{z}\}(\mathbf{x}_\mathbf{t}\mathbf{x}_\mathbf{s}^{-1}) \bmod \pi_1(Y_{\bar{b}}^{ml,l^{2n}}, \overrightarrow{\mathfrak{w}}_Y).$$

Then, apply $\vartheta_{ml} \bmod l^{2n}$ to both sides of (6.9.3). Noticing that $\vartheta_{ml}(\mathbf{x}_\mathbf{t}\mathbf{x}_\mathbf{s}^{-1}) \equiv 0 \bmod l^{2n}$ by Lemma 6.8.2, we find

$$\begin{aligned}(6.9.4)\qquad (1-l^2)\nu_{\mathbf{r},\mathbf{s}}^{ml,l^{2n}}(\sigma) &\equiv \vartheta_{ml}\big(\mathbf{z}^{\xi_m(\sigma)}(G_{r_1,r_2}(\sigma)\cdot\mathbf{z})(\mathbf{x}_\mathbf{t}\mathbf{x}_\mathbf{s}^{-1})\big)\\ &= \vartheta_{ml}(\{\xi_m(\sigma) + G_{r_1,r_2}(\sigma)\}\cdot\mathbf{z}) + \vartheta_{ml}(\mathbf{x}_\mathbf{t}\mathbf{x}_\mathbf{s}^{-1})\\ &\equiv \xi_m(\sigma)(l^2-1) + l^2\int_{(ml\mathbb{Z}_\mathcal{C})^2} dG_{r_1,r_2}(\sigma) - \int_{(m\mathbb{Z}_\mathcal{C})^2} dG_{r_1,r_2}(\sigma)\\ &= \xi_m(\sigma)(l^2-1) + l^2\,\mathbb{E}_{ml}(\sigma; r_1, r_2) - \mathbb{E}_m(\sigma; r_1, r_2),\end{aligned}$$

where the congruence is taken modulo l^{2n}.

Now, let us apply the above (6.9.4) by replacing m, l^{2n} by ml^i, l^{2n-2i} ($i = 0, 1, \dots$) respectively. Then we obtain the following congruence modulo l^{2n-2i}:

$$(6.9.5)_i \qquad (1-l^2)\nu_{\mathbf{r},\mathbf{s}}^{ml^{i+1},l^{2n-2i}}(\sigma) \equiv (l^2-1)\xi_{ml^i}(\sigma) + l^2\mathbb{E}_{ml^{1+i}}(\sigma; r_1, r_2) - \mathbb{E}_{ml^i}(\sigma; r_1, r_2).$$

Taking $\sum_{i\geq 0} l^{2i} \times (6.9.5)_i$, we obtain

$$\mathbb{E}_m(\sigma; r_1, r_2) \equiv (l^2-1)\sum_{i=0}^{\infty} l^{2i}\{\xi_{ml^i}(\sigma) + \nu_{\mathbf{r},\mathbf{s}}^{ml^{i+1},l^{2n-2i}}(\sigma)\} \bmod l^{2n}, \tag{6.9.6}$$

where $\sum_{i=0}^{\infty}$ is essentially a finite sum. Combining Lemma 6.6.1 and Corollary 6.9.1, we compute, for $0 \leq i \leq n-1$,

$$\xi_{ml^i}(\sigma) + \nu_{\mathbf{r},\mathbf{s}}^{ml^{i+1},l^{2n-2i}}(\sigma) = \frac{\rho_\Delta(\sigma)}{12} - \frac{\rho_l(\sigma)}{l^2-1} - \rho_{ml^{i+1}} + \frac{1}{12(l^2-1)}\big(\kappa_{l^{-i}x\to l^{-i}y}^{ml^i,m^2l^{2n-2i}}(\sigma) - l^2\kappa_{l^{-i-1}x\to l^{-i-1}}^{ml^{i+1},m^2l^{2n-2i-2}}(\sigma)\big).$$

Noting that $\sum_{i=0}^{\infty}(i+1)l^{2i} = (1-l^2)^{-2}$ in $\mathbb{Z}_l$, we finally obtain the fundamental equation

$$\mathbb{E}_m(\sigma; r_1, r_2) \equiv \tfrac{1}{12}\kappa_{x\to y}^{m,m^2l^{2n}}(\sigma) - \tfrac{1}{12}\rho_\Delta(\sigma) + \rho_m(\sigma) \bmod l^{2n}. \tag{6.9.7}$$

This completes the proof of Theorem 6.2.1. □

Corollary 6.9.8. *Let $M \in |\mathcal{C}|$ and let $\varepsilon = 0, 1$ according as $2 \nmid M$, $2|M$ respectively. Then the value $\mathbb{E}_m^{\mathcal{C}}(\sigma; u, v)$ modulo M^2 is periodic in (u, v) modulo $mM^2 2^\varepsilon$. Consequently, for $\sigma \in \pi_1(S, \bar{b})$, the values $\mathbb{E}_m(\sigma; u, v)$ mod M^2 at $(u, v) \in \mathbb{Z}_{\mathcal{C}}^2$ determine a unique element of the finite group ring $(\mathbb{Z}/M^2\mathbb{Z})[(\mathbb{Z}/mM^2 2^\varepsilon\mathbb{Z})^2]$.*

Note. From numerical evidence (as in §7), one could immediately observe possibilities to improve the above corollary by refining modulus and period more generally (e.g., not only for squares $M^2 \in |\mathcal{C}|$; cf. Remark 3.4.3 and [N12]).

Proof. Suppose first that $(u, v), (u', v') \in \hat{\mathbb{Z}}^2 \backslash (m\hat{\mathbb{Z}})^2$ satisfy the congruence $(u, v) \equiv (u', v') \bmod mM^2 2^\varepsilon$. Then the congruence $\mathbb{E}_m^{\mathcal{C}}(\sigma; u, v) \equiv \mathbb{E}_m^{\mathcal{C}}(\sigma; u', v') \bmod M^2$ follows from the congruence formula (6.9.4) and the determination of $\nu_{\mathbf{r},\mathbf{s}}^{ml,l^n}$ through the cuspidal point determined by $\mathbf{z}_{uv}$ according to Corollary 6.8.3. Suppose next that $(u, v), (u', v') \in (m\hat{\mathbb{Z}})^2$. Then Proposition 3.4.8 reduces the desired congruence to the above case and the obvious congruence $u - u' \equiv v - v' \equiv 0 \bmod M^2 2^\varepsilon$. □

§6.10. Explicit formula for $\mathcal{E}^{\mathcal{C}}_{\sigma}$

Let $\mathcal{C}$ be a full class of finite groups. We shall study behaviors of $\mathbb{E}^{\mathcal{C}}_m(\sigma)$ and $\mathcal{E}^{\mathcal{C}}_{\sigma}$ introduced in §3.6 on the pro-$\mathcal{C}$ congruence kernel $\pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})$. As $\rho^{\mathcal{C}}(\sigma) = 1$ for $\sigma \in \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})$, for every $x \in (\frac{1}{m}\mathbb{Z})^2$, the quantity $\kappa^{m,m^2\infty}_{x\to x,\mathcal{C}}(\sigma) := \kappa^{m,m^2M}_{x\to x,\mathcal{C}}(\sigma)$ is well defined (independent of $M \in |\mathcal{C}|$). Recalling that the structure ring $B^{\mathcal{C}}$ of $S^{\mathcal{C}}$ contains all $\mathcal{C}$-power roots of unity, we find that $\kappa^{m,m^2\infty}_{x\to x,\mathcal{C}} : \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}}) \to \mathbb{Z}_{\mathcal{C}}$ is defined by the ordinary Kummer property

$$\theta_x^{1/N}|_{\mathfrak{a}_\sigma} = \theta_x^{1/N} \cdot \zeta_N^{\kappa^{m,m^2\infty}_{x\to x}(\sigma)} \qquad (\sigma \in \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}}),\ N \in |\mathcal{C}|), \tag{6.10.1}$$

and depends only on the class of x in $\mathbb{Q}^2/\mathbb{Z}^2$. Here, note also that, no matter whether 2 or 3 belongs to $|\mathcal{C}|$, the above quantity $\kappa^{m,m^2\infty}_{x\to x}(\sigma) \in \mathbb{Z}_{\mathcal{C}}$ for $\sigma \in \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})$ is divisible by 12 by Proposition 4.2.1. Define now $\boldsymbol{\mu}^{\mathcal{C}}_m(\sigma) \in \mathbb{Z}_{\mathcal{C}}[(\mathbb{Z}/m\mathbb{Z})^2]$ (with notations of §3.6) by

$$\boldsymbol{\mu}^{\mathcal{C}}_m(\sigma)\ \Big(= \sum_{\mathbf{a}\in(\mathbb{Z}/m\mathbb{Z})^2} \boldsymbol{\mu}^{\mathcal{C}}_m(\sigma,\mathbf{a})\mathbf{e}_{\mathbf{a}}\Big) := -\rho_m(\sigma)\mathbf{e}_0 + \sum_{mx\in\mathbf{a}\neq\mathbf{0}} \tfrac{1}{12}\kappa^{m,m^2\infty}_{x\to x,\mathcal{C}}(\sigma)\,\mathbf{e}_{\mathbf{a}}. \tag{6.10.2}$$

The distribution law of θ_x in Proposition 4.1.5 ensures that the sequence $\{\boldsymbol{\mu}^{\mathcal{C}}_m(\sigma)\}_{m\in|\mathcal{C}|}$ forms a measure $\boldsymbol{\mu}^{\mathcal{C}} \in \mathbb{Z}_{\mathcal{C}}[[\mathbb{Z}^2_{\mathcal{C}}]]$ on $\mathbb{Z}^2_{\mathcal{C}}$ with no constant term (i.e., the image under the augmentation map $\varepsilon : \mathbb{Z}_{\mathcal{C}}[[\mathbb{Z}^2_{\mathcal{C}}]] \to \mathbb{Z}_{\mathcal{C}}$ vanishes): $\varepsilon(\boldsymbol{\mu}^{\mathcal{C}}) = 0$. Note also that, by Proposition 4.2.2, $\boldsymbol{\mu}^{\mathcal{C}}_m(\sigma,\mathbf{a}) = \boldsymbol{\mu}^{\mathcal{C}}_m(\sigma,-\mathbf{a})$, i.e., $\boldsymbol{\mu}^{\mathcal{C}}(\sigma)$ is an "even measure". Set $\mathbf{e}_m := \sum_{\mathbf{a}\in(\mathbb{Z}/m\mathbb{Z})^2}\mathbf{e}_{\mathbf{a}}$.

Theorem 6.10.3. *For $\sigma \in \pi_1(S^{\mathcal{C}}, \bar{b}^{\mathcal{C}})$, we have*

$$\mathcal{E}^{\mathcal{C}}_{\sigma} = \tfrac{1}{12}\rho_{\Delta}(\sigma)\cdot\boldsymbol{\delta}_0 + \boldsymbol{\mu}^{\mathcal{C}}(\sigma) = \varprojlim_{m\in|\mathcal{C}|}\big(\mathbb{E}^{\mathcal{C}}_m(\sigma) + \tfrac{1}{12}\rho_{\Delta(E,mdx/y)}(\sigma)\,\mathbf{e}_m\big),$$

where $\boldsymbol{\delta}_0$ indicates the unit Dirac measure at 0.

Proof. As observed in §3.6, $\mathbb{E}^{\mathcal{C}}_m(\sigma,\mathbf{a}) = \mathcal{E}^{\mathcal{C}}_m(\sigma,\mathbf{a}) - \mathcal{E}^{\mathcal{C}}_m(\sigma;0,0)$. On the other hand, by Theorem 6.2.1, it follows that $\mathbb{E}^{\mathcal{C}}_m(\sigma,\mathbf{a}) = \boldsymbol{\mu}^{\mathcal{C}}_m(\sigma,\mathbf{a}) - \frac{1}{12}\rho_{\Delta}(\sigma) + \rho_m(\sigma)$ for $0 \neq \mathbf{a} \in (\mathbb{Z}/m\mathbb{Z})^2$. Combining these, we obtain a formula

$$\boldsymbol{\mu}^{\mathcal{C}}_m(\sigma,\mathbf{a}) - \mathcal{E}^{\mathcal{C}}_m(\sigma,\mathbf{a}) = \tfrac{1}{12}\rho_{\Delta}(\sigma) - \rho_m(\sigma) - \mathcal{E}^{\mathcal{C}}_m(\sigma;0,0)\ (=: Y_m(\sigma)). \tag{6.10.4}$$

Now, observe that $\boldsymbol{\mu}^{\mathcal{C}}_m(\sigma,\mathbf{a}) - \mathcal{E}^{\mathcal{C}}_m(\sigma,\mathbf{a})$ varies coherently with respect to m in $\mathbf{a} \in (\mathbb{Z}/m\mathbb{Z})^2 \setminus \{0\}$, while the RHS, denoted $Y_m(\sigma)$, does not depend on $\mathbf{a}$. Hence, for any prime power $l^i \in |\mathcal{C}|$, we obtain $l^2 Y_{ml^{i+1}}(\sigma) = Y_{ml^i}(\sigma)$. This means $l^{\infty} \mid Y_m(\sigma)$, hence $Y_m(\sigma) = 0$ (cf. also [N95, p. 220]). This, together with 6.10.4,

completely determines $\mathcal{E}_m(\sigma)$ as

$$\mathcal{E}_m(\sigma,\mathbf{a}) = \begin{cases} \boldsymbol{\mu}_m^{\mathcal{C}}(\sigma,\mathbf{a}) = \boldsymbol{\mu}_m^{\mathcal{C}}(\sigma,-\mathbf{a}) & (\mathbf{a}\neq 0), \\ \frac{1}{12}\rho_\Delta(\sigma) - \rho_m(\sigma) & (\mathbf{a}=0). \end{cases} \tag{6.10.5}$$

The statement of the theorem is nothing but the limit case of the above formula as $m\to\infty$ in the language of measures on $\mathbb{Z}_{\mathcal{C}}^2$. □

Proof of Proposition 3.6.6. By using the composition law (3.5.8) repeatedly, in general, we have for $\sigma,\tau\in\pi_1(S,\bar{b})$ and $\epsilon\in \mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}})$,

$$\mathbb{E}_m^{\epsilon}(\sigma^{-1}) = -\chi(\sigma)^{-1}\mathbb{E}_m^{\rho(\sigma^{-1})\epsilon}(\sigma), \tag{6.10.6}$$

$$\mathbb{E}_m^{\epsilon}(\sigma\tau\sigma^{-1}) = \chi(\sigma)\mathbb{E}_m^{\rho(\sigma)^{-1}\epsilon}(\tau) + \mathbb{E}_m^{\rho(\tau\sigma^{-1})\epsilon}(\sigma) - \chi(\tau)\mathbb{E}_m^{\rho(\sigma^{-1})\epsilon}(\sigma). \tag{6.10.7}$$

Now, in the second formula above, put $\rho(\tau)=1$ (hence $\chi(\tau)=1$) and $\epsilon=1$. Then

$$\mathbb{E}_m(\sigma\tau\sigma^{-1}) = \chi(\sigma)\mathbb{E}_m^{\rho(\sigma)^{-1}}(\tau). \tag{6.10.8}$$

Let us compute the coefficient of $\mathbf{e_a}$ for $\mathbf{a}\neq 0$. For the left hand side, it turns out that

$$\mathbb{E}_m(\sigma\tau\sigma^{-1},\mathbf{a}) = \mathcal{E}_m(\sigma\tau\sigma^{-1},\mathbf{a}) - \chi(\sigma)\mathcal{E}_m(\tau;0,0)$$

as $\mathcal{E}_m(*,0,0)$ is the Kummer 1-cocycle $\frac{1}{12}\rho_\Delta-\rho_m$. Let us examine the right hand side of the definition of twisted invariants in §3.5. If $\rho(\sigma)^{-1}=\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right)$, then calculations with (3.5.2) yield

$$G_{\binom{u}{v}}^{\rho(\sigma)^{-1}}(\tau) = (\bar{\mathbf{x}}_1^{-\alpha u-\beta v}\bar{\mathbf{x}}_2^{-\gamma u-\delta v}-1)\mathcal{E}_\tau^{\mathcal{C}}.$$

Therefore, taking the mod m measure at 0, we see that

$$\begin{aligned}\chi(\sigma)\mathbb{E}_m^{\rho(\sigma)^{-1}}(\tau,\mathbf{a}) &= \chi(\sigma)(\mathcal{E}_m(\tau;\alpha u+\beta v,\gamma u+\delta v)-\mathcal{E}_m(\tau;0,0)) \\ &= \chi(\sigma)\mathcal{E}_m(\tau;\mathbf{a}\cdot{}^t\rho(\sigma)^{-1}) - \chi(\sigma)\mathcal{E}_m(\tau;0,0).\end{aligned}$$

Thus, we obtain

$$\mathcal{E}_m(\sigma\tau\sigma^{-1};\mathbf{a}) = \chi(\sigma)\mathcal{E}_m(\tau;\mathbf{a}\cdot{}^t\rho(\sigma)^{-1}),$$

which turns out to hold for all $\mathbf{a}\in(\mathbb{Z}/m\mathbb{Z})^2$. Noticing that the action of $\rho(\sigma)$ on the group ring $\mathbb{Z}_{\mathcal{C}}[(\mathbb{Z}/m\mathbb{Z})^2]$ is given by $\mathbf{e_a}\mapsto\mathbf{e}_{\mathbf{a}\cdot{}^t\rho(\sigma)}$, we conclude the proof. □

Proof of Proposition 5.7.3. We have only to show that the restriction of the Weierstrass tangential section $s_{\overrightarrow{\mathfrak{w}}}:\pi_1(M_{1,1}^{\omega},\bar{q})\to\pi_1(M_{1,2}^{\omega},\overrightarrow{\mathfrak{w}}_{\bar{q}})$ to the geometric part maps $\tau_1,\tau_2\in\hat{B}_3$ to those in $\hat{B}_4$ respectively. Since the image of $s_{\overrightarrow{\mathfrak{w}}}$ is in the normalizer of $\langle\mathbf{z}\rangle$, without loss of generality we may set $s_{\overrightarrow{\mathfrak{w}}}(\tau_1)=\tau_1\mathbf{z}^{c_1}$, $s_{\overrightarrow{\mathfrak{w}}}(\tau_2)=\tau_2\mathbf{z}^{c_2}$ for some $c_1,c_2\in\hat{\mathbb{Z}}$. The commutativity of $\mathbf{z}=(\omega_3)^2\omega_4^{-1}$ and the braid relation $\tau_1\tau_2\tau_1=\tau_2\tau_1\tau_2$ allow us to assume $c=c_1=c_2$. Now, consider the element

$\sigma := (\tau_1\tau_2)^6$, which is in the congruence kernel $\ker(\hat{B}_3 \to \mathrm{SL}_2(\hat{\mathbb{Z}}))$. The constant term of $\mathcal{E}_\sigma$ is then $\frac{1}{12}\rho_\Delta(\sigma) = -1$. On the other hand, the monodromy action $\varphi(\sigma)$ on $\hat{\Pi}_{1,1}$ is given by the inner action by $s_{\overrightarrow{\mathfrak{w}}}(\sigma) = (\tau_1\tau_2)^6\mathbf{z}^{6c} = \mathbf{z}^{1+6c}\omega_4$. Taking into consideration

$$\left(\frac{\partial \mathbf{z}\mathbf{x}_1^{-1}\mathbf{z}^{-1}\mathbf{x}_1}{\partial \mathbf{x}_1}\right)^{\mathrm{ab}} = (\bar{\mathbf{x}}_2 - 1)(1 - \bar{\mathbf{x}}_1^{-1}) \tag{6.10.9}$$

with (3.2.3), we see $G_{10}(\mathrm{Int}(z)) = 1 - \bar{\mathbf{x}}_1^{-1} = (\bar{\mathbf{x}}_1^{-1} - 1)\cdot\mathcal{E}_{\mathrm{Int}z}$. Therefore, by the definition (§3.6), $\mathcal{E}_\sigma = (-1 - 6c)\boldsymbol{\delta}_0$ ($\boldsymbol{\delta}_0$ the unit Dirac measure). Thus we obtain $-1 = -1 + 6c$ in $\hat{\mathbb{Z}}$. Comparing the l-adic components, we conclude $c = 0$ and the proof of Proposition 5.7.3. □

§7. Generalized Dedekind sums

§7.1. Elementary characters

In this section, we study our invariant $\mathbb{E}_m$ on the fundamental group $\pi_1(M^\omega_{1,1}(\mathbb{C}), \bar{q}) \cong \hat{B}_3$ in the universal setting introduced in §5. The braid group B_3 has a simple presentation $B_3 = \langle \tau_1, \tau_2 \mid \tau_1\tau_2\tau_1 = \tau_2\tau_1\tau_2\rangle$, whose generators τ_1, τ_2 are given standard identification as elements of $\pi_1(M^\omega_{1,1}(\mathbb{C}), \bar{q})$ (§§5.4–5.7). For any given full class $\mathcal{C}$ of finite groups, we have a pair of elementary characters:

$$(\rho^{\mathcal{C}}, \rho_\Delta) : \hat{B}_3 \to \mathrm{SL}_2(\mathbb{Z}_{\mathcal{C}}) \times \mathbb{Z}_{\mathcal{C}}, \quad \sigma \mapsto \left(\begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma)\end{pmatrix}, \rho_\Delta(\sigma)\right). \tag{7.1.1}$$

Recall that, with our notational conventions, $\rho^{\mathcal{C}}$ maps τ_1, τ_2 to $\left(\begin{smallmatrix} 1 & 0 \\ -1 & 1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1\end{smallmatrix}\right)$ respectively, and ρ_Δ maps both of them to -1. In the pro-$\mathcal{C}$ setting, the above pair of characters never gives an injection, as most of the congruence kernel $\pi_1(M^{\omega,\mathcal{C}}_{1,1}, \bar{q}^{\mathcal{C}}) = \ker(\rho^{\mathcal{C}})$ must be annihilated by ρ_Δ. But if we restrict the range of σ to the discrete fundamental group $B_3 = \pi_1(M^\omega_{1,1}(\mathbb{C})^{\mathrm{an}}, \bar{q})$ ($\subset \hat{B}_3$), then the discrete group B_3 is embedded into $\mathrm{SL}_2(\mathbb{Z}) \times \mathbb{Z}$ by the elementary characters.

In this section, generically we drop the superscript $\mathcal{C}$ to designate objects at the discrete level. The main purpose of this section is to give an explicit formula for $\mathbb{E}_m(\sigma; u, v)$ where $\sigma \in B_3$ and $(u, v) \in \mathbb{Z}^2$.

§7.2. Generalized Dedekind sum formula

In the beautiful work [St87], G. Stevens gave an interpretation of the Rademacher function on $\mathrm{GL}_2(\mathbb{Q})^+$ and its generalizations by using the Borel–Serre compactification of the upper half-plane. The special case of weight 2 had also been studied intensively in [St82], [St85] as well as in the classic work [Sch74] by B. Schoeneberg. We quote it in the restricted form on $\mathrm{SL}_2(\mathbb{Z})$ and with weight 2 in our notation.

(A generalization to higher weights and its arithmetic properties are also discussed in [N03], which we hope to continue in future work.)

Definition 7.2.1. The *generalized Rademacher function* of weight two on $\mathrm{SL}_2(\mathbb{Z})$ is defined, for $x = (x_1, x_2) \in \mathbb{Q}^2$ and $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, by

$$\Phi_x(A)\ (= \Phi_x^{(2)}(A)) = \begin{cases} -\dfrac{P_2(x_1)}{2}\,\dfrac{b}{d} & (c = 0), \\ -\dfrac{P_2(x_1)}{2}\,\dfrac{a}{c} - \dfrac{P_2(ax_1 + cx_2)}{2}\,\dfrac{d}{c} & \\ \quad + \displaystyle\sum_{i=0}^{c-1} P_1\left(\frac{x_1 + i}{c}\right) P_1\left(x_2 + a\frac{x_1 + i}{c}\right) & (c > 0), \end{cases}$$

so that it factors through $\mathrm{PSL}_2(\mathbb{Z})$ for $c < 0$. Here, P_1 and P_2 are the periodic Bernoulli functions as in §4.3. The last term in the above description for $c > 0$ is called a *generalized Dedekind sum*.

It is known that $\Phi_x(A)$ is invariant with respect to x mod $\mathbb{Z}^2$. We consider it only for $A \in \mathrm{SL}_2(\mathbb{Z})$, but still its values generally have denominators. If $x \in (\frac{1}{N}\mathbb{Z})^2$, then $\Phi_x(A)$ has integer values for $A \in \Gamma(12N^2)$.

Definition 7.2.2 (Correction term). Let $[x]^o$ and $\mathsf{P}_1^{\vdash}(x)$ denote respectively the "mild flooring function" and the "right continuous periodic sawtooth function" defined by

$$[x]^o := x - 1/2 - P_1(x), \qquad \mathsf{P}_1^{\vdash}(x) := B_1(\{x\}) = x - \lfloor x \rfloor - 1/2.$$

For $x = (x_1, x_2)$ and $A \in \mathrm{SL}_2(\mathbb{Z})$, define

$$K_x(A) := C_x - C_{xA}, \quad \text{where} \quad C_x := \frac{1}{2} + \frac{x_2(x_1 - 1)}{2} - \mathsf{P}_1^{\vdash}(x_2) \cdot [x_1]^o.$$

The main result of this section is the following

Theorem 7.2.3 (Generalized Dedekind sum formula). *Let $m \geq 1$ and for every $(r_1, r_2) \in \mathbb{Z}^2 \setminus (m\mathbb{Z})^2$, set $x = (x_1, x_2) = (r_1/m, r_2/m)$. Then, for each $\sigma \in B_3$,*

$$\mathbb{E}_m(\sigma; r_1, r_2) = K_x(A_\sigma) - \Phi_x^{(2)}(A_\sigma) - \tfrac{1}{12}\rho_\Delta(\sigma), \qquad \textit{where } A_\sigma = {}^t\rho(\sigma) \in \mathrm{SL}_2(\mathbb{Z}).$$

Note that by definition $\mathbb{E}_m(\sigma; 0, 0) = 0$, and $\mathbb{E}_m(\sigma; mk_1, mk_2)$ can be evaluated from $\mathbb{E}_m(\sigma; mk_1 + 1, mk_2)$, $\mathbb{E}_m(\sigma; 1, 0)$ and an elementary term as remarked in Proposition 3.4.8. We will also compute it in detail later in Proposition 7.5.1.

Most of this section will be devoted to the proof of the above theorem. Our basic idea is to apply Theorem 6.2.1 in this discrete situation. Obviously, the congruence condition on $(u, v) \equiv \mathbf{r}$ modulo $mM^2 2^\varepsilon$ and $\rho^{\mathcal{C}}(\sigma)$-admissibility condition on $\mathbf{r}/m \to \mathbf{s}/m$ modulo m^2M^2 become void if we put $(u, v) = \mathbf{r}$ and $\mathbf{s} = \mathbf{r}\,{}^t\rho(\sigma)$.

The Kummer quantity $\kappa_{x\to y}^{m,m^2\infty}(\sigma)$ turns out then to be a unique rational integer, and the assertion gives an equality of integers. This allows us to evaluate $\mathbb{E}_m(\sigma;u,v)$ in the complex analytic model of §2.9, §4.5.

Example 7.2.4. Let us here present an example to illustrate how the above Theorem realizes the integer valued invariant $\mathbb{E}_m(\sigma;r_1,r_2)$ for $\sigma\in B_3$ and $(r_1,r_2)\in \mathbb{Z}^2\setminus(m\mathbb{Z})^2$. Pick any braid $\sigma\in B_3$ so that

$$^t\rho(\sigma)=A:=\begin{pmatrix}11 & 24\\ 5 & 11\end{pmatrix}\in \mathrm{SL}_2(\mathbb{Z}).$$

Such a σ can be given (say, $\tau_1^{-2}\tau_2^6\tau_1^2\tau_2(\tau_1\tau_2)^{-3}$) up to $\langle(\tau_1\tau_2)^6\rangle$, hence $\frac{1}{12}\rho_\Delta(\sigma)$ is determined up to integer values. Set $m=3$. Calculation using generalized Dedekind sums yields the following (3-stride periodic) matrix for $(r_1,r_2)=(i-4,j-4)\in[-3,3]^2$ $(\subset\mathbb{Z}^2)$:

$$-\Phi(A):=(-\Phi^{(2)}_{(i-4)/3,(j-4)/3}(A))_{i,j=1}^7=\begin{bmatrix}
\frac{1}{6} & \frac{2}{9} & \frac{2}{9} & \frac{1}{6} & \frac{2}{9} & \frac{2}{9} & \frac{1}{6}\\
\frac{1}{12} & \frac{-19}{36} & \frac{2}{9} & \frac{1}{12} & \frac{-19}{36} & \frac{2}{9} & \frac{1}{12}\\
\frac{1}{12} & \frac{2}{9} & \frac{-19}{36} & \frac{1}{12} & \frac{2}{9} & \frac{-19}{36} & \frac{1}{12}\\
\frac{1}{6} & \frac{2}{9} & \frac{2}{9} & \frac{1}{6} & \frac{2}{9} & \frac{2}{9} & \frac{1}{6}\\
\frac{1}{12} & \frac{-19}{36} & \frac{2}{9} & \frac{1}{12} & \frac{-19}{36} & \frac{2}{9} & \frac{1}{12}\\
\frac{1}{12} & \frac{2}{9} & \frac{-19}{36} & \frac{1}{12} & \frac{2}{9} & \frac{-19}{36} & \frac{1}{12}\\
\frac{1}{6} & \frac{2}{9} & \frac{2}{9} & \frac{1}{6} & \frac{2}{9} & \frac{2}{9} & \frac{1}{6}
\end{bmatrix},$$

while the correction terms turn out to provide the (non-periodic) matrix

$$K(A):=(K_{(i-4)/3,(j-4)/3}(A))_{i,j=1}^7$$
$$=\begin{bmatrix}
-289 & \frac{-8723}{36} & \frac{-6707}{36} & -139 & \frac{-3863}{36} & \frac{-2567}{36} & -44\\
\frac{-1039}{6} & \frac{-1238}{9} & \frac{-3467}{36} & \frac{-379}{6} & \frac{-383}{9} & \frac{-767}{36} & \frac{-49}{6}\\
\frac{-523}{6} & \frac{-2243}{36} & \frac{-320}{9} & \frac{-103}{6} & \frac{-263}{36} & \frac{-5}{9} & \frac{-13}{6}\\
-30 & \frac{-587}{36} & \frac{-155}{36} & 0 & \frac{-47}{36} & \frac{-335}{36} & -25\\
\frac{-13}{6} & \frac{4}{9} & \frac{-83}{36} & \frac{-73}{6} & \frac{-221}{9} & \frac{-1703}{36} & \frac{-463}{6}\\
\frac{-25}{6} & \frac{-443}{36} & \frac{-266}{9} & \frac{-325}{6} & \frac{-2783}{36} & \frac{-1031}{9} & \frac{-955}{6}\\
-35 & \frac{-1955}{36} & \frac{-3107}{36} & -125 & \frac{-5735}{36} & \frac{-7607}{36} & -270
\end{bmatrix}.$$

The resulting right hand side in Theorem 7.2.3 on $[-3,3]^2$ ($\subset \mathbb{Z}^2$) for a σ with $\frac{1}{12}\rho_\Delta(\sigma) = -\frac{1}{12}$ (such a σ is, in fact, equal to $\tau_1^{-2}\tau_2^6\tau_1^2\tau_2(\tau_1\tau_2)^{-3}$) is then

$$-\Phi(A)+K(A)+\tfrac{1}{12}[1^{7\times 7}] = \begin{bmatrix} \frac{-1155}{4} & -242 & -186 & \frac{-555}{4} & -107 & -71 & \frac{-175}{4} \\ -173 & -138 & -96 & -63 & -43 & -21 & -8 \\ -87 & -62 & -36 & -17 & -7 & -1 & -2 \\ \frac{-119}{4} & -16 & -4 & \frac{1}{4} & -1 & -9 & \frac{-99}{4} \\ -2 & 0 & -2 & -12 & -25 & -47 & -77 \\ -4 & -12 & -30 & -54 & -77 & -115 & -159 \\ \frac{-139}{4} & -54 & -86 & \frac{-499}{4} & -159 & -211 & \frac{-1079}{4} \end{bmatrix}.$$

By Theorem 7.2.3, we conclude that the components of the above matrix coincide with those of $(\mathbb{E}_3(\sigma; i-4, j-4))_{i,j=1}^7$, except for $*/4$ at (i,j)-components with $i-1 \equiv j-1 \equiv 0 \bmod m = 3$. Generally, exceptional gaps between the two sides of the equality in Theorem 7.2.3 appear at locations of $(m\mathbb{Z})^2$ ($\subset \mathbb{Z}^2$). This phenomenon essentially signifies the singularity at $\mathbf{0}$ of the Eisenstein–Dedekind symbol of G. Stevens [St87] that is reflected in the periodic part $\Phi_x^{(2)}(A_\sigma)$ for $x \in \mathbb{Z}^2$.

§7.3. Siegel units vs. generalized Dedekind functions

To evaluate the left hand side of the congruence in Theorem 6.2.1, we need to identify the branch of power roots of the Siegel units $g_x(\tau)$ $\big(x = (x_1, x_2) \in \mathbb{Q}^2 \backslash \mathbb{Z}^2\big)$ in the complex model. This can be attained by identifying the branch of $\log g_x$, which, in view of (4.3.4), requires determining a suitable constant term for the indefinite integral of the Eisenstein series $E_2^{(\mathbf{x})}$ of weight 2 ($\mathbf{x} = x \bmod \mathbb{Z}$). We achieve this by comparing g_x with the generalized Dedekind function "$\eta_x(\tau) = e^{\psi_x(\tau)}$" given in the book of B. Schoeneberg [Sch74, Chap. VIII, §1.3], whose infinite product form is given by

$$\eta_x(\tau) := e^{\gamma_0(x)} e^{\pi i P_2(x_1)\tau} \prod_{0<s\in x_1+\mathbb{Z}} (1-e^{2\pi i x_2} q_\tau^s) \prod_{0<s\in -x_1+\mathbb{Z}} (1-e^{-2\pi i x_2} q_\tau^s), \tag{7.3.1}$$

where

$$\gamma_0(x) = \begin{cases} \pi i P_1(x_2) + \log(1-e^{-2\pi i x_2}), & x_1 \in \mathbb{Z},\ x_2 \notin \mathbb{Z}, \\ 0, & \text{otherwise.} \end{cases} \tag{7.3.2}$$

Comparing this with the infinite product form of g_x (cf. §4, Lemma 4.3.5) (and noting $-e^{2\pi i x_2} e^{-\pi i P_1(x_2)} = e^{\pi i P_1(x_2)}$ for $x_2 \notin \mathbb{Z}$), we obtain the following relation

between them:

$$g_x(\tau) = e^{\pi i} e^{\pi i x_2(x_1-1)} \eta_x(\tau) e^{-2\pi i \lfloor x_1 \rfloor (x_2 - 1/2)} [e^{\pi i P_1(x_2)}]^{\delta_{x_1 \in \mathbb{Z}}} \quad (x \in \mathbb{Q}^2 \setminus \mathbb{Z}^2), \tag{7.3.3}$$

where $\delta_{x_1 \in \mathbb{Z}} = 1, 0$ according as $x_1 \in \mathbb{Z}$ or $\notin \mathbb{Z}$ respectively.

A careful examination shows that Schoeneberg's lift $\psi_x(\tau)$ for $\eta_x(\tau) = e^{\psi_x(\tau)}$ can be identified, in fact, with $= e^{\gamma_0(x) + \psi_x^{St}(\tau)}$ where $\psi_x^{St}(\tau)$ is "half of G. Stevens' lift" given in his book [St82, Def. 2.3.1]) as follows:

$$\begin{aligned} \psi_x^{St}(\tau) &= \pi i P_2(x_1)\tau \\ &\quad - \sum_{0 < s \in x_1 + \mathbb{Z}} \sum_{k=1}^{\infty} \frac{1}{k} e^{2\pi i x_2 k} q_\tau^{sk} - \sum_{0 < s \in -x_1 + \mathbb{Z}} \sum_{k=1}^{\infty} \frac{1}{k} e^{-2\pi i x_2 k} q_\tau^{sk} \\ &= -2\pi i \left(\int_0^\tau a_0(E_2^{(x)})\, du + \int_{i\infty}^\tau \widetilde{E_2^{(x)}}(u)\, du \right), \end{aligned} \tag{7.3.4}$$

where $a_0(E_2^{(x)})$ (resp. $\widetilde{E_2^{(x)}}(u)$) is the constant term (resp. the remaining part) of the Eisenstein series $E_2^{(x)}$ (4.3.2).

In view of (7.3.3), in the home region $\{x = (x_1, x_2) \mid 0 < x_1, x_2 < 1\}$, $g_x(\tau)$ can be written as $e^{\pi i + \pi i x_2(x_1-1)} \eta_x(\tau)$, so we choose the branch of $\log g_x$ to be $\pi i + \pi i x_2(x_1 - 1) + \psi_x(\tau)$. For general $x \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, we will make it a principle to fit with our normalization of Kummer characters given in §5.10, which is compatible with its use in the proof of Lemma 6.5.4, i.e., with our moving rule: "walk first along $\mathbf{x}_2^{r_2}$ and then along $\mathbf{x}_1^{r_1}$". For this purpose, we shall choose a branch of $\log g_x(\tau)$ so as to be continuous in the complex plane minus $((-\infty, 0) \cup (1, +\infty)) \times \mathbb{Z}$ with limits from the right (above) in $\lim_{\varepsilon \to 0+} \log g_{x_2 + \varepsilon}$ for $x_1 \notin \mathbb{Z}$, $x_2 \in \mathbb{Z}$. For a fixed $x_2 \notin \mathbb{Z}$, if x_1 moves continuously from $n - \varepsilon$ to $n + \varepsilon$ for some $n \in \mathbb{Z}$, then ψ_x^{St} gets one new term $-\sum_k e^{2\pi i x_2 k} e^{2\pi i \varepsilon k \tau}$ and looses one old term $+\sum_k e^{-2\pi i x_2 k} e^{2\pi i(-\varepsilon)k\tau}$, so that when $\varepsilon \to 0$, the jump of $\psi_x^{St}(\tau)$ is counted as

$$\begin{aligned} -\sum_k e^{2\pi i x_2 k} + \sum_k e^{-2\pi i x_2 k} &= \log(1 - e^{2\pi i x_2}) - \log(1 - e^{-2\pi i x_2}) \\ &= 2\pi i (x_2 - 1/2). \end{aligned}$$

Therefore, to keep continuity of our lift $\log g_x(\tau)$, each time x_1 goes up across an integer value, we need to add an extra $-2\pi i(x_2 - 1/2)$. This explains the term $-2\pi i(x_2 - 1/2)\lfloor x_1 \rfloor$. The term coming from the inside of $[*]^{\delta_{x_1 \in \mathbb{Z}}}$ is to back up Schoeneberg's term which intends to take the mean of the upper and lower limits at every discontinuity point. Finally, after reaching the nearest unit square, one may want to arrive at a destination with $x_2 \in \mathbb{Z}$ from above. So we substitute

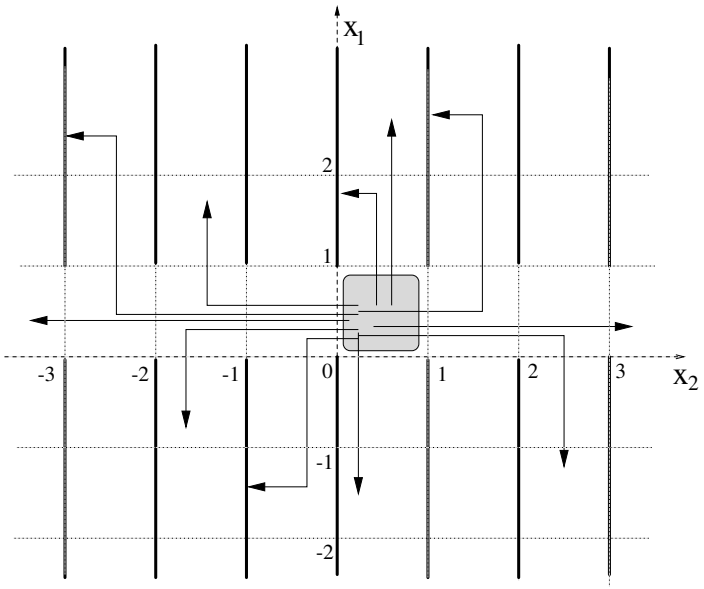


Figure 3

$\mathsf{P}_1^{\vdash}(x_2)$ for $P_1(x_2)$. Consequently, our choice of logarithm of Siegel units can be summarized as

$$\begin{aligned}(7.3.5)\qquad \log g_x(\tau) &= 2\pi i\left(\frac{1}{2}+\frac{x_2(x_1-1)}{2}-\mathsf{P}_1^{\vdash}(x_2)[x_1]^o\right)+\psi_x(\tau)\\ &= 2\pi i C_x+\psi_x(\tau)\quad (x=(x_1,x_2)\in\mathbb{Q}^2\setminus\mathbb{Z}^2),\end{aligned}$$

which uniformizes our choice of $g_x^{1/N}$ as $e^{\frac{1}{N}\log g_x}$ for all $N\geq 1$.

§7.4. Completion of proof of Theorem 7.2.3

To finish the proof of Theorem 7.2.3, we only need to identify the Kummer character $\kappa_{x\to y}^{m,m^2\infty}(\sigma)$ for $x=(r_1/m,r_2/m)$, $y=(s_1/m,s_2/m)$ with $\binom{s_1}{s_2}=\rho(\sigma)\binom{r_1}{r_2}$, i.e., $(s_1,s_2)=(r_1,r_2)A$, where $A={}^t\rho(\sigma)\in \mathrm{SL}_2(\mathbb{Z})$ for a given $\sigma\in B_3$. We now have

$$\frac{\theta_x^{1/N}|_{\mathfrak{a}_\sigma}}{\theta_y^{1/N}}=\zeta_N^{\kappa_{x\to y}^{m,m^2\infty}(\sigma)}\qquad(\mathfrak{a}_\sigma=A={}^t\rho(\sigma)).$$

Recalling Schoeneberg's formula from [Sch74, Chap. VIII, §3 (30), p. 199]:

$$(7.4.1)\qquad \psi_x(A\tau)-\psi_{xA}(\tau)=-2\pi i\Phi_x^{(2)}(A)$$

together with our convention of SL_2-action on the upper half-plane (cf. §4.6), we deduce from (7.3.5) that

$$\zeta_N^{\kappa_{x\to y}^{m,m^2\infty}(\sigma)}\frac{\left(\exp\left(\frac{12}{N}(2\pi iC_x+\psi_x(\tau))\right)\right)\big|_A}{\exp\left(\frac{12}{N}(2\pi iC_{xA}+\psi_{xA}(\tau))\right)}=\exp\left(\frac{24\pi i(K_x(A)-\Phi_x^{(2)}(A))}{N}\right)$$

for all $N\geq 1$. Thus, $\kappa_{x\to y}^{m,m^2\infty}(\sigma)=12(K_x(A)-\Phi_x^{(2)}(A))$. Applying Theorem 6.2.1 to the present situation where $\rho_m(\sigma)=0$, we complete the proof of Theorem 7.2.3. □

§7.5. Explicit formula for $\mathbb{E}_m$ on $B_3\times(m\mathbb{Z})^2$

We shall compute $\mathbb{E}_m(\sigma;u,v)$ for $\sigma\in B_3$ in case $u,v\in\mathbb{Z}$ are divisible by m.

Proposition 7.5.1. *Let $m\in\mathbb{N}$. For $\sigma\in B_3$ with $\rho(\sigma)=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$ and for $(k_1,k_2)\in\mathbb{Z}^2$, we have*

$$\mathbb{E}_m(\sigma;mk_1,mk_2)=-bck_1k_2-\tfrac{1}{2}\{k_1(ack_1+a-c-1)+k_2(bdk_2+b-d+1)\}.$$

Observe that the term in curly brackets is always an even integer, since a and c (resp. b and d) have different parity in view of $ad-bc=1$.

By using the above proposition, one can "repair" the last matrix in Example 7.2.4 at components of $(3\mathbb{Z})^2$ $(\subset\mathbb{Z}^2)$ to get

$$(\mathbb{E}_3(\sigma,i-4,j-4))_{i,j=1}^7=\begin{bmatrix}-289&-242&-186&-139&-107&-71&-44\\-173&-138&-96&-63&-43&-21&-8\\-87&-62&-36&-17&-7&-1&-2\\-30&-16&-4&0&-1&-9&-25\\-2&0&-2&-12&-25&-47&-77\\-4&-12&-30&-54&-77&-115&-159\\-35&-54&-86&-125&-159&-211&-270\end{bmatrix}.$$

Proof of Proposition 7.5.1. Applying Theorem 7.2.3 to the RHS in Proposition 3.4.8, we obtain

$$\mathbb{E}_m(\sigma;u,v)=K_{((u+1)/m,v/m)}(A)-K_{(1/m,0/m)}(A)+\left\lfloor\frac{au+bv}{m}\right\rfloor\cdot\left\lfloor\frac{c}{m}\right\rfloor,\tag{7.5.2}$$

where $A={}^t\rho(\sigma)=\left(\begin{smallmatrix}a&c\\b&d\end{smallmatrix}\right)$. It is easy to see that the terms of $K_{((u+1)/m,v/m)}(A)-K_{(1/m,0/m)}(A)$ can be classified into three families of terms: a quadratic form in k_1, k_2, a linear form in k_1 and a linear form in k_2. After a simple computation, we obtain from it those terms of the RHS of the desired formula together with $-(ak_1+bk_2)\lfloor c/m\rfloor$ which cancels with the last term of (7.5.2). □

§7.6. Examples of special cases

Now, we shall examine, for some simple braids $\sigma \in B_3$, the values $\mathbb{E}_m(\sigma; u, v)$ for $(u, v) \in \mathbb{Z}^2$ by means of their original definition given in §3. These examples are also useful to check the validity of the above Theorem 7.2.3 and Proposition 7.5.1.

Case $\sigma = \tau_1^\alpha$ $(\alpha \in \mathbb{Z})$. First, using Proposition 5.7.3 one sees that the action of the Weierstrass lift $s_{\overrightarrow{\mathfrak{w}}}(\sigma)$ is given by $\mathbf{x}_1 \mapsto \mathbf{x}_1\mathbf{x}_2^{-\alpha}$, $\mathbf{x}_2 \mapsto \mathbf{x}_2$. Therefore, according to (3.3.3), $\mathcal{S}_{uv}(\sigma) = \mathbf{x}_2^{-v}(\mathbf{x}_1\mathbf{x}_2^{-\alpha})^{-u}\mathbf{x}_1^u\mathbf{x}_2^{u-\alpha v}$. The corresponding $G_{uv}(\sigma)$ (3.3.4) can be deduced by the formula (3.2.3) of free differential calculus, and is found to be

$$G_{uv}(\tau_1^\alpha) = \frac{\bar{\mathbf{x}}_1^{-u}\bar{\mathbf{x}}_2^{\alpha u - v}}{\bar{\mathbf{x}}_2 - 1}\left(\frac{\bar{\mathbf{x}}_1^u - 1}{\bar{\mathbf{x}}_1 - 1} - \frac{(\bar{\mathbf{x}}_1\bar{\mathbf{x}}_2^{-\alpha})^u - 1}{\bar{\mathbf{x}}_1\bar{\mathbf{x}}_2^{-\alpha} - 1}\right). \tag{7.6.1}$$

Recalling (Definition 3.4.1) that our invariant $\mathbb{E}_m(\sigma; u, v)$ is the integral of the measure $dG_{uv}(\sigma)$ on $(m\hat{\mathbb{Z}})^2$, we find

$$\mathbb{E}_m(\tau_1^\alpha; u, v) = \begin{cases} \displaystyle\sum_{\substack{1 \le k \le u-1 \\ m \mid k}} \left(\left\lceil \frac{\alpha u - v}{m} \right\rceil - \left\lceil \frac{\alpha k - v}{m} \right\rceil\right) & (u > 0), \\ 0 & (u = 0), \\ \displaystyle\sum_{\substack{0 \le k \le -u-1 \\ m \mid k}} \left(-\left\lceil \frac{\alpha u - v}{m} \right\rceil + \left\lceil \frac{-\alpha k - v}{m} \right\rceil\right) & (u < 0). \end{cases} \tag{7.6.2}$$

In the calculation, we make use of the definition of the (profinite) ceiling function as an integral (Remark 3.4.7). The following matrix illustrates $\mathbb{E}_3(\tau_1, u, v)$ for $(u, v) \in [-6, 6]^2$:

$$(\mathbb{E}_3(\tau_1, i-7, j-7))_{i,j=1}^{13} = \begin{bmatrix} 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 1 & 3 & 3 & 1 & 3 & 3 & 1 & 3 & 3 & 1 & 3 & 3 & 1 \\ 1 & 1 & 3 & 1 & 1 & 3 & 1 & 1 & 3 & 1 & 1 & 3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Case $\sigma = \tau_2^{\alpha}$ $(\alpha \in \mathbb{Z})$. In this case, the Weierstrass lift $s_{\overrightarrow{\mathfrak{w}}}(\sigma)$ acts as $\mathbf{x}_1 \mapsto \mathbf{x}_1$ and $\mathbf{x}_2 \mapsto \mathbf{x}_2\mathbf{x}_1^{\alpha}$, and hence $\mathcal{S}_{uv}(\sigma) = (\mathbf{x}_2\mathbf{x}_1^{\alpha})^{-v}\mathbf{x}_1^{\alpha v}\mathbf{x}_2^{v}$. It follows that

$$G_{uv}(\tau_2^{\alpha}) = \frac{(\bar{\mathbf{x}}_2\bar{\mathbf{x}}_1^{\alpha})^{-v}}{\bar{\mathbf{x}}_1 - 1}\left(\frac{(\bar{\mathbf{x}}_2\bar{\mathbf{x}}_1^{\alpha})^{v} - 1}{\bar{\mathbf{x}}_2\bar{\mathbf{x}}_1^{\alpha} - 1} - \bar{\mathbf{x}}_1^{\alpha v}\frac{\bar{\mathbf{x}}_2^{v} - 1}{\bar{\mathbf{x}}_2 - 1}\right). \tag{7.6.3}$$

Integration over $(m\hat{\mathbb{Z}})^2$ then yields

$$\mathbb{E}_m(\tau_2^{\alpha}; u, v) = \begin{cases} \displaystyle\sum_{\substack{1\le k\le v\\ m|k}} -\left\lceil\frac{\alpha k}{m}\right\rceil & (v > 0),\\ 0 & (v = 0),\\ \displaystyle\sum_{\substack{0\le k\le -v-1\\ m|k}} -\left\lceil\frac{\alpha k}{m}\right\rceil & (v < 0). \end{cases} \tag{7.6.4}$$

In this case, it is remarkable that $\mathbb{E}_m(\tau_2^{\alpha}; u, v)$ does not depend on u. The following matrix illustrates $\mathbb{E}_3(\tau_2, u, v)$ for $(u, v) \in [-6, 6]^2$:

$$(\mathbb{E}_3(\tau_2, i-7, j-7))_{i,j=1}^{13}$$

$$= \begin{bmatrix} -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3 \end{bmatrix}.$$

Case $\sigma = \tau_1\tau_2\tau_1$. In this case, the Weierstrass lift $s_{\overrightarrow{\mathfrak{w}}}(\sigma)$ maps $\mathbf{x}_1 \mapsto \mathbf{x}_2^{-1}$, $\mathbf{x}_2 \mapsto \mathbf{x}_2\mathbf{x}_1\mathbf{x}_2^{-1}$. Then $\mathcal{S}_{uv}(\sigma) = \mathbf{x}_2\mathbf{x}_1^{-v}\mathbf{x}_2^{u-1}\mathbf{x}_1^{v}\mathbf{x}_2^{-u}$, and

$$G_{uv}(\tau_1\tau_2\tau_1) = \frac{\bar{\mathbf{x}}_2 - \bar{\mathbf{x}}_2^{u}}{\bar{\mathbf{x}}_2 - 1}\cdot\frac{\bar{\mathbf{x}}_1^{-v} - 1}{\bar{\mathbf{x}}_1 - 1}. \tag{7.6.5}$$

By integration of $dG_{uv}(\sigma)$ over $(m\hat{\mathbb{Z}})^2$, we obtain the formula

$$\mathbb{E}_m(\tau_1\tau_2\tau_1; u, v) = \left(1 - \left\lceil \frac{u}{m} \right\rceil\right) \cdot \left\lceil \frac{-v}{m} \right\rceil. \tag{7.6.6}$$

The following matrix illustrates $\mathbb{E}_3(\tau_1\tau_2\tau_1, u, v)$ for $(u, v) \in [-6, 6]^2$:

$$(\mathbb{E}_3(\tau_1\tau_2\tau_1, i-7, j-7))_{i,j=1}^{13}$$

$$= \begin{bmatrix} 6 & 6 & 6 & 3 & 3 & 3 & 0 & 0 & 0 & -3 & -3 & -3 & -6 \\ 4 & 4 & 4 & 2 & 2 & 2 & 0 & 0 & 0 & -2 & -2 & -2 & -4 \\ 4 & 4 & 4 & 2 & 2 & 2 & 0 & 0 & 0 & -2 & -2 & -2 & -4 \\ 4 & 4 & 4 & 2 & 2 & 2 & 0 & 0 & 0 & -2 & -2 & -2 & -4 \\ 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & -1 & -1 & -1 & -2 \\ 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & -1 & -1 & -1 & -2 \\ 2 & 2 & 2 & 1 & 1 & 1 & 0 & 0 & 0 & -1 & -1 & -1 & -2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -2 & -2 & -2 & -1 & -1 & -1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\ -2 & -2 & -2 & -1 & -1 & -1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \\ -2 & -2 & -2 & -1 & -1 & -1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 \end{bmatrix}.$$

Case $\sigma = \tau_1\tau_2$. In this case, the Weierstrass lift $s_{\overrightarrow{\mathfrak{w}}}(\sigma)$ transforms generators as $\mathbf{x}_1 \mapsto \mathbf{x}_2^{-1}$, $\mathbf{x}_2 \mapsto \mathbf{x}_2\mathbf{x}_1$. Therefore, $\mathcal{S}_{uv} = (\mathbf{x}_2\mathbf{x}_1)^{-v}\mathbf{x}_2^u\mathbf{x}_1^v\mathbf{x}_2^{v-u}$, and it turns out that

$$G_{uv}(\tau_1\tau_2) = \frac{(\bar{\mathbf{x}}_2\bar{\mathbf{x}}_1)^{-v}}{\bar{\mathbf{x}}_2 - 1}\left(\bar{\mathbf{x}}_2^u \frac{\bar{\mathbf{x}}_1^v - 1}{\bar{\mathbf{x}}_1 - 1} - \bar{\mathbf{x}}_2 \frac{(\bar{\mathbf{x}}_1\bar{\mathbf{x}}_2)^v - 1}{\bar{\mathbf{x}}_1\bar{\mathbf{x}}_2 - 1}\right). \tag{7.6.7}$$

By integrating over $(m\hat{\mathbb{Z}})^2$, we find

$$\mathbb{E}_m(\tau_1\tau_2; u, v) = \begin{cases} \displaystyle\sum_{\substack{1 \le k \le v \\ m \mid k}} \left(\left\lceil \frac{u-v}{m} \right\rceil - \left\lceil \frac{1-k}{m} \right\rceil\right) & (v > 0), \\ 0 & (v = 0), \\ \displaystyle\sum_{\substack{0 \le k \le -v-1 \\ m \mid k}} \left(-\left\lceil \frac{u-v}{m} \right\rceil + \left\lceil \frac{1+k}{m} \right\rceil\right) & (v < 0). \end{cases} \tag{7.6.8}$$

The following matrix illustrates $\mathbb{E}_3(\tau_1\tau_2, u, v)$ for $(u, v) \in [-6, 6]^2$:

$$(\mathbb{E}_3(\tau_1\tau_2, i-7, j-7))_{i,j=1}^{13}$$

$$= \begin{bmatrix}
3 & 3 & 3 & 2 & 2 & 2 & 0 & 0 & 0 & -3 & -3 & -3 & -7 \\
1 & 3 & 3 & 1 & 2 & 2 & 0 & 0 & 0 & -2 & -3 & -3 & -5 \\
1 & 1 & 3 & 1 & 1 & 2 & 0 & 0 & 0 & -2 & -2 & -3 & -5 \\
1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & -2 & -2 & -2 & -5 \\
-1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & -1 & -2 & -2 & -3 \\
-1 & -1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & -1 & -2 & -3 \\
-1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3 \\
-3 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 \\
-3 & -3 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 \\
-3 & -3 & -3 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
-5 & -3 & -3 & -2 & -1 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\
-5 & -5 & -3 & -2 & -2 & -1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\
-5 & -5 & -5 & -2 & -2 & -2 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}.$$

Errata to [N95]:
P. 205, line 4: order $12(l^2-1)$ in $l^m\mathfrak{L}$ and poles of order 12 in $l^{m-1}\mathfrak{L}\backslash l^m\mathfrak{L}$.
P. 206, (2.6): $\vartheta_m(*)$ should be defined by 12-multiples of the RHS.
P. 207, (2.10) Lemma: RHS should read $\zeta_N^{12(l^2-1)\nu_{ab}^m(\sigma)}$.
P. 207, line↑ 5,6: Replace $\zeta_N^{-\nu(l^2-1)}$ by $\zeta_N^{-12\nu(l^2-1)}$.
P. 209, (3.5.1): RHS should read $\zeta_N^{12\mu_m(a,b;\sigma)}$.
P. 210, (3.8): RHS should read $\zeta_N^{12\varepsilon(\mu^{(r)}(\sigma))}$.
P. 212, (3.11.4): RHS should read $\zeta_N^{12\kappa_{ij}(\sigma)}$.

Errata to [N99]:
On p. 204, p. 213 figures should be inserted (same as in §5 of the present paper).
P. 211: sign of $g_3(q)$.
P. 212, (3.3): $\frac{\chi_{m+1}(\sigma)}{1-l^m}$ should read $\frac{\chi_{m+1}(\sigma)}{1-p^m}$.
P. 213, line 6: $(1-q^n)^{24}$; line 22: ∞_{n-1}^{-1}.

Note and acknowledgements

A seminal key idea of relating my old work [N95] to Dedekind sums was first suggested to the author by Tomoyoshi Ibukiyama when we accidentally came across each other on a train to the 1993 Kinosaki conference. The first version of the present paper was a manuscript entitled "On exterior monodromy representations associated with affine elliptic curves", prepared during the author's stay at Bonn

University in the summer of 2001 (cf. [N01]). After a couple of years' lack of chance to work out the subject (except for some related works [N02j, N03j, N03]), an essential part of the present paper was written up during my participation in the project "Non-Abelian Fundamental Groups in Arithmetic Geometry" organized by J. Coates, M. Kim, F. Pop, M. Saidi and P. Schneider at Newton Institute in 2009. An earlier compiled version of this paper then appeared in RIMS Kyoto University Preprint Series (RIMS-1691, February 2010). In view of the above long history of this paper, I would like to express my sincere gratitude to all people and institutions named above for their support and hospitality. Finally, I thank the referees very much for numerous useful remarks and comments that have improved the presentation of arguments of this paper.

This work was supported partly by JSPS KAKENHI 21340009.

References

[A89] G. Anderson, The hyperadelic gamma function, Invent. Math. **95** (1989), 63–131. Zbl 0682.14011 MR 0969414

[As01] M. Asada, The faithfulness of the monodromy representations associated with certain families of algebraic curves, J. Pure Appl. Algebra **159** (2001), 123–147. Zbl 1045.14013 MR 1828935

[BK10] K. Bannai and S. Kobayashi, Algebraic theta functions and the p-adic interpolation of Eisenstein–Kronecker numbers, Duke Math. J. **153** (2010), 229–295. Zbl 1205.11076 MR 2667134

[BL94] A. Beilinson and A. Levin, Elliptic polylogarithms, in *Motives*, U. Jannsen et al. (eds.), Proc. Sympos. Pure Math. 55, Part 2, Amer. Math. Soc., 1994, 123–192. MR 1265553

[B79] G. V. Belyĭ, On Galois extensions of a maximal cyclotomic field, Izv. Akad. Nauk SSSR **8** (1979), 267–276 (in Russian); English transl.: Math. USSR-Izv. **14** (1980), 247–256. Zbl 0429.12004 MR 0534593

[Bl84] S. Bloch, letter to P. Deligne, 1984.

[B-1] N. Bourbaki, *Éléments de Mathématique, Algèbre*, Hermann, Paris, 1962.

[B-2] N. Bourbaki, *Éléments de Mathématique, Algèbre Commutative*, Hermann, Paris, 1961.

[C89] R. Coleman, Anderson–Ihara theory: Gauss sums and circular units, in *Algebraic number theory*, Adv. Stud. Pure Math. 17, Academic Press, 1989, 55–72. Zbl 0733.14012 MR 1097609

[De89] P. Deligne, Le groupe fondamental de la droite projective moins trois points, in *Galois groups over* $\mathbb{Q}$, Y. Ihara et al. (eds.), MSRI Publ. 16, Springer, 1989, 79–297. Zbl 0742.14022 MR 1012168

[Dr90] V. G. Drinfeld, On quasitriangular quasi-Hopf algebras and a group closely connected with $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, Algebra i Analiz **2** (1990), 149–181 (in Russian); English transl.: Leningrad Math. J. **2** (1991) 829–860. Zbl 0728.16021 MR 1080203

[E10] B. Enriquez, Elliptic associators, arXiv:1003.1012.

[Fr16] R. Fricke, Die Elliptische Funktionen und ihre Anwendungen, Erster Teil, Teubner, Leipzig, 1916. JFM 46.0599.02

[F10] H. Furusho, Pentagon and hexagon equations, Ann. of Math. **171** (2010), 545–556. Zbl 1257.17019 MR 2630048

[G84] A. Grothendieck, Esquisse d'un programme, 1984, in *Geometric Galois actions I*, P. Lochak and L. Schneps (eds.), London Math. Soc. Lecture Note Ser. 242, Cambridge Univ. Press, 1997, 5–48. Zbl 0901.14001 MR 1483107

[GR71] A. Grothendieck and M. Raynaud, Revêtements Etales et Groupe Fondamental (SGA1), Lecture Note in Math. 224, Springer, 1971. Zbl 0234.14002

[GM71] A. Grothendieck and J. P. Murre, *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*, Lecture Notes in Math. 208, Springer, 1971. Zbl 0216.33001 MR 0316453

[Ha97] R. Hain, Infinitesimal presentations of the Torelli groups, J. Amer. Math. Soc. **10** (1997), 597–651. Zbl 0915.57001 MR 1431828

[Ho09] Y. Hoshi, On the fundamental groups of log configuration schemes, Math. J. Okayama Univ. **51** (2009), 1–26. Zbl 1169.14022 MR 2482403

[Ih86a] Y. Ihara, Profinite braid groups, Galois representations, and complex multiplications, Ann. of Math. **123** (1986), 43–106. Zbl 0595.12003 MR 0825839

[Ih86b] ———, On Galois representations arising from towers of coverings of $\mathbf{P}^1 - \{0, 1, \infty\}$, Invent. Math. **86** (1986), 427–459. Zbl 0585.14020 MR 0860676

[Ih90] ———, Braids, Galois groups, and some arithmetic functions, in *Proc. Int. Congress of Math. Kyoto 1990*, 99–120. Zbl 0757.20007 MR 1159208

[Ih99-00] ———, On beta and gamma functions associated with the Grothendieck–Teichmüller modular group, in *Aspects of Galois theory*, H. Völklein et al. (eds.), London Math. Soc. Lecture Note Ser. 256, Cambridge Univ. Press, 1999, 144–179; Part II, J. Reine Angew. Math. **527** (2000), 1–11. Zbl 1046.14010(I) Zbl 1046.14009(II) MR 1708605(I) MR 1794015(II)

[Ih02] ———, Some arithmetic aspects of Galois actions in the pro-p fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$, in *Arithmetic fundamental groups and noncommutative algebra* (Berkeley, CA, 1999), Proc. Sympos. Pure Math. 70, Amer. Math. Soc., 2002, 247–273. Zbl 1065.14025 MR 1935408

[IKY87] Y. Ihara, M. Kaneko and A. Yukinari, On some properties of the universal power series for Jacobi sums, in *Galois representations and arithmetic algebraic geometry*, Adv. Stud. Pure Math. 12, North-Holland, 1987, 65–86. Zbl 0642.12012 MR 0948237

[IM95] Y. Ihara and M. Matsumoto, On Galois actions on profinite completions of braid groups, in *Recent developments in the inverse Galois problem*, M. Fried et al. (eds.), Contemp. Math. 186, Amer. Math. Soc., 1995, 173–200. Zbl 0848.11058 MR 1352271

[IN97] Y. Ihara and H. Nakamura, On deformation of maximally degenerate stable marked curves and Oda's problem, J. Reine Angew. Math. **487** (1997), 125–151. Zbl 0910.14010 MR 1454262

[K76] N. Katz, p-adic interpolation of real analytic Eisenstein series, Ann. of Math. **104** (1976), 459–571. Zbl 0354.14007 MR 0506271

[KM85] N. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Ann. of Math. Stud. 108, Princeton Univ. Press, 1985. Zbl 0576.14026 MR 0772569

[Ki07] M. Kim, p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication, Ann. of Math. **172** (2010), 751–759. Zbl 1223.11080 MR 2680431

[KL81] D. Kubert and S. Lang, *Modular units*, Springer, 1981. Zbl 0492.12002 MR 0648603

[L87] S. Lang, *Elliptic functions*, 2nd ed., Grad. Texts in Math. 112, Springer, 1987. Zbl 0615.14018 MR 0890960

[LS06] P. Lochak and L. Schneps, Open problems in Grothendieck–Teichmüller theory, in *Problems on mapping class groups and related topics*, Proc. Sympos. Pure Math. 74, Amer. Math. Soc., 2006, 165–186. Zbl 1222.14046 MR 2264540

[Ma96] M. Matsumoto, Galois representations on profinite braid groups on curves, J. Reine Angew. Math. **474** (1996), 169–219. Zbl 0858.12002 MR 1390695

[Ma97] ———, Galois group $G_{\mathbb{Q}}$, singularity E_7 and moduli M_3, in *Geometric Galois actions, 2*, P. Lochak and L. Schneps (eds.), London Math. Soc. Lecture Note Ser. 243, Cambridge Univ. Press, 1997, 179–218. Zbl 0979.14001 MR 1653014

[Mh86] H. Matsumura, *Commutative ring theory*, Cambridge Univ. Press, 1986. Zbl 0603.13001 MR 0879273

[MS03] W. G. McCallum and R. Sharifi, A cup product in the Galois cohomology of number fields, Duke Math. J. **120** (2003), 269–310. Zbl 1047.11106 MR 2019977

[Moc99] S. Mochizuki, Extending families of curves over log regular schemes, J. Reine Angew. Math. **511** (1999), 43–71. Zbl 0933.14012 MR 1695789

[Moc02] S. Mochizuki, Anabelian geometry in the Hodge–Arakelov theory of elliptic curves, in *Communications in arithmetic fundamental groups*, H. Nakamura (ed.), RIMS Kokyuroku **1267** (2002), 96–111. MR 1954370

[Mor93] S. Morita, The extension of Johnson's homomorphism from the Torelli group to the mapping class group, Invent. Math. **111** (1993), 197–224. Zbl 0787.57008 MR 1193604

[Mum83] D. Mumford, *Tata lectures on theta I*, Birkhäuser, 1983. Zbl 0509.14049 MR 0688651

[N94] H. Nakamura, Galois rigidity of pure sphere braid groups and profinite calculus, J. Math. Sci. Univ. Tokyo **1** (1994), 71–136. Zbl 0901.14012 MR 1298541

[N95] ———, On exterior Galois representations associated with open elliptic curves, J. Math. Sci. Univ. Tokyo **2** (1995), 197–231. Zbl 0914.11035 MR 1348028

[N97] ———, Galois representations in the profinite Teichmüller modular groups, in *Geometric Galois actions I*, L. Schneps and P. Lochak (eds.), London Math. Soc. Lecture Note Ser. 242, Cambridge Univ. Press, 1997, 159–173. Zbl 0911.14014 MR 1483116

[N99] ———, Tangential base points and Eisenstein power series, in *Aspects of Galois theory*, H. Völklein et al. (eds.), London Math. Soc. Lecture Note Ser. 256, Cambridge Univ. Press, 1999, 202–217. Zbl 0986.14013 MR 1708607

[N99-02] ———, Limits of Galois representations in fundamental groups along maximal degeneration of marked curves, I, Amer. J. Math. **121** (1999) 315–358; II, Proc. Sympos. Pure Math. 70, Amer. Math. Soc., 2002, 43–78. Zbl 1006.12001(I) Zbl 1162.14307(II) MR 1680325(I) MR 1935405(II)

[N01] ———, Some arithmetic in fundamental groups of affine elliptic curves, talk at Euresco Conference at Acquafredda Maratea, 2001.

[N02j] ———, On exterior monodromy representation associated with elliptic curves and Eisenstein measure function, RIMS Kokyuroku **1281** (2002), 176–183 (in Japanese). MR 1959683

[N03j] ———, On Magnus representation arising from elliptic curves and Eisenstein power series, in *Report collection of 47th algebra symposium*, A. Tamagawa and S.Yoshihara (eds.), 2002, 143–149 (in Japanese).

[N03] ———, Generalized Rademacher functions and some congruence properties, in *Galois theory and modular forms*, K. Hashimoto et al. (eds.), Development Math. 11, Kluwer, 2003, 375–394. Zbl 1060.11023 MR 2059775

[N12] ———, Some congruence properties of Eisenstein invariants associated to elliptic curves, in *Galois–Teichmüller theory and arithmetic geometry*, H. Nakamura et al. (eds.), Adv. Stud. Pure Math. 63, Math. Soc. Japan, 2012, 813–832.

[NS00] H. Nakamura and L. Schneps, On a subgroup of the Grothendieck–Teichmüller group acting on the tower of profinite Teichmüller modular groups, Invent. Math. **141** (2000), 503–560. Zbl 1077.14030 MR 1779619

[NT03-06] H. Nakamura and H. Tsunogai, Harmonic and equianharmonic equations in the Grothendieck–Teichmüller group, Forum Math. **15** (2003), 877–892; II, in *Primes and knots*, T. Kohno and M. Morishita (eds.), Contemp. Math. 416, Amer. Math. Soc., 2006, 197–211. Zbl 1054.14038(I) Zbl 1130.14022(II) MR 2010283(I) MR 2276142(II)

[NTY10] H. Nakamura, H. Tsunogai and S. Yasuda, Harmonic and equianharmonic equations in the Grothendieck–Teichmüller group, III, J. Inst. Math. Jussieu **9** (2010), 431–448. Zbl 1203.14033 MR 2602032

[Od90-95] T. Oda, A note on ramification of the Galois representation on the fundamental group of an algebraic curve, J. Number Theory **34** (1990), 225–228; II, J. Number Theory **53** (1995), 342–355. Zbl 0716.14014(I) Zbl 0844.14013(II) MR 1042495(I) MR 1348768(II)

[Rad73] H. Rademacher, *Topics in analytic number theory*, Springer, 1973. Zbl 0253.10002 MR 0364103

[Sch74] B. Schoeneberg, *Elliptic modular functions. An introduction*, Springer, 1974. Zbl 0285.10016 MR 0412107

[Sh71] G. Shimura, *Introduction to arithmetic theory of automorphic functions*, Iwanami Shoten and Princeton Univ. Press, 1971. Zbl 0221.10029 MR 1291394

[St82] G. Stevens, *Arithmetic on modular curves*, Progr. Math. 20, Birkhäuser, 1982. Zbl 0529.10028 MR 0670070

[St85] ———, The cuspidal group and special values of L-functions, Trans. Amer. Math. Soc. **291** (1985), 519–550. Zbl 0579.10011 MR 0800251

[St87] ———, The Eisenstein measure and real quadratic fields, in *Théorie des nombres* (Quebec, PQ, 1987), de Gruyter, Berlin, 1987, 887–927. Zbl 0684.10028 MR 1024612

[Sti08] J. Stix, On cuspidal sections of algebraic fundamental groups, in *Galois–Teichmüller theory and arithmetic geometry* (Kyoto, 2010), H. Nakamura et al. (eds.), Adv. Stud. Pure Math. 63, Math. Soc. Japan, 2012, 519–563.

[Ta97] A. Tamagawa, The Grothendieck conjecture for affine curves, Compos. Math. **109** (1997), 135–194. Zbl 0899.14007 MR 1478817

[Tsu95a] H. Tsunogai, On the automorphism group of a free pro-l meta-abelian group and an application to Galois representations, Math. Nachr. **171** (1995), 315–324. Zbl 0823.14015 MR 1316365

[Tsu95b] ———, On some derivations of Lie algebras related to Galois representations, Publ. RIMS Kyoto Univ. **31** (1995), 113–134. Zbl 0838.11040 MR 1317526

[Tsu03] ———, The stable derivation algebras for higher genera, Israel J. Math. **136** (2003), 221–250. Zbl 1051.14025 MR 1998111

[Woj04] Z. Wojtkowiak, On a torsor of paths of an elliptic curve minus a point, J. Math. Sci. Univ. Tokyo **11** (2004), 353–399. Zbl 1162.11359 MR 2110920