RIMS-1691

ON ARITHMETIC MONODROMY REPRESENTATIONS OF EISENSTEIN TYPE IN FUNDAMENTAL GROUPS OF ONCE PUNCTURED ELLIPTIC CURVES

By

Hiroaki NAKAMURA

February 2010

京都大学　数理解析研究所

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES

KYOTO UNIVERSITY, Kyoto, Japan

ON ARITHMETIC MONODROMY REPRESENTATIONS OF EISENSTEIN TYPE IN FUNDAMENTAL GROUPS OF ONCE PUNCTURED ELLIPTIC CURVES

HIROAKI NAKAMURA

Department of Mathematics, Faculty of Science,
Okayama University, Okayama 700-8530, Japan
h-naka@math.okayama-u.ac.jp

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 the generalized Dedekind-Rademacher functions as a main periodic part of the invariant.

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 $\Delta = \Delta(E, \frac{dx}{y}) = g_2^3 - 27g_3^2 \in k^\times$. The local coordinate $t := -\frac{2x}{y}$ 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 $\vec{\mathfrak{w}}$ and a split exact sequence of profinite fundamental groups

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

It is well known that the geometric fundamental group $\pi_1(E_{\bar{k}} \setminus \{O\}, \vec{\mathfrak{w}})$ 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 $\pi_1(E_{\bar{k}} \setminus \{O\}, \vec{\mathfrak{w}})$. Write $\varphi_{\vec{\mathfrak{w}}} : G_k \to \mathrm{Aut}(\pi)$ 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 sum [Ih86a], and proposed a new power series representation

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

from the meta abelian reduction of $\varphi_{\vec{\mathfrak{w}}}$ 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

---

1991 *Mathematics Subject Classification.* Primary 14H30; Secondary 11G05, 11G16, 11F20.
Key words and phrases. Galois representation, arithmetic fundamental group, elliptic curve.
Version 1.37 [RIMS-Preprint]

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 the 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]. Our main motivation of this 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 elliptic case still by extending Tsunogai's treatment but in a somewhat twisted way. Consequently, for each l-power m, we will construct a certain continuous mapping

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

from the meta-abelian reduction $G_k \to \mathrm{Aut}(\pi/\pi'')$ of $\varphi_{\vec{\mathfrak{w}}}$. 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 as to determine 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 $\mathbb{Z}_l^2$:

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

where $\rho_{\Delta(E, m\frac{dx}{y})}$ means a Kummer 1-cocycle along (a specified sequence of) l-power roots of $\Delta(E, m\frac{dx}{y}) = m^{-12}(g_2^3 - 27g_3^2)$, 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 of finite groups $\mathcal{C}$ closed under formation of subgroups, quotients and extensions. Moreover, we consider the Weierstrass equation (1.1) with k arbitrary algebra B over $\mathbb{Q}$, which naturally fits in the language of $\Gamma(1)$-test object 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 $\varphi_{\vec{\mathfrak{w}}} : \pi_1(S, \bar{b}) \to \mathrm{Aut}(\pi)$. Writing $|\mathcal{C}| := \{m \in \mathbb{N}; (\mathbb{Z}/m\mathbb{Z}) \in \mathcal{C}\}$, $\mathbb{Z}_\mathcal{C} := \varprojlim_{M \in |\mathcal{C}|} (\mathbb{Z}/M\mathbb{Z})$, we obtain then the invariants (as continuous mappings in profinite topology)

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

These invariants, after collected over all $m \in |\mathcal{C}|$, will turn out to recover the meta-abelian reduction of $\varphi_{\vec{\mathfrak{w}}}$ 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 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 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, entered into our view is anabelian geometry of the moduli space $M_{1,1}^\omega$ $(= \mathrm{Spec}(\mathbb{Q}[g_2, g_3, \frac{1}{\Delta}]))$ 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 Neron polygons 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 $M_{1,1}^{\omega}$ from the representing point of $\bar{b}$ to the locus of Tate elliptic curve $\mathrm{Tate}(q)/\mathbb{Q}((q))$. In §5, we will discuss location of several significant tangential base points on $M_{1,2}^{\omega}$ and $M_{1,1}^{\omega}$ in the spirit of our collaboration with L. Schneps [NS00], 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 providing 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 $(u,v)\in\mathbb{Z}_{\mathcal{C}}^2\setminus(m\mathbb{Z}_{\mathcal{C}})^2$, pick two pairs of rational integers $\mathbf{r}=(r_1,r_2)$, $\mathbf{s}=(s_1,s_2)$ such that $\mathbf{r}\equiv(u,v)\mod mM^22^{\varepsilon}$ (where $\varepsilon=0,1$ according as $2\nmid M$, $2|M$ respectively) and $\binom{s_1}{s_2}\equiv\rho^{\mathcal{C}}(\sigma)\binom{r_1}{r_2}\mod m^2Me_{\mathcal{C}}$, where $e_{\mathcal{C}}\in\{1,3,4,12\}$ according as $\mathcal{C}$ contains both, either or none of $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ (cf. §5.10). Then,

$$\mathbb{E}_m(\sigma;u,v)\equiv\frac{\kappa^{m,m^2M^2}_{\frac{\mathbf{r}}{m}\to\frac{\mathbf{s}}{m}}(\sigma)-\rho_{\Delta(E,m\frac{dx}{y})}(\sigma)}{12}\mod M^2,$$

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

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 $\sigma\in B_3$ and $(u,v)\in\mathbb{Z}^2$, as the congruence assumptions modulo mM^22^{ε}, $m^2M^2e_{\mathcal{C}}$ come to be void (or, hold true for $M=\infty$) when $\mathbf{s}$ is obtained from $\mathbf{r}=(u,v)$ by multiplication of a matrix in $\mathrm{SL}_2(\mathbb{Z})$. In §7, we are led to evaluation of the quantity $\kappa^{m,m^2\infty}_{\frac{\mathbf{r}}{m}\to\frac{\mathbf{s}}{m}}(\sigma)$ through examining specific choices of logarithm 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 $A=\binom{a\,b}{c\,d}\in\mathrm{SL}_2(\mathbb{Z})$, given explicitly by

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

where P_1 and P_2 denote the 1st and 2nd 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 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 by 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 $x = (x_1, x_2) = (\frac{r_1}{m}, \frac{r_2}{m})$. Then, for $\sigma \in B_3$, we have

$$\mathbb{E}_m(\sigma; r_1, r_2) = K_x(A_\sigma) - \Phi_x^{(2)}(A_\sigma) - \frac{1}{12}\rho_\Delta(\sigma). \quad \square$$

Since each of the above three terms $\frac{1}{12}\rho_\Delta(\sigma)$, $\Phi_x^{(2)}(A_\sigma)$ and $K_x(A_\sigma)$ generally has a rational value with denominator, it would be curious 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 of the present paper 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 subsequent authors (cf. e.g., [De89], [Ih90, Ih02], [MS03] etc.) Our approach basically follows a 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 observe closely monodromy permutations of inertia subsets in $\pi_1(E\backslash\{O\})$ distinguished by punctures on a certain family of meta-abelian coverings of $E\backslash\{O\}$. Along with our early works [N95, N99] together with subsequent complementary results such as [N01, N02j, N03j], the author had realized that a 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 that in $\pi_1(\mathbf{P}^1 - \{0, 1, \infty\})$. We hope that our innovation of the bypass object $\mathbb{E}_m(\sigma; u, v)$ in the present paper could propose 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 extended 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 cocycle property but allowing denominators. In genus one case, we should still leave it for future studies to investigate an unknown extension in this 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 subsequent works, we hope to discuss them in more details. 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 Introduction, we should like to mention some related works suggesting further hopeful directions. Good reduction criterion of Oda-Tamagawa (cf. [Od95],[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], R.Hain [Ha97], M.Kim [Ki07], S.Mochizuki [Moc02], J.Stix [Sti08] and H.Tsunogai [Tsu95b, Tsu03], which enlarge (and enrich) our scope on this fundamental object. 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], Bannai-Kobayashi [BK07]. At the time of writing this paper, however, the author does not see explicit links between their works and ours. We hope to see relations with their works in future studies.

The construction of this paper is as follows. In §2, we prepare some terminologies 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 view point of combinatorial group-theoretical treatment. In §4, we review and formulate basic modular forms, especially, Siegel units and Eisenstein series and their behaviors under GL_2-action. In §5, we focus on the universal once-punctured elliptic curves $M_{1,2}^{\omega}$ over the moduli space $M_{1,1}^{\omega}$ 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 this 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).

Acknowledgements. A seminal key idea of relating my old work [N95] with Dedekind sums was first suggested to the author by Tomoyoshi Ibukiyama when we accidentally came across to each other on a train to a Kinosaki conference in 1993, Japan. An original version of the present paper had started as a manuscript entitled "On exterior monodromy representations associated with affine elliptic curves" since 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]), essential part of the present paper has been written up during my participation in the project "Non-Abelian Fundamental Groups in Arithmetic Geometry" organized by J.Coates, M.Kim, F.Pop and M.Saidi at Newton Institute in 2009. In view of the above amount of logbooks on history of this paper, I would like to express my sincere gratitude to all named in the above for their assistance and hospitality during the present work.

2. **Some terminologies on elliptic curves**

In this section, we shall prepare some notations and terminologies on elliptic curves and their moduli space following mainly the formulation found in the paper by N. Katz [K76]. Since we will only be concerned with 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 object.** 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 $A[x,y]/(y^2 = 4x^3 - g_2x - g_3)$ for some $g_2, g_3 \in A$.

The above x, y and g_2, g_3 are uniquely determined on each $\mathrm{Spec}(A) \in \mathcal{U}$ 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

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

where g_2, g_3 are indeterminates. We understand the superscript ω of $M_{1,1}^\omega$ here is 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 0-section O given by $(x : y : z) = (0 : 1 : 0)$.

To see the universal property of $(\mathcal{E}/M_{1,1}^\omega, O, \omega = dx/y)$ 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 $f_{A_i} : \mathrm{Spec}(A_i) \to M_{1,1}^\omega$. By the uniqueness of x, y and g_2, g_3 for each E_{A_i}, one sees that the collection $\{f_{A_i}\}$ patch together to yield a (canonical) morphism $S \to M_{1,1}^\omega$.

It is obvious from the above construction that any $\Gamma(1)$-test object $(E/B, O, \omega)$ can be realized as the pull back of $(\mathcal{E}/M_{1,1}^\omega, O, \omega = dx/y)$ by a unique morphism $S = \mathrm{Spec}(B) \to M_{1,1}^\omega$. Through the pullback 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 these (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) and suppose $S = \mathrm{Spec}(B)$ is a connected and normal. Suppose we are given a geometric point $\bar{b} : \mathrm{Spec}(\Omega) \to S$ (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 $\Omega\{\{t\}\}$, 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 along O allowed 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 $\mathcal{E}/M_{1,1}^\omega$ respectively. Then, applying the Grothendieck-Murre theory

([GM71]), we obtain a commutative diagram of exact sequences of fundamental groups:

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

In fact, the exactness of the bottom sequence follows from the fact that $M_{1,1}^{\omega}(\mathbb{C})$ is $K(\pi,1)$ and the center-triviality of $\pi_1(E \setminus \{O\})$. 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), it turns out that the left horizontal arrows are also injective. This explains the exactness of the above three lines.

2.4. **Weierstrass tangential section.** In the above diagram, we also would 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), which we shall call the *Weierstrass tangential section.* The following argument to construct such a section may be viewed as a simple digest of “tangential morphism” explained in [Ma97] or in a more thorough formulation using log geometry [Moc99], [Ho09]. Here it suffices to argue in the classical context using the device of Grothendieck-Murre [GM71]. Namely, in our case, we may construct a fiber functor of Galois categories $\Phi : \mathrm{Rev}^O((E/O)^\wedge) \to \mathrm{Rev}(S)$ 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 ring 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 the following description of this group. Let $B^{ur} \subset \Omega$ be the universal etale cover of the ring B such that $\mathrm{Aut}(B^{ur}/B)$ is canonically identified with $\pi_1(S,\bar{b})$. Then, the automorphism group of the ring of Puiseux series $\bigcup_n B^{ur}[[t^{1/n}]]$ over $B[[t]]$ gives $\pi_1^O((E/O)^\wedge, \bar{a})$. This means that any connected finite cover Y of $\mathrm{Spf} B[[t]]$ ramified only over $t=0$ is dominated by $\mathrm{Spf} B^{ur}[[t^{1/n}]]$ for some large enough n. But since $B^{ur}[[t^{1/n}]] \otimes_{B[[t]]} B[[t^{1/n}]] = B^{ur}[[t^{1/n}]]^n$ which is etale over $B[[t^{1/n}]]$, it follows that the intermediate cover $Y \otimes_{B[[t]]} B[[t^{1/n}]]$ is also etale over $B[[t^{1/n}]]$. But since the category of finite etale covers over $B[[t^{1/n}]]$ (fixed n) is equivalent to the category of those over B ([GM71] 3.2.4), there corresponds to Y an etale cover $\Phi(Y)$ over $S = \mathrm{Spec}(B)$ which turns out to be determined independently of n. The functor $Y \mapsto \Phi(Y)$ gives our desired fiber functor $\Phi : \mathrm{Rev}^O((E/O)^\wedge) \to \mathrm{Rev}(S)$.

Once the functor Φ is obtained, it is not difficult to check that, for any base points $\bar{b}$ 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 $\bar{b} : \mathrm{Rev}(Y) \to \mathit{Sets}$. In slightly more general, 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 rather a 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.

2.5. **Pro-$\mathcal{C}$ monodromy representation.** Below, we suppose that any full class $\mathcal{C}$ of finite group 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 concerning a $\Gamma(1)$-test object $(E/B, O, \omega)$ and turn now to the exact sequence discussed in §2.3:

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

with the Weierstrass section $s_{\overrightarrow{\mathfrak{w}}}$ (§2.4). Then, by conjugation through $s_{\overrightarrow{\mathfrak{w}}}$, there arises 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 $\Pi_{1,1} = \langle \mathbf{x}_1, \mathbf{x}_2, \mathtt{z} \mid [\mathbf{x}_1, \mathbf{x}_2]\mathtt{z} = 1\rangle$ so that $\mathtt{z}$ generates an inertia subgroup over O. We will take $\mathtt{z}$ 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: $t^{1/n}|_{\mathfrak{a}_{\mathtt{z}}} = \zeta_n^{-1} t^{1/n}$ $(n \geq 1)$ in our later terminology in §6.1. It is easy to see then that $\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}}(\pi_1(S, \bar{b}))$ stabilizes $\langle \mathtt{z}\rangle$ and acts on it by the $\mathcal{C}$-adic cyclotomic character.

The monodromy representation in the maximal abelian quotient of $\Pi_{1,1}(\mathcal{C})$ corresponds to the action on the first etale homology group of the issued elliptic curves. 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. **Multiplication by N isogeny covering.** 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 $\Pi_{1,1} = \langle \mathbf{x}_1, \mathbf{x}_2, \mathtt{z} \mid [\mathbf{x}_1, \mathbf{x}_2]\mathtt{z} = 1\rangle$ is given and fixed, so that $\mathtt{z}$ 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 of N-division points $E_{\bar{b}}[N]$ 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 the 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 labelled 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 the 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 labelled by $\mathbb{Z}_{\mathcal{C}}^2$. 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 $\rho^{\mathcal{C}} : \pi_1(S, \bar{b}) \to \mathrm{GL}(\mathbb{Z}_{\mathcal{C}}^2)$. 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

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

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 changes up to conjugation by an element of $\mathrm{Aut}(S^N/S)$.

With each morphism $\phi : T = \mathrm{Spec}(R) \to S^N$ associated is 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

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

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

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

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

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

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) 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 $\alpha_{\phi'} : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E_{\phi'}[N]$. As similar to (2.7.3-4), the two morphisms $T \to M_{1,1}$ through ϕ, ϕ' are the same, so that after identifying $E_\phi = E_{\phi'}$, we have

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

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)

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

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

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

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 $\{((2\pi i)(\frac{\tau}{N}x + \frac{1}{N}y), \tau) | \tau \in \mathfrak{H}\}$.

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 claim then,

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

Proof. Let τ_0 designate the image of 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 one in regard with equivalences under the action of $\mathbb{Z}^2 \rtimes \mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{C} \times \mathfrak{H}$. It follows then:

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

The interpretation is that the point represented by the elliptic curve $\mathcal{E}_{\tau_0}$ with level structure $\alpha_\phi : (x,y) \mapsto (2\pi i)(\frac{\tau_0}{N}x + \frac{1}{N}y)$ 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 from the matrix A. Namely, the corresponding action of $\rho^N(\sigma)/\pm 1$ on $\mathcal{E}[N]$ must come from $\binom{x}{y} \mapsto \binom{a\,c}{b\,d}\binom{x}{y}$. Hence $\alpha_{\phi'} = \pm\alpha_\phi \circ \binom{a\,c}{b\,d}$, which implies $\rho^N(\sigma) = \pm\binom{a\,c}{b\,d}$ 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 normal affine scheme $S = \mathrm{Spec}(B)$ with associated parameter (x, y, g_2, g_3, t) as in §2.1, 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 consider then the pro-$\mathcal{C}$ monodromy representation $\varphi^{\mathcal{C}}_{\overrightarrow{\mathfrak{w}}_{\bar{b}}} : \pi_1(S, \bar{b}) \longrightarrow \mathrm{Aut}(\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})(\mathcal{C}))$ as in §2.5. Let us 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. Call $\pi^{\mathrm{ab}} := \pi/\pi'$ the abelianization of π. The abelianization map extends to a natural projection of the complete group algebras of π to that of π^{ab}:

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

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 Blanchfied-Lyndon exact sequence of $\mathbb{Z}_{\mathcal{C}}[[\pi^{\mathrm{ab}}]]$-modules:

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

where $\partial(s) := (\frac{\partial s}{\partial \mathbf{x}_1})^{\mathrm{ab}} \oplus (\frac{\partial s}{\partial \mathbf{x}_2})^{\mathrm{ab}}$ 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 $\varphi^{\mathcal{C}}_{\vec{\mathfrak{w}}_{\bar{b}}}$ just by

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

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

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

so that $\sigma(\mathbf{x}_1) \equiv \mathbf{x}_1^{a(\sigma)} \mathbf{x}_2^{c(\sigma)}$, $\sigma(\mathbf{x}_2) \equiv \mathbf{x}_1^{b(\sigma)} \mathbf{x}_2^{d(\sigma)} \bmod \pi'$. Observe then 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

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

Note that, by definition, $\mathcal{S}_{00}(\sigma) = 1$, $G_{00}(\sigma) = 0$, hence $\mathbb{E}^{\mathcal{C}}_m(\sigma; 0, 0) = 0$. One of our principal concerns in this and the following subsections is to examine dependency of $\mathbb{E}^{\mathcal{C}}_m(\sigma; u, v)$ 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*

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

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

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

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

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

Note. In the above notation $\mathrm{Rest}\binom{ab}{cd}.\binom{u}{v}$, the dot between $\binom{ab}{cd}$ and $\binom{u}{v}$ plays separation of matrix component and 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:

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

Then, apply (3.2.2-3) to each of the three factors. Note that for free differential calculus, we can make use of basic laws of Leibniz type as shown in [Ih86b]. Only one nontrivial point is to show a formula like

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

which, however, follows easily by induction for non-negative integers u, and then by the standard argument of continuity. □

Remark 3.4.3. In general, there are no reasons to expect that the values $\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v)$ are periodic in (u,v) with any modulus. But we will see later (see Corollary 6.9.8) that $\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v) \bmod M^2$ $(M\in|\mathcal{C}|)$ 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

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

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

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 held 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 same notations of the above proposition. Since $\mathbb{Z}_{\mathcal{C}}[[\mathbb{Z}_{\mathcal{C}}^2]]$ has no zero-divisors as shown in [Ih99-00], the above Tsunogai's equation implies that only $G_{-1,0}$ determines $G_{0,-1}$ or vice versa.

Proposition 3.4.5. *Let $\sigma\in\pi_1(S,\bar{b})$ with $\rho^{\mathcal{C}}(\sigma)=\binom{ab}{cd}$. 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 $\binom{ab}{cd}.\binom{u}{v}=u\binom{a}{c}+v\binom{b}{d}$.*
(i) It holds that

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

where $\lfloor\frac{\alpha}{m}\rfloor:=-\int_{m\mathbb{Z}_{\mathcal{C}}}d\left(\frac{x^{-\alpha}-1}{x-1}\right)$ for $\alpha\in\mathbb{Z}_{\mathcal{C}}$.
(ii) The values of $\left\{\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v)\mid(u,v)\in\mathbb{Z}_{\mathcal{C}}^2,m\geq 1\right\}$ determine the action of σ on π/π''.

Proof. By simple calculation from definition, it follows that

$$G_{uv}(\sigma) = G_{u+1,v}(\sigma) - (\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v G_{10}(\sigma) + \mathrm{Rest}\binom{ab}{cd}.\binom{u+1}{v} - \mathrm{Rest}\binom{ab}{cd}\binom{u}{v}$$
$$= G_{u+1,v}(\sigma) - (\bar{\mathbf{x}}_1^{-a}\bar{\mathbf{x}}_2^{-c})^u(\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d})^v G_{10}(\sigma) - \bar{\mathbf{x}}_2^{-cu-dv}\frac{\bar{\mathbf{x}}_2^{-c}-1}{\bar{\mathbf{x}}_2-1}\frac{\bar{\mathbf{x}}_1^{-au-bv}-1}{\bar{\mathbf{x}}_1-1}. \tag{3.4.6}$$

Integrating measures represented by the above terms over the subspace $(m\mathbb{Z}_{\mathcal{C}})^2 \subset \mathbb{Z}_{\mathcal{C}}^2$ enables us to find $\int_{C_m(u,v)} dG_{10}(\sigma) - \mathbb{E}_m^{\mathcal{C}}(u+1,v) + \mathbb{E}_m^{\mathcal{C}}(u,v)$ 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 $G_{10}(\sigma) \in \mathbb{Z}_{\mathcal{C}}[[\mathbb{Z}_{\mathcal{C}}^2]]$ from the collection of values $\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v)$ ($(u,v) \in \mathbb{Z}_{\mathcal{C}}^2$, $m \in |\mathcal{C}|$). 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 $\mathcal{S}_{0,-1}(\sigma) = \sigma(\bar{\mathbf{x}}_1)\bar{\mathbf{x}}_1^{-b}\bar{\mathbf{x}}_2^{-d}$ 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 $m \in \mathbb{N}$, $\alpha \in \mathbb{Z}_{\mathcal{C}}$ to designate the pro-$\mathcal{C}$ floor (resp. ceiling) function. Obviously, $\lceil -\frac{\alpha}{m}\rceil = -\lfloor\frac{\alpha}{m}\rfloor$. In fact, it is not difficult to verify the following: If $\alpha = m\beta$, then, $\lceil\frac{\alpha}{m}\rceil = \beta$. 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 $\lceil\frac{\alpha}{m}\rceil = 1 + \frac{\alpha-\langle\alpha\rangle_m}{m}$.

The following proposition allows us to compute $\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v)$ with both u and v divisible by m in $\mathbb{Z}_{\mathcal{C}}$ from the values of $\mathbb{E}_m^{\mathcal{C}}(\sigma;1,0)$, $\mathbb{E}_m^{\mathcal{C}}(\sigma;u+1,v)$ 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 $\rho^{\mathcal{C}}(\sigma) = \binom{ab}{cd}$,*

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

Proof. If we consider terms in the RHS of (3.4.6) as measures on the space $\mathbb{Z}_{\mathcal{C}}^2$, then, under the assumption $(u,v) \in (m\mathbb{Z}_{\mathcal{C}})^2$, 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 effects upon integration over $(m\mathbb{Z}_{\mathcal{C}})^2$. 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

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

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

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

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

A merit to introduce 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*

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

Proof. We start from studying composition rules for G_{10} and G_{01}. Let $\rho(\sigma) = \binom{a\,b}{c\,d}$, $\rho(\tau) = \binom{\alpha\,\beta}{\gamma\,\delta}$ so that $\rho(\sigma\tau) = \binom{a\alpha+b\gamma\;\; a\beta+b\delta}{c\alpha+d\gamma\;\; c\beta+d\delta}$. Then, in π'/π'' we have:

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

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 $\sigma(\mathbf{x}_2)^{-\gamma}\sigma(\mathbf{x}_1)^{-\alpha}\mathbf{x}_1^{a\alpha+b\gamma}\mathbf{x}_2^{c\alpha+d\gamma}$, the latter is equivalent to $G_{\alpha\gamma}(\sigma)\cdot\bar{z} \bmod \pi''$ with $G_{\alpha\gamma}$ is 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

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

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 $\pi_1(M_{1,1}, f(\bar{b}))$ and the above formula can hold true for all elements $\sigma,\tau \in \pi_1(M_{1,1}, f(\bar{b}))$. 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 by ρ of some element $\tau \in \pi_1(M_{1,1}, f(\bar{b}))$. Apply then (3.5.6) to $\sigma = \sigma_1\sigma_2$, then one gets

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

This concludes the proposition. □

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

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

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 $\mathbb{Z}_\mathcal{C}^2$, one derives easily from Prop. 3.5.3 that

$$\mathbb{E}^{\epsilon}_m(\sigma\tau;u,v) = \mathbb{E}^{\rho(\tau)\epsilon}_m(\sigma;u,v) + \chi(\sigma)\mathbb{E}^{\epsilon}_m(\tau;u,v) \qquad (\sigma,\tau\in\pi_1(S,\bar{b}),\ (u,v)\in\mathbb{Z}_\mathcal{C}^2). \tag{3.5.8}$$

3.6. **Measure $\mathcal{E}^{\mathcal{C}}_\sigma$ on the congruence kernel.** In our argument so far, we have not allowed m to move 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 Prop. 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:

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

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 $\sum_{\mathbf{a}\in(\mathbb{Z}/m\mathbb{Z})^2} \mathcal{E}^{\mathcal{C}}_m(\sigma,\mathbf{a})(\sigma)\mathbf{e}_{\mathbf{a}}$, 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 of finite groups $\mathcal{C}$, $\mathcal{C}'$ satisfy $\mathcal{C} \subset \mathcal{C}'$, then 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 in our hand. 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.,*

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

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

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

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 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 $\mathfrak{L}$:

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

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 2nd kind, i.e., without residues; hence the integral is well defined. It is easy to see

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

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 w.r.t. $\mathfrak{L}$, i.e.,

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

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

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

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

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

Proof. These are just 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 $\sigma(z, \tau) = \sigma(z, \mathfrak{L}_\tau)$, $\theta(z, \tau) = \theta(z, \mathfrak{L}_\tau)$. 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 as follows (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 in the 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:

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

where $B_2(T) = T^2 - T + \frac{1}{6}$ is the 2nd 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

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

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.** If $x = (x_1, x_2)$ is fixed to be a pair of rational numbers, then $\theta_x(\tau) := \theta(x_1\tau + x_2, \tau)$ is a holomorphic function on the upper half plane $\mathfrak{H}$ known as the 12-th power of what is called the Siegel function $g_x(\tau)$:

$$g_x(\tau) = -q_\tau^{B_2(x_1)/2} e^{\pi i x_2(x_1-1)}(1-q_z)\prod_{n\geq 1}(1-q_\tau^n q_z)(1-q_\tau^n q_z^{-1}), \quad (z = x_1\tau + x_2).$$

The detailed properties of $g_x(\tau)$ are closely studied in the book [KL81] by Kubert-Lang. Here, we shall collect several properties of them for our later use. Let $m \geq 1$ and assume $x = (r_1/N, r_2/N)$ ($r_1, r_2 \in \mathbb{Z}, N \geq 1$). Then, we consider the condition

$$\mathrm{Q}(x,N,m) : \begin{cases} \text{If } N \text{ is odd, then } mr_1^2 \equiv mr_2^2 \equiv mr_1r_2 \equiv 0 \bmod N. \\ \text{If } N \text{ is even, then } mr_1^2 \equiv mr_2^2 \equiv 0 \bmod 2N,\ mr_1r_2 \equiv 0 \bmod N. \end{cases}$$

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 N if and only if the condition $Q(x, N, 12m)$ holds. In particular, $\theta(x_1\tau + x_2, \tau)$ is modular of level N^2.

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

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

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

Proposition 4.2.2. *Let $x = (x_1, x_2) \in \mathbb{Q}^2$ and $A = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Then, we have*

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

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

Proof. The Siegel function $g_x(\tau)$ is by definition the product of $(2\pi i)\eta(\tau)^2$ and the Klein form $\ell_x(\tau) = e^{-\boldsymbol{\eta}(z,\tau)z/2}\sigma(z, \mathfrak{L}_\tau)$. 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 in the level of g_x. But it 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 Prop.3.3.1 for certain powers of the Dedekind η-function $\eta(\tau)=q_\tau^{1/24}\prod_{n=1}^\infty(1-q_\tau^n)$.

Proposition 4.2.3. *(i) $\eta(\tau)^{24}=\Delta((2\pi i)\mathfrak{L}_\tau)$ is a modular form of weight 12 and level 1.*
(ii) $\eta(\tau)^8$ is a modular form of weight 4 and level 3.
(iii) $\eta(\tau)^6$ is a modular form of weight 3 and level 4.

Proof. This is essentially included in [KL81] Chap.3, Lemma 5.1. We reproduce a proof for the sake of reader's convenience. The general transformation formula of η is :

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

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

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

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

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

Since $8|(1-d^2)$ for $d=odd$, when $4|b,c$, we have $\varepsilon(a,b,c,d)^6=\exp(\frac{3}{2}\pi id)$. Given $A=\big(\begin{smallmatrix}a&c\\c&d\end{smallmatrix}\big)\in\Gamma(4)$, if $c>0$, then 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 $c<0$, then we apply the formula for $-A$. Then, $\varepsilon(-a,-b,-c,-d)^6=i$. But in 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. □

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 $m_1\equiv a_1$, $m_2\equiv a_2 \pmod N$. Note that, in the above formula, if $k\geq 3$ then we do not need $\lim_s$ and the factor $|...|^s$, because $\sum'_{m_1,m_2}1/(m_1\tau+m_2)^k$ converges absolutely and uniformly on each compact sets. 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:

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

where

$$\alpha_\nu(N,k,\mathbf{a})=\begin{cases}\delta(\frac{a_1}{N})\sum'_{m_2\equiv a_2(N)}\frac{1}{m_2^k}, & (\nu=0),\\ \frac{(-2\pi i)^k}{N^k(k-1)!}\sum_{m|\nu\ \frac{\nu}{m}\equiv a_1(N)}m^{k-1}sgn(m)\zeta_N^{a_2m} & (\nu\geq 1).\end{cases}$$

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

$$E_k^{(\mathbf{x})}(\tau):=\frac{(k-1)!}{(2\pi i)^k}\sum_{\bar{a}\in(\mathbb{Z}/N\mathbb{Z})^2} e^{2\pi i(x_1a_2-x_2a_1)}G_k^{(\mathbf{a}\bmod N)}(\tau).$$

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

$$\text{(4.3.2)}\quad E_k^{(\mathbf{x})}(\tau)=-\frac{P_k(x_1)}{k}+\sum_{0<s\in x_1+\mathbb{Z}}\sum_{l=1}^{\infty}s^{k-1}e^{2\pi il(x_2+s\tau)}+\sum_{0<s\in -x_1+\mathbb{Z}}\sum_{l=1}^{\infty}s^{k-1}e^{2\pi il(-x_2+s\tau)},$$

for $k\geq 3$ or $x\neq\mathbf{0}$, while in the exceptional case of $k=2$ and $\mathbf{x}=(0,0)$, the above right hand side should be added by 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 Gaussian notation by $[*]$, define $P_k(t\bmod\mathbb{Z})$ to be $B_k(t-[t])$ 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 see the transformation formulae:

$$\text{(4.3.3)}\qquad G_k^{(\mathbf{a}\bmod N)}(A\tau)=(c\tau+d)^kG_k^{(\mathbf{a}A\bmod N)},$$
$$E_k^{(\mathbf{x})}(A\tau)=(c\tau+d)^kE_k^{(\mathbf{x}A)}.$$

for $A=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$. It follows then 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:

$$\text{(4.3.4)}\qquad \frac{d}{d\tau}\log g_x(\tau)=(-2\pi i)E_2^{(\mathbf{x})}(\tau),\qquad(\mathbf{x}=x\bmod\mathbb{Z}).$$

In §7.3, we will discuss a standard lift of this equation which will play a crucial role in our proof of Theorem B stated in 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 $\Gamma(N)^{arith}$-test object $(E,\beta:\mathbb{Z}/N\mathbb{Z}\times\mu_N\xrightarrow{\sim}E[N],\omega)$ over an R-algebra B, 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,

$$\phi_s(F(E_s,\beta_s,\omega_s))=\left(\frac{2\pi i}{\omega_2}\right)^k f(\tau),$$

where $\tau = \omega_1/\omega_2 \in \mathfrak{H}$ is given as the quotient of a $\mathbb{Z}$-basis (ω_1, ω_2) of the lattice obtained as the collection of period integrals of ω_s along loops on E_x so that $\frac{1}{N}\omega_1 \bmod \mathfrak{L} = \beta((1,1))$, $\frac{1}{N}\omega_2 \bmod \mathfrak{L} = \beta((0, e^{2\pi i/N}))$.

Conversely, suppose we are given an algebraic modular form F of weight k and level N over $R \subset \mathbb{C}$. Then, the corresponding f is given by $f(\tau) = F(\mathbb{C}^\times/(q_{\tau/N})^{N\mathbb{Z}}, \iota, dx/x)$, where $q_{\tau/N} = e^{2\pi i\tau/N}$ and ι is the canonical embedding $\mathbb{Z}/N\mathbb{Z} \times \mu_N \hookrightarrow \mathbb{C}^\times/q_\tau^{\mathbb{Z}}$ with $(a, e^{2\pi ib/N}) \mapsto (q_{\tau/N}^a, e^{2\pi ib/N})$. The value of F at the Tate curve $\mathrm{Tate}(q^N)/R((q))$ gives the $q(= e^{2\pi i\tau/N})$-expansion of f.

The above story may be applied to the modular units and modular forms in 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 N unless $k = 2$ and $\mathbf{x} = \mathbf{0}$. The q-expansion given in (3.4.3) 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 $\Gamma(N)^{arith}$-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 $\Gamma(N)^{arith}$-test object with 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

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

In the similar way, since the modular forms $\Delta = \eta^{24}$, η^8, η^6 which appeared in Prop. 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:

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

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 Prop.4.2.1, $\theta_x(\tau) = g_x(\tau)^{12}$ and its inverse are modular functions of level N^2. Observing the q-expansion, we know that there are corresponding algebraic modular forms $\theta_x^{\pm 1}$ of weight 0 and level N^2 defined over $\mathbb{Q}(\mu_{N^2})$. So, we may apply $\theta_x^{\pm 1}$ to the $\Gamma(N^2)^{arith}$-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 $\mathrm{Spec}(B)$ to the modular curve $Y(N^2)$ of level 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 $\Gamma(N^2)$ whose Fourier coefficients with respect to $e^{2\pi i\tau/N^2}$ are lying in $\mathbb{Q}(\mu_{N^2})$, so that $Y(N^2) = \mathrm{Spec}(\mathcal{O}(\Gamma(N^2)))$. Then by [Sh71] Prop. 6.9, we see

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

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

For the other cases of Prop.4.2.1 where g_x^{12m}, g_x^{4m} or g_x^{3m} becomes a modular function of level N under suitable condition, 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 $D = \{\left(\begin{smallmatrix}1 & 0\\ 0 & d\end{smallmatrix}\right) | d \in (\mathbb{Z}/N\mathbb{Z})^\times\}$, and define the action on $\mathfrak{F}_N$ of each component as follows. Let $f(\tau) \in \mathfrak{F}_N$ whose Fourier expansion in $q_\tau^{1/N}$ has coefficients in $\mathbb{Q}(\mu_N)$. We define the action of $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ by $f \to f|_{{}^tA}$. Identify D with the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ and define its action on $f(\tau)$ by Galois transformation of the Fourier coefficients. It follows, in particular, that

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

The above action is compatible with the context we developed in §2.8-9 as follows. With each $\sigma \in \pi_1(M_{1,1}, \bar{b})$ associated are 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 contained 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 by the homomorphism $\mathfrak{F}_N \to \mathbb{Q}(\mu_N)((q^{1/N}))$, which corresponds to a representative morphism $\phi : \mathrm{Spec}\mathbb{Q}(\mu_N)((q^{1/N})) \to Y(N)$. 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 $\zeta_N \to \zeta_N^d$. □

The above sort of compatibility also extends to the context of $\Gamma(1)$-test object (§2.6) as follows. Suppose that $(E/B, O, \omega)$ is $\Gamma(1)$-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 associated an automorphism $\mathfrak{a}_\sigma^N \in \mathrm{Aut}(S^N/S)$ in §2.7. On the other hand, the image σ' of the 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, apriori, 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 pullback of $M_{1,1}[N]/M_{1,1}$ by $S \to M_{1,1}$ which is preserved by the pullbacks of $\mathfrak{a}^N_{\sigma'}$ ($\sigma \in \pi_1(S, \bar{b})$), ensures the commutativity of

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

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

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

4.6. GL_2**-action on modular units and its refinements.** We are particularly interested in a consequence of the above discussion on the modular units θ_x, g_x^4, g_x^3 of level N^2, $3N^2$, $4N^2$ respectively. First, observing 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 Prop.4.2.2 imply the formula

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

Note that the lower equation of (4.1.4) implies

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

In other words, $\mathrm{GL}_2(\mathbb{Z}/N^2\mathbb{Z})$ has a well defined action on the indices $(\frac{1}{N}\mathbb{Z}/N\mathbb{Z})^2$ of modular units θ_x's. Then, combining (4.5.3) and (4.5.4), we obtain for any $\Gamma(N^2)$-test object (E, α, ω),

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

In exactly 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 product of $(2\pi i)\eta^2$ and the Klein form $\ell_x(\tau)$. As seen in Prop. 4.2.1 and 4.2.3, the function 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 $\ell_x\left(\begin{smallmatrix}\omega_1\\\omega_2\end{smallmatrix}\right)$, the transformation of formulas with respect to $x = (\frac{r}{N}, \frac{s}{N}) \in (\frac{1}{N})^2$, $y = (b_1, b_2) \in \mathbb{Z}^2$ and $A = \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) \in \Gamma(N)$ in [KL] (K2) (K3) p.28 read:

$$\begin{cases} \ell_{x+y}(\left(\begin{smallmatrix}\omega_1\\\omega_2\end{smallmatrix}\right)) = \varepsilon(x, y)\ell_x(\left(\begin{smallmatrix}\omega_1\\\omega_2\end{smallmatrix}\right)), \\ \ell_x(A\left(\begin{smallmatrix}\omega_1\\\omega_2\end{smallmatrix}\right)) = \ell_{xA}(\left(\begin{smallmatrix}\omega_1\\\omega_2\end{smallmatrix}\right)) = \varepsilon_x(A)\ell_x(\left(\begin{smallmatrix}\omega_1\\\omega_2\end{smallmatrix}\right)), \end{cases} \tag{4.6.4}$$

with

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

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

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

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

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

Concerning GL_2-action, invariance of type (4.6.1) or Prop. 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

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

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

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 the Grothendieck-Teichmüller theory was Belyi'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 $\hat{F}_2 := \pi_1(\mathbf{P}^1_{\overline{\mathbb{Q}}} - \{0, 1, \infty\})$. 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:

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

Usually, we fix an embedding of $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, and take $\mathbf{x}$, $\mathbf{y}$ as loops illustrated as below:

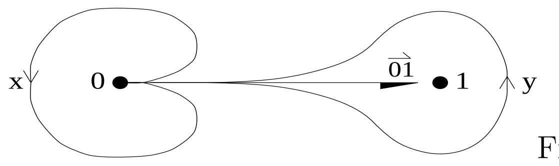


Figure 1

and the above standard lift (Belyi's lift of $G_{\mathbb{Q}}$ into $\mathrm{Aut}(\hat{F}_2)$) is understood geometrically by 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 in 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 version/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 $\mathbb{I}\Gamma$ 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 informations 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 by a series of works by Y.Ihara and his colleagues [Ih86a], [Ih86b], [IKY87], [A89], [C89], [Ih99-00], [Ih02], [MS03]. Some other studies of this direction have also been investigated, e.g., in a series of works [NT03-06], [NTY10].

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

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

where

$$g_2(q)=20\Big(-\frac{B_4}{8}+\sum_{n\geq1}\sigma_3(n)q^n\Big), \tag{5.2.1}$$

$$g_3(q)=\frac{7}{3}\Big(-\frac{B_6}{12}+\sum_{n\geq1}\sigma_5(n)q^n\Big). \tag{5.2.2}$$

($B_4=-1/30$, $B_6=1/42$ are the Bernoulli numbers.) Let $\bar q$ the generic geometric point over $S_q:=\mathrm{Spec}\mathbb{Q}((q))$ valued in the Puiseux power series field

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

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 semi-direct 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) is in the form:

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

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 Neron polygons of Deligne-Rapoport type, we introduced suitable generators $\mathbf{x}_1,\mathbf{x}_2,\mathtt{z}$ of $\Pi_{1,1}:=\pi_1((\mathrm{Tate}(q)\otimes\Omega\setminus\{O\},\overrightarrow{\mathfrak{w}}_{\bar q})$ with $[\mathbf{x}_1,\mathbf{x}_2]\mathtt{z}=1$ so that $\mathtt{z}$ 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 $(\chi(\sigma),\mathfrak{f}_\sigma)\in\widehat{GT}$:*

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

(This theorem was shown for $\mathcal{C}=\{$all finite groups$\}$, hence holds for 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.

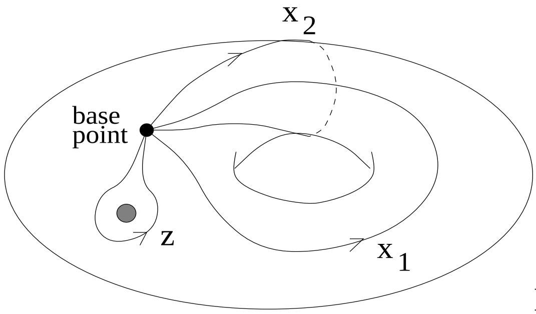


Figure 2

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 $T_i = \bar{\mathbf{x}}_i - 1$ $(i = 1, 2)$.

Theorem 5.2.6 ([N99] Th. 3.3 and Th. 3.5)**.** *Consider $\mathcal{E}_\sigma^{(p)} \in \mathbb{Z}_p[[T_1, T_2]]$ for the Tate curve* 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 Soule character defined by the properties:

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

In fact, in [N99] we gave proofs in twofold; one using the explicit formula given in [N95], and one using the formula of Magnus-Gassner type. In the next section, we shall generalize the explicit formula for finite level's $\mathbb{E}_m^{\mathcal{C}}$ $(m \in |\mathcal{C}|)$.

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 object $(E/B, O, \omega)$ with an extra section $P : B \to E$ disjoint from O.

It is also often useful to consider $M_{1,2}^\omega$ 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

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

by the variable transformation

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

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

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

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 has been given in [NTY10], where used is a modified version of $\mathfrak{M}$ (written $\mathcal{M}$ in loc. cit.) 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 the braid configuration spaces. Let $\mathbf{A}_u^n \setminus D$ denote the space of monic polynomials of degree n in variable u with no multiple roots (here D is understood the discriminant locus), and let $(\mathbf{A}_u^n \setminus D)_0$ denote its subspace of those with second highest coefficient vanishing.

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

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

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

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

(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 are given as $S_1 = -(T_1+T_4)(T_2+T_3)$, $S_2 = -(T_1+T_3)(T_2+T_4)$, $S_3 = -(T_1+T_2)(T_3+T_4)$. (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 4 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

$$\begin{array}{rccc} 4\iota : & (\mathbf{A}^3 \setminus D)_0 & \longrightarrow & M_{1,1}^\omega \\ & \gamma(u) & \longmapsto & y^2 = -4\gamma(-x), \end{array}$$

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

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

where horizontal arrows give isomorphisms of schemes.

Since there is a well known deformation retract of Tschirnhaus type between the spaces $\mathbf{A}^n \setminus D$ and $(\mathbf{A}_u^n \setminus D)_0$, 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 $\mathbf{A}^n \setminus D$, 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 $v = (v_1, \dots, v_n)$ 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 basepoint $v = (0, t^{n-1}, \dots, t^2, t)$ 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 presented as the profinite completion of the Artin braid group B_n which has standard generators $\tau_1, \dots, \tau_{n-1}$ with braid relations $\tau_i\tau_j = \tau_j\tau_i$, $\tau_i\tau_{i+1}\tau_i = \tau_{i+1}\tau_i\tau_{i+1}$ $(i = 1, \dots, n-1, i+1 < j)$, 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 $\sigma \in G_{\mathbb{Q}}$:

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

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 by $(0, t^3, t^2, t)$ 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 $(0, t^4 - t^5, t^3 - t^5) \sim (0, t^4, t^3) \sim \bar{b}_3$. Thus we may regard $\mathcal{F}(\bar{b}_4) \approx \bar{b}_3$ from the Galois theoretic point of view. Thus we obtain a $G_{\mathbb{Q}}$-compatible homomorphism

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

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

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

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 Tate elliptic curve over $\mathbb{Q}((q))$ given in Theorem 5.2.4.

NB. The above choice of generators follow the way taken in [N99] and differs from [NTY10](2.9), [NT-II] (4.2.2), [Na-I] §4 with '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 $\mathbb{C}/\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and P is a point $(\wp(z), \wp'(z))$, where $\wp$ is the Weierstrass $\wp$-function with respect to the lattice

$\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\tau := \omega_1/\omega_2 \in \mathfrak{H}$. Set $e_1 := \wp(\frac{\omega_1}{2})$, $e_2 := \wp(\frac{\omega_2}{2})$ and $e_3 := \wp(\frac{\omega_1+\omega_2}{2})$. It is known that there is a canonical choice of a square root of $e_2 - e_1$ given by

$$\sqrt{e_2 - e_1} = \frac{\pi}{\omega_2}\prod_{n=1}^{\infty}(1-q^{2n})^2(1+q^{2n-1})^4 \quad (q = q_\tau^{1/2} = e^{\pi i \tau}). \tag{5.5.1}$$

See [Fr1916] p.406. Let $\mathrm{sn}(z)$, $\mathrm{cn}(z)$, $\mathrm{dn}(z)$ denote the Jacobian elliptic functions with fundamental parallelogram given by $2K = \omega_2\sqrt{e_2-e_1}$, $2iK' = \omega_1\sqrt{e_2-e_1}$.

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 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, then the classical formula of Cardano-Ferrari tells us that the issued four solutions are obtained as $\frac{1}{2}(\sqrt{S_1}+\sqrt{S_2}+\sqrt{S_3})$ for any choice of the 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 [Fr1916] p.389) for $w = \sqrt{e_2-e_1}z$ that

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

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 of Tate-Weierstrass point and $\bar{b}_4$.** Let us fit the Tate elliptic curve $\mathrm{Tate}(q)/\mathbb{Q}((q))$ in $M_{1,2}^{\omega} \to M_{1,1}^{\omega}$ to obtain a pair of tangential points ($\overrightarrow{\mathfrak{w}}_{\bar{q}}$, $\bar{q}$) on ($M_{1,2}^{\omega}$, $M_{1,1}^{\omega}$) respectively. We shall connect the inverse Mordell transformation of $\overrightarrow{\mathfrak{w}}_{\bar{q}}$ to the standard base point $\bar{b}_4$ on $\mathbf{A}_u^4 \setminus D$ by using Proposition 5.5.2. Observe that the defining coefficients $g_2(q)$, $g_3(q)$ of $\mathrm{Tate}(q)$ in (5.2.1-2) are those $g_2(\omega_1,\omega_2)$, $g_3(\omega_1,\omega_2)$ applied to the lattice generated by $\omega_1 = (2\pi i)\tau$, $\omega_2 = (2\pi i)$. In this case, $\sqrt{e_2-e_1} \sim \frac{1}{2i}$. We look at the point (T_4,T_3,T_2,T_1) on $\mathbf{A}_v^4 \setminus \Delta$, which, by parallel transportation, gives an equivalent tangential base point to

$$\begin{aligned}&(0, T_3-T_4, T_2-T_4, T_1-T_4)\\ &\quad\sim \frac{\sqrt{e_2-e_1}}{2}\left(0, \frac{2(\mathrm{dn}(w)-1)}{\mathrm{sn}(w)}, \frac{2(\mathrm{cn}(w)-1)}{\mathrm{sn}(w)}, \frac{2(\mathrm{cn}(w)+\mathrm{dn}(w))}{\mathrm{sn}(w)}\right) \sim \left(0, \frac{k^2z}{8}, \frac{z}{8}, \frac{2}{z}\right),\end{aligned}$$

where

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

and we used in the last equivalence the well known Taylor expansions (cf. [Fr1916] p.399)

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

The Weierstrass tangential base point is defined by $t=\frac{-2x}{y}$ which is, in analytic case, equivalent to $\frac{-2\wp}{\wp'}\sim z$. Since these equivalences hold algebraically at the level of formal series, we see that

$$\mathfrak{M}^{-1}(\overrightarrow{\mathfrak{w}}_{\bar q})\sim(0,2tq,\frac{t}{8},\frac{2}{t})\sim(0,t_1t_2t_3,t_2t_3,t_3) \tag{5.6.2}$$

with $t_1=16q$, $t_2=\frac{t^2}{16}$, $t_3=\frac{2}{t}$ in the Ihara-Matsumoto coordinates (cf. [IM95]) of $\mathbf{A}_v^4-\Delta$ such that $t_1,t_2\in\mathbf{A}^1-\{0,1\}$, $t_3\in\mathbf{A}^1-\{0\}$. Define a path $\varepsilon=(\varepsilon_1,\varepsilon_2,\varepsilon_3):\bar b_4\rightsquigarrow\mathfrak{M}^{-1}(\overrightarrow{\mathfrak{w}}_{\bar q})$ on $\mathbf{A}_u^4\setminus D$ as the projection image of the path from (t_1,t_2,t_3) to the above $(16q,t^2/16,2/t)$ on $\mathbf{A}_v^4\setminus\Delta$ by using positive roots of 16 and 2. Then, we have

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

for $\sigma\in G_{\mathbb{Q}}$.

Let us also calculate the image $\mathcal{F}(\mathfrak{M}^{-1}(\overrightarrow{\mathfrak{w}}_{\bar q}))$ on $\mathbf{A}_u^3\setminus D$. Using the above (5.6.2), the Ferrari resolvents on $\mathbf{A}_v^3\setminus\Delta$ can be seen as $(S_1,S_2,S_3)\sim(-\frac14-4q,-\frac14-\frac{t^2q}{4},-4q-\frac{t^2q}{4})$ which is also equivalent to

$$(0,S_2-S_1,S_3-S_1)\sim(0,4q,\frac14)\sim(0,s_1s_2,s_2). \tag{5.6.4}$$

We observe that the image $\mathcal{F}(\varepsilon)$ looks like a segment path $\overrightarrow{01}\rightsquigarrow\frac{1}{16}\overrightarrow{01}$ on the s_1-line. This kind of avatar of the principal coefficient 16 of the modular function $\lambda(\tau)$ (5.6.1) was observed in [N99-02] §4.10, and has continuously appeared in our works [N97], [NS00] etc.

5.7. **Standard splittings of $\pi_1(M_{1,2}^\omega)$.** Below, we shall switch our working place to $M_{1,2}^\omega$-side of the Mordell transformation (5.4.1). We write by the same symbols the images of the base point $\bar b_4$ and the above path ε on $\mathbf{A}_u^4\setminus D$ on $M_{1,2}^\omega$ by $\mathfrak{M}$. Let $\beta_1(\sigma)\in\pi_1(M_{1,2}^\omega,\bar b_4)$, $\mathfrak{s}_1(\sigma)\in\pi_1(M_{1,2}^\omega,\overrightarrow{\mathfrak{w}}_{\bar q})$ denote the elements corresponding to $\sigma\in G_{\mathbb{Q}}$. Also we represent the images of generator elements of $\hat B_4$ by $\mathfrak{M}$ by the same symbols, which are in the first sense loops based at $\bar b_4$ but also may be regarded as loops based at $\overrightarrow{\mathfrak{w}}_{\bar q}$ by conjugation by ε. Under these abuse of notations, we may rephrase the above formula (5.6.3) as

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

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:

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

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

Next we shall look at the kernel of projection $\pi_1(M_{1,2}^\omega, \overrightarrow{\mathfrak{w}}_{\bar{q}}) \to \pi_1(M_{1,1}^\omega, \bar{q})$ which is identified with the Ferrari kernel $\ker(\pi_1(\mathcal{F}))$ (5.4.3). In [N99-02] §4, we considered $\pi_1(M_{1,2}) = \pi_1(M_{1,2}^\omega)/\langle\omega_4\rangle$ 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 $G_\mathbb{Q}$-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 $\pi_1(M_{1,2}^\omega, \overrightarrow{\mathfrak{w}}_{\bar{q}})$.

At this stage, it is probably appropriate to expose how the above formulas can consistently be combined to deduce a key formula of Theorem 5.2.4, namely, to the fact that $\mathfrak{s}_1(\sigma)$ acts on $\mathbf{x}_2$ by

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

In fact, since $\mathbf{x}_2 = \tau_1\tau_3^{-1}$, one can easily see from (5.7.2) that

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

Now, recall the relation (IV) satisfied by $G_\mathbb{Q}$ in $\widehat{GT}$ which was found in [N99-02] Theorem 4.16. It (equivalently) implies (cf. also [NS00] p.543) the equation

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

The above $(*)$ follows then immediately after noting $\omega_3^2 = \mathbf{z}\omega_4$.

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., splitting of $\pi_1(M_{1,2}^\omega, \overrightarrow{\mathfrak{w}}_{\bar{q}})$ with it:

Proposition 5.7.3. *The image of the Weierstrass section*

$$s_{\overrightarrow{\mathfrak{w}}} : \pi_1(M_{1,1}^\omega, \bar{q}) \longrightarrow \pi_1(M_{1,2}^\omega, \overrightarrow{\mathfrak{w}}_{\bar{q}})$$

coincides with the subgroup $\langle\tau_1, \tau_2\rangle \rtimes \mathfrak{s}_1(G_\mathbb{Q})$*. 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* $\pi_1(M_{1,1}^\omega, \bar{q}) = \hat{B}_3 \rtimes \mathfrak{s}_0(G_\mathbb{Q})$ *at* $\bar{q}$ *is given by*

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

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

We will give a proof of this proposition later in §7.

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 $\mathcal{O}^\omega_{1,1}[x,y]/(4x^3-g_2x-g_3-y^2)$. 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 two 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 the above, we have already selected (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 ρ^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 $(E^N/\widetilde{\mathcal{O}^\omega_{1,1}}^N, \alpha:(\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E^N[N], \omega^N)$ with the pair of base points $(\overrightarrow{\mathfrak{w}}_{\bar{q}^N}, \bar{q}^N)$ as pointed subjects 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-functions and Eisenstein series introduced in §4 can be lifted to certain elements of $\widetilde{\mathcal{O}^\omega_{1,1}}$. In fact, by Prop. 4.2.1, the Siegel function g_x ($x\in(\frac{1}{N}\mathbb{Z}/\mathbb{Z})^2$) is a modular function of level $12N^2$ with $q^{1/N}$-expansion in $\mathbb{Q}(\mu_{2N^2})$. By Prop. 4.2.3, the square of eta function η^2 is a modular form of weight 1 and level 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 N^2 with $q^{1/N}$-expansion 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 $(E^N/\widetilde{\mathcal{O}^\omega_{1,1}}^N, \alpha:(\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E^N[N], \omega^N)$ in $\widetilde{\mathcal{O}^\omega_{1,1}}$. Note that an algebraic form of level N may also be of level MN that, 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 by $\widetilde{\mathcal{O}^\omega_{1,1}}\to\Omega\subset\overline{\mathbb{Q}}\{\{q\}\}$ at $\bar{q}$.

5.9. **Power roots of 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 the leading term $q^{1/12N}$. Put also $\Delta^{1/N}:=((\eta^2)^{1/N})^{12}$.

The Kummer character

$$\rho_\Delta : \pi_1(M^\omega_{1,1}, \bar{q}) \longrightarrow \hat{\mathbb{Z}}$$

is defined by

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

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, it holds that*

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

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 principal coefficient 1, so ρ_Δ vanishes. On the discrete geometric fundamental group B_3, we interpret ρ_Δ as the rounding 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 ($x = (\frac{r_1}{m}, \frac{r_2}{m})$), recall that the principal term of $q^{1/12m^2}$-expansion reads by definition (see §4.2) as:

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

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

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

and let $(1 - \zeta_m^{r_2})^{1/N}$ be the principal branch having the least argument as the complex number. Certainly, we define $g_x^{1/N}$ for $x = (\frac{r_1}{m}, \frac{r_2}{m})$ with $(r_1, r_2) \in [0, m)^2 - \{\mathbf{0}\}$ so that the principal coefficient of $q^{1/12m^2N}$ is $\zeta_{2N}\zeta_{2Nm^2}^{r_2(r_1-1)}$ with multiplied by the $(1 - \zeta_m^{r_2})^{1/N}$ when $r_1 = 0$. But we take a slightly more careful process using the complex 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, which 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 that whose Fourier expansion at $i\infty$ has principal coefficient $e^{\pi(1+x_2(x_1-1))/N}$ with multiplied by $(1 - e^{2\pi i x_2})^{1/N}$ when $x_1 = 0$. For general $(x_1, x_2) = (\frac{r_1}{m}, \frac{r_2}{m}) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$, pick a sufficiently small real number $\frac{1}{m}\varepsilon > 0$, and trace the branch of $g_\xi^{1/N}$ from $\xi = (\varepsilon, \varepsilon)$ in the already defined region $[0, 1)^2 - \{0\}$ along the piecewise line path $\xi = (\varepsilon, \varepsilon) \longrightarrow (\varepsilon, \varepsilon + x_2) \longrightarrow (\varepsilon + x_1, \varepsilon + x_2)$, and then take the limit $\varepsilon \to 0$: the process may be summarized as

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

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, namely $(g_x^{1/MN})^N = g_x^{1/M}$ for $M, N \in N$. 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 approximating $\mathbb{E}_m^{\mathcal{C}}(\sigma)$-invariant, which we will discuss in details 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 $\Pi_{1,1}$, and 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

$$\begin{pmatrix} s_1 \\ s_2 \end{pmatrix} \equiv \rho^{\mathcal{C}}(\sigma) \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \quad \mathrm{mod}\ m^2 M e_{\mathcal{C}}$$

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

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

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), (4.6.7-8), $(g_x)^{c_l}|_{\mathfrak{a}_\sigma} = \zeta \cdot (g_y)^{c_l}$ $(\zeta \in \mu_{e_l})$, 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

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

by

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

An easy observation: Each l-component of $\kappa_{x\to y,\mathcal{C}}^{m,m^2M}(\sigma)$ for prime $l \in |\mathcal{C}|$ can be interpreted as $\kappa_{x\to y,(l)}^{m,m^2M}(\sigma)$, i.e., that 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 $\sigma \in \pi_1(M_{1,1}^{\omega}, \bar{q})$ is given. Therefore $\kappa_{x\to y,\mathcal{C}}^{m,m^2M}$ does not form a single function on $\pi_1(M_{1,1}^{\omega}, \bar{q})$ 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 $\kappa_{x\to x,\mathcal{C}}^{m,m^2M}$ gives an additive character (even independent of M). We will discuss about it in more details 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 normal ring $B(\supset \mathbb{Q})$ 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 $r : S \to M_{1,1}^{\omega}$ together with $r_E : E \setminus \{O\} \to M_{1,2}^{\omega}$. Pick any path γ from $r(\bar{b})$ to the standard basepoint $\bar{q}$ 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 $M_{1,2}^{\omega}$ lifting γ. Note that this uniquely determines a lift $r_E(\overrightarrow{\mathfrak{w}}_{\bar{b}})^{\sim}$ on $\widetilde{M_{1,2}^{\omega}}$ 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 $H^0(E\setminus\{O\}, \mathcal{O}) = B[x, y]/(y^2 = 4x^3 - g_2 x - g_3)$ 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 $\widetilde{M_{1,2}^{\omega}}$ and $E \setminus \{O\}$ over $M_{1,2}^{\omega}$ is, in general, not connected. But since there is a canonical bijection between the fiber set $\widetilde{M_{1,2}^{\omega}}(r_E(\overrightarrow{\mathfrak{w}}_{\bar{b}}))$ 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

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

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

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

As usual, for any two pointed Galois etale covers $f : (Y, \bar{y}) \to (X, \bar{x})$ 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 $\mathfrak{a}_{Y/X}(\sigma)(\bar{y}) = \sigma(\bar{y})$. Observe also that the maximal unramified subextension B^{ur} of B inside the above $\widetilde{\mathcal{O}}_E$ whose spectrum S^{ur} is naturally pointed by $\tilde{\mathfrak{w}}_{\bar{b}}$. Thus, each of the spectrums of those rings in the inclusion series

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

has a standard base point valued in Ω which we will write $\bar{b}, \bar{b}^N, \bar{b}^{\mathcal{C}}, \bar{b}^{ur}$ respectively. From the anti-isomorphism $\mathfrak{a}_{S^{ur}/S} : \pi_1(S, \bar{b}) \to \mathrm{Aut}(S^{ur}/S)$, we have a standard isomorphism $\pi_1(S, \bar{b}) \xrightarrow{\sim} \mathrm{Aut}(B^{ur}/B)$ written $\sigma \mapsto (*|\mathfrak{a}(\sigma))$ The above homomorphism $\widetilde{r_E}^{*}$ induces by restriction a ring homomorphism $\widetilde{\mathcal{O}_{1,1}^{\omega}} \longrightarrow B^{ur}$. 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, $\frac{1}{12}\rho_\Delta$, $\kappa_{x\to y}^{m,m^2M,\mathcal{C}}$ make senses on $\pi_1(S, \bar{b})$ which factor through $\pi_1(M_{1,1}^{\omega}, \bar{q})$ via the representative morphism $r : S \to M_{1,1}^{\omega}$ 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 $\Pi_{1,1} = \pi_1(\mathrm{Tate}_{\bar{q}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{q}})$ to $\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ (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 $E_{\bar b}\setminus\{O\}$. From this, 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 $\mathbf{r}\equiv(u,v)$ mod mM^22^ε (where $\varepsilon=0,1$ according as $2\nmid M$, $2|M$ respectively) and $x=(\frac{r_1}{m},\frac{r_2}{m})\to y=(\frac{s_1}{m},\frac{s_2}{m})$ is $\rho^{\mathcal{C}}(\sigma)$-admissible at level m modulo m^2M^2. Then,*

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

Since $\Delta(E,m\omega)=m^{-12}\Delta(E,\omega)$, the above right hand side can be written in the form Theorem A of 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 a full class of all finite groups (cf. Remark 3.6.4). By the Chinese Remainder Theorem, we may also assume $M=l^n$ for a prime l. Below, we shall start arguments to prove this theorem in form of 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.

6.3. **Geometrically abelian coverings.** Let N be an integer in $|\mathcal{C}|$. The isogeny $E\xrightarrow{N}E$ by multiplication by N gives an etale B-cover of degree N^2. Let us write this covering as $E^N_B\to E$ to distinguish the copy E^N_B from E/B. We have specified differential forms both on E/B and E^N_B which will be written ω and ω_N respectively. (We need to reserve the notations ω_1,ω_2 also for the two components of fundamental period integrals in $\mathbb{C}$. There would not be chances to confuse them with the ω_N introduced here.) The pullback of ω to E^N_B is then $N\omega_N$. The associated parameter of E^N_B 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 by the original ones for E/B by classically well known N-division formulas of elliptic functions. Especially, t_N can be expanded in the power series of the form $Nt(1+tB[[t]])$.

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

$$E^N_0:=E^N_B\setminus E[N]\longrightarrow E_0:=E\setminus\{O\}.$$

The etale neighborhoods of zero sections O in both E^N_0 and E_0 are canonically isomorphic, i.e., $\mathrm{Rev}^O((E^N_B/O)^\wedge)\approx\mathrm{Rev}^O((E/O)^\wedge)$. From this we obtain a unique tangential base point $\overrightarrow{\mathfrak{w}}_N$ valued in $\Omega\{\{t\}\}$ near the zero section of E^N_0 that lifts the Weierstrass base point $\overrightarrow{\mathfrak{w}}_{\bar b}$ on E_0. Note that Weierstrass base point $\overrightarrow{\mathfrak{w}}^N_{\bar b}$ of E^N_0 valued in $\Omega\{\{t_N\}\}$ itself has to be distinguished from $\overrightarrow{\mathfrak{w}}_N$. But since $t_N\sim Nt$ and since we have a standard power root system $\{\sqrt[n]{N}>0\}$, we can fix an isomorphism of Puiseux power series

$$\Omega\{\{t_N\}\}\xrightarrow{\sim}\Omega\{\{t\}\}\qquad(t_N^{1/n}\mapsto\sqrt[n]{N}t^{1/n},\ n=1,2,3,\dots)$$

which defines a standard path from $\overrightarrow{\mathfrak{w}}_N$ to $\overrightarrow{\mathfrak{w}}^N_{\bar b}$. The fundamental group $\pi_1(E^N_0,\overrightarrow{\mathfrak{w}}_N)$ is a subgroup of $\pi_1(E_0,\overrightarrow{\mathfrak{w}}_{\bar b})$, and is naturally isomorphic to $\pi_1(E^N_0,\overrightarrow{\mathfrak{w}}^N_{\bar b})$ via the above path $\overrightarrow{\mathfrak{w}}_N\rightsquigarrow\overrightarrow{\mathfrak{w}}^N_{\bar b}$.

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 $(n = 1, 2, ...)$ 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). Define then

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

Note that $\Delta(E_B^N, O, \omega_N) \in B^\times$. 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 $div(\Theta_{l,N})$ of $\Theta_{l,N}$ is given by:

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

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

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

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

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 $(E_0^N)_{\bar{b}} = E_{\bar{b}} \setminus E_{\bar{b}}[N]$ 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 induced level ml-structure, and let $(\mathbb{Z}/ml\mathbb{Z})_0^2$ be the subset of $(\mathbb{Z}/ml\mathbb{Z})^2$ consisting of the pairs $\mathbf{a} = (a_1, a_2)$ such that $l\mathbf{a} \neq \mathbf{0}$. 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 with the support of $div(\Theta_{l,ml})$, the value $\Theta_{l,ml}(\alpha^{ml}(\mathbf{a}))$ lies in $(B^{ml})^\times$. In fact, the classical formula (cf. e.g. [KL81] §10, Th. 2.2) gives

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

for $\mathbf{a} \in (\mathbb{Z}/ml\mathbb{Z})_0^2$, where $x = (\frac{r_1}{ml}, \frac{r_2}{ml}) \in \mathbb{Q}^2$ such that $r_i \in [0, ml]$ $(i = 1, 2)$ are integers with $a_i = r_i \bmod ml$.

Now, we shall consider distributions of inertia subsets in $\pi_1(Y^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$. Since the support of the divisor of $\Theta_{l,ml}$ is in $E^N[l]$, the inertia groups over $P_{\mathbf{a}}$ $(\mathbf{a} \in (\mathbb{Z}/ml\mathbb{Z})_0^2)$ splits into a union of l^k conjugacy classes of inertia subgroups in $\pi_1(Y^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$.

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 generated by

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

Let X^{ml,l^k} be the integral closure of $E_B^{ml} - E[l]$ 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 $\beta_{u,v}^{ml,l^k} : S^{ur} \to X^{ml,l^k}$. Composing these two, one obtains a unit of S^{ur} which will be written as

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

On the other hand, the B^{ur}-point $\beta_{u,v}^{ml,l^k} : S^{ur} \to X^{ml,l^k}$ of $X^{ml,l^k}/B$ lies over the B^{ml}-point of $E_B^{ml} - E[l]$ 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 $x = (\frac{r_1}{ml}, \frac{r_2}{ml}) \in \mathbb{Q}^2$. Then, we have*

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

where θ^{1/l^k} is the pull-back by $(M_{1,1}^\omega)^{ur} \to S^{ur}$ of the corresponding element introduced in the previous section.

Proof. By functoriality of construction, it suffices to work in the complex analytic models with $E \setminus \{O\} = M_{1,2}^\omega$ and $\bar{b} = \bar{q}$ on $M_{1,1}^\omega$. First, we shall see that one of the inertia group over $P_{\mathbf{a}}$ is generated by z_{uv} with $(u, v) \in \hat{\mathbb{Z}}^2$ satisfying $(u, v) \equiv \mathbf{a} \bmod N$. The starting inertia element $\mathsf{z} = \mathsf{z}_{00}$ determines the origin puncture $O = P_{\mathbf{0}}$ on $E^{ml} \setminus E[ml]$ which is tangent to the tangential base point $\overrightarrow{\mathfrak{w}}^{ml}$ represented by (the image of) the real analytic small region $\{(\varepsilon\tau+\varepsilon) \mid 0<\varepsilon \ll 1\}$. Note that the puncture $P_{\mathbf{a}}$ is obtained as those points tangent to the regions obtained from $\overrightarrow{\mathfrak{w}}^{ml}$ by continuously tracing the paths $\mathbf{x}_1^u\mathbf{x}_2^v$ for any $u,v\in\mathbb{Z}$, $(u,v)\equiv\mathbf{a} \bmod m$. The automorphism $\mathfrak{a}_{\mathbf{x}_1^u\mathbf{x}_2^v}\in\mathrm{Aut}(E^{ml}\setminus E[ml])$ is determined by $\mathbf{x}_1^u\mathbf{x}_2^v(\overrightarrow{\mathfrak{w}}^{ml})=\mathfrak{a}_{\mathbf{x}_1^u\mathbf{x}_2^v}(\overrightarrow{\mathfrak{w}}^{ml})=\mathfrak{a}_{\mathbf{x}_2}^v\mathfrak{a}_{\mathbf{x}_1}^u(\overrightarrow{\mathfrak{w}}^{ml})$. Extend $\mathfrak{a}_\gamma\in\mathrm{Aut}(E^{ml}\setminus E[ml])$ to a unique automorphism $\overline{\mathfrak{a}_\gamma}$ of E^{ml}. Observing

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

we see that the element $\mathsf{z}_{uv}:=\mathbf{x}_2^{-v}\mathbf{x}_1^{-u}\mathsf{z}\mathbf{x}_1^u\mathbf{x}_2^v$ ($(u,v)\equiv\mathbf{a} \bmod m$) 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 $\pi_1(E_{\bar b}^{ml}\setminus E[ml],\overrightarrow{\mathfrak{w}}_{\bar b}^{ml})$.

Next we consider the cover $Y^{ml,l^k}\to E^{ml}\setminus E[ml]$ and its partial compactification $X^{ml,l^k}\to E^{ml}\setminus E[l]$. As an element of $\widetilde{\mathcal{O}_{1,2}^{\omega}}$, $\Theta_{l,ml}^{1/l^k}$ is taken so that its principal coefficient in z (in the complex model) coincides with $(\frac{\Delta^{l^2}}{l^{12}}z^{12})^{1/l^k}$. Expressing $\Theta_{l,ml}$ as quotients of theta function (4.1.6) with non-holomorphic factors cancelled, the principal factor in z is contributed from factors "$(1-q_z)$" when $(x_1,x_2)\in[0,\frac{1}{l})^2$ for the denominator and $(x_1,x_2)\in[0,1)^2$ for the numerator. This observation together with (6.5.1) settles the claim when $(r_1,r_2)\in[0,m)^2$. For general (r_1,r_2), we need to interpret the place where the inertia element $\mathsf{z}_{\mathbf{r}}=(\mathbf{x}_2^{-r_2}\mathbf{x}_1^{-r_1})\mathsf{z}(\mathbf{x}_1^{r_1}\mathbf{x}_2^{r_2})$ detects. As in the similar account to the above paragraph, it must be obtained as the puncture tangent to $\mathbf{x}_1^{r_1}\mathbf{x}_2^{r_2}(\overrightarrow{\mathfrak{w}}_Y)$ whose location is detected by tracing the continuous move of the tangential base point $\overrightarrow{\mathfrak{w}}_Y$ represented by a real analytic small region $\{z^{1/l^k}=(\varepsilon\tau+\varepsilon)^{1/l^k} \mid 0<\varepsilon\ll 1\}$ along the paths $\mathbf{x}_2^{r_2}$ first and then $\mathbf{x}_1^{r_1}$ afterwards. From this, it turns out that our choice of the branch of power roots of Siegel units (§5.10) keeps the assertion of our lemma valid even for general (r_1,r_2). □

6.6. **Estimating difference of sections.** We now work in the extension of the profinite groups

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

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 $Y^{ml,l^k}\to E_B^{ml}\setminus E[ml]$ is connected, defined over B and totally ramified over O. Taking $n\to\infty$, 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 $\pi_1(S,\bar b)$. Since $\pi_1(Y^{ml,l^\infty},\overrightarrow{\mathfrak{w}}_Y)\cap\langle\mathsf{z}\rangle=\{1\}$, 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 the σ. Let us compare the difference between $\bar\sigma$ and σ_m. Note that $\bar\sigma$ is also contained in the normalizer of $\langle\mathsf{z}\rangle$, and $\pi_1(E\setminus E[ml],\overrightarrow{\mathfrak{w}}_{ml})$ contains this normalizer. The difference $\bar\sigma\sigma_m^{-1}$ is thus belongs to $\pi_1(E_{\bar b}\setminus E_{\bar b}[ml],\overrightarrow{\mathfrak{w}}_{ml})$. Since $\pi_1(E_{\bar b}\setminus E[ml],\overrightarrow{\mathfrak{w}}_{ml})/\pi_1(Y_{\bar b}^{lm,l^\infty},\overrightarrow{\mathfrak{w}}_Y)$ 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.

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

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

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

Since $t_{ml} \sim t/ml$, we get

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

in the respective case $l \geq 5, = 3, = 2$. By the definition, the 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 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 $E_B^{ml} \setminus E[l] \to \mathbf{G}_{\mathrm{m}}$, the pull-backed scheme Y^{ml,l^k} still has a canonical model over S. In particular, we have an exact sequence

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

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 $E_B^{ml} - E[l]$ 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 $\mathsf{z} \in \Pi_{1,1} = \pi_1(E \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ lies in $\pi_1(E_B^{ml} \setminus E[ml], \overrightarrow{\mathfrak{w}}_{ml})$ which contains $\pi_1(Y_{\bar{b}}^{ml,l^k}, \overrightarrow{\mathfrak{w}}_Y)$ as a normal subgroup. The conjugation by z induces a permutation of $\cup_Q \mathfrak{I}_Q$, hence that of $\mathfrak{Q}^{ml,l^k}$.

On the other hand, we also have the conjugate action by a preimage σ_m of σ by 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 z_{uv} (Definition 6.5.2) lies also in $\mathfrak{Q}^{ml,l^k}$. In the following proposition, we examine the above twofold conjugate actions on those inertia subsets including those 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 $\rho(\sigma) = \binom{ab}{cd} \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ 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 $\mathbf{s} \equiv (ar_1 + cr_2, br_1 + dr_2)$ mod $m^2 l^k$.

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 up to modulo l^k by either of the following equivalent conditions.*

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

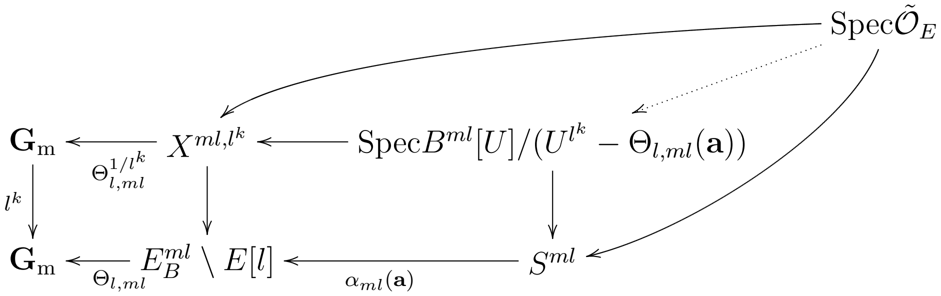
(2) $\dfrac{\left(\Theta_{l,ml}^{1/l^k}(r_1,r_2)\right)|_{\mathfrak{a}_\sigma}}{\Theta_{l,ml}^{1/l^k}(s_1,s_2)} = \zeta_{l^k}^{-c_l(l^2-1)\nu}$,
where $c_l = 12, 4, 3$ *according as* $l \geq 5, = 3, = 2$.

(3) $\zeta_{e_l l^k}^{\rho_\Delta(\sigma)} \left(\dfrac{(g_x^{1/l^k})^{c_l l^2}}{(g_{lx}^{1/l^k})^{c_l}} \right) \Bigg|_{\mathfrak{a}_\sigma} = \zeta_{l^k}^{-c_l(l^2-1)\nu} \left(\dfrac{(g_y^{1/l^k})^{c_l l^2}}{(g_{ly}^{1/l^k})^{c_l}} \right)$,
where $x = (\frac{r_1}{ml}, \frac{r_2}{ml})$, $y = (\frac{s_1}{ml}, \frac{s_2}{ml}) \in \mathbb{Q}^2$, 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 $\langle \mathsf{z} \rangle$, the conjugate action by 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 up to 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 labelling of the set $\mathfrak{Q}^{ml,l^k}$. Recall first that X^{ml,l^k} is the integral closure of $E_B^{ml} - E[l]$ 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} which are dominated by $\mathrm{Spec}\tilde{\mathcal{O}}_E = \widetilde{E_0}$. The partial compactifications $E_0^{ml} \subset E_B^{ml} \setminus E[l]$ and $Y^{ml,l^k} \subset X^{ml,l^k}$ fit 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 $\Theta_{l,ml}^{1/l^k}(\mathbf{a}) \in (B^{ur})^\times$ as the image of U in $B^{ur} \subset \tilde{\mathcal{O}}_E$. Now, the carriers of the points $\mathfrak{Q}^{ml,l^k}$ as schemes over $S^{ur} = \mathrm{Spec}(B^{ur})$ are of the form

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

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

Each (physical) component $\mathrm{Spec}(B^{ur}[U]/(U-\zeta_{l^k}^b\Theta_l(\mathbf{a})^{1/l^k}))$ 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 labellings of our issued sets:

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

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 $(S^{ur})^\times$ 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 $\mathtt{z}\in\Pi_{1,1}$ and $\sigma_m\in\pi_1(S,\bar b)$ on $\mathfrak{Q}^{ml,l^k}$ in geometric terms.

On one hand, the standard generator $\mathtt{z}\in\Pi_{1,1}=\pi_1(E\setminus\{O\},\overrightarrow{\mathfrak{w}}_{\bar b})$ lies in $\pi_1(E_B^{ml}\setminus E[ml],\overrightarrow{\mathfrak{w}}_{ml})$ which also induces an automorphism $\mathfrak{a}_{\mathtt{z}}$ of $Y^{ml,l^k}\otimes_B B^{ur}$ which extends naturally to an automorphism $\overline{\mathfrak{a}_{\mathtt{z}}}$ of $X^{ml,l^k}\otimes_B B^{ur}$. Write by the same symbol $\overline{\mathfrak{a}_{\mathtt{z}}}$ for 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 by $\sigma_m(*)$, as it corresponds to a preimage σ_m of σ by 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* $Q\in\mathfrak{Q}^{ml,l^k}$, $\mathfrak{I}_{\overline{\mathfrak{a}_{\mathtt{z}}}^\nu(Q)}=\mathtt{z}^{-\nu}\mathfrak{I}_Q\mathtt{z}^\nu$.

Proof. This is only a general theory (but needs a careful treatment on conventions of path compositions). Consider the pointed universal etale cover $\tilde Y$ of $(E_B^{ml}\setminus E[ml])_{\bar b}$ dominating Y^{ml,l^k} and partial compactification $\tilde X$ as the projective limit of the integral closures of finite layers over $(E_B^{ml}\setminus E[l])_{\bar b}$. The profinite set $\tilde{\mathfrak{Q}}:=\tilde X-\tilde Y$ is regarded as the set of cusps. Then, for each $\gamma\in\pi_1(E_B^{ml}\setminus E[ml])_{\bar b},\overrightarrow{\mathfrak{w}}_{ml})$, let $\overline{\mathfrak{a}_\gamma}$ denote the restriction on $\tilde{\mathfrak{Q}}$ 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 $Q\in\tilde{\mathfrak{Q}}$, i.e., $\overline{\mathfrak{a}_\gamma}(Q)=Q$, then, generally it follows from our convention (cf. (2.7.1)) that

$$\begin{aligned}\overline{\mathfrak{a}_{\mathtt{z}^{-1}\gamma\mathtt{z}}}(\overline{\mathfrak{a}_{\mathtt{z}}}(Q)) &= \overline{\mathfrak{a}_{\mathtt{z}\cdot\mathtt{z}^{-1}\gamma\mathtt{z}}}(Q)\\ &= \overline{\mathfrak{a}_{\gamma\mathtt{z}}}(Q)\\ &= \overline{\mathfrak{a}_{\mathtt{z}}}(\overline{\mathfrak{a}_\gamma}(Q))=\overline{\mathfrak{a}_{\mathtt{z}}}(Q).\end{aligned}$$

The statement is only a reflection of this computation. □

Thus, we established the existence of $\nu=\nu_{\mathbf{r},\mathbf{s}}^{ml,l^k}$ and their coincidence in the conditions (1) and (2). The condition (3) is only a restatement of (2) after 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 completed. □

6.8. **Count character for winding numbers.** Now, recalling that $Y_{\bar{b}}^{ml,l^\infty}$ is given as the Kummer cover over $E_{\bar{b}} \setminus E_{\bar{b}}[ml]$, we have the following exact sequence

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

where $c_l \cdot \vartheta_{ml} : \pi_1(E_{\bar{b}} \setminus E_{\bar{b}}[ml]) \to \mathbb{Z}_l$ (with $c_l = 12, 4, 3$ according to $l \geq 5, = 3, = 2$ respectively) counts rounding numbers of the images of paths by $\Theta_{l,ml}$ around zero. As observed in [N95] (2.6), it is easy to show that ϑ_{ml} is given by

$$\vartheta_{ml}(\mathbf{x}_1^{ml}) = -l(l-1)/2; \tag{6.8.1}$$

$$\vartheta_{ml}(\mathbf{x}_2^{ml}) = l(l-1)/2; \tag{6.8.2}$$

$$\vartheta_{ml}(\mathbf{z}_{\mathbf{r}}) = \begin{cases} (l^2-1), & \mathbf{r} \in ml\mathbb{N}^2, \\ -1, & \mathbf{r} \in m\mathbb{N}^2 \setminus ml\mathbb{N}^2, \\ 0, & \text{otherwise}. \end{cases} \tag{6.8.3}$$

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 $\pi_1((E_B^{ml} \setminus E[ml])_{\bar{b}}, \overrightarrow{\mathfrak{w}}_{ml})$ is generally not invariant under the conjugate action of $\pi_1((E_B \setminus \{O\})_{\bar{b}}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$, especially we do not expect a formula like $\vartheta_{ml}(x\mathbf{z}x^{-1}) = \vartheta_{ml}(\mathbf{z})$.

If (u,v), $(u',v') \in \hat{\mathbb{Z}}^2$ satisfies 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 $\pi_1((E_B^{ml} \setminus E[ml])_{\bar{b}}, \overrightarrow{\mathfrak{w}}_{ml})$. The following lemma gives an estimate of its value via ϑ_{ml}.

Lemma 6.8.4. *If (u,v), $(u',v') \in \hat{\mathbb{Z}}^2$ satisfies the congruence $(u,v) \equiv (u',v')$ mod 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 $(u,v) \equiv (u',v')$ mod 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 α, $\beta \in \hat{\mathbb{Z}}$. 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 variable separate type, we may 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 accounts that $\varepsilon = ml^{k+1}\alpha$, we see that both 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. 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 the similar way to the above case. This completes the proof. □

Corollary 6.8.5. *If (u,v), $(u',v') \in \hat{\mathbb{Z}}^2 \setminus (m\hat{\mathbb{Z}})^2$ satisfy the congruence $(u,v) \equiv (u',v')$ mod ml^{k+1}, then, z_{uv} and $\mathsf{z}_{u'v'}$ determine the same cusp on Y^{ml,l^k}. If $l \geq 3$, then the assumption may be replaced by $(u,v) \equiv (u',v')$ mod ml^k.*

Proof. To prove the proposition in this case, it suffices to show that the difference of conjugating factors for z_{uv} and $\mathsf{z}_{u'v'}$ to 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 z_{uv} with a fixed residue class of (u,v) modulo ml gives the same cusp in $\mathfrak{Q}^{ml,l}$. From this remark, especially, one should notice that the points of the form Q_{uv}^{ml,l^k} $(u,v) \in \hat{\mathbb{Z}}^2 \setminus (m\hat{\mathbb{Z}})^2$ 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 $(r_1,r_2) \equiv (u,v)$ mod ml^{2n+1}. Then, by Proposition 6.8.4, the cusps determined by z_{uv} and $\mathsf{z}_{\mathbf{r}}$ are the same on $Y^{ml,l^{2n}}$. Set $x = (\frac{r_1}{m}, \frac{r_2}{m})$, $y = (\frac{s_1}{m}, \frac{s_2}{m})$, so that $x \to y$ is $\rho(\sigma)$-admissible at level m modulo m^2l^{2n} from x, and $l^{-1}x \to l^{-1}y$ is $\rho(\sigma)$-admissible at level ml modulo m^2l^{2n-2} (in fact, still modulo m^2l^{2n}). Proposition 6.7.2 (3) implies, then

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

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

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

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

We shall 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 $\mathbf{t} \equiv \mathbf{s}$ mod m^2l^{2n}, and put $\mathbf{x_t} = \mathbf{x}_2^{-t_2}\mathbf{x}_1^{-t_1}$, $\mathbf{x_s} = \mathbf{x}_2^{-s_2}\mathbf{x}_1^{-s_1}$ so that $\mathsf{z}_{\mathbf{t}} = \mathbf{x_t}\mathsf{z}\mathbf{x_t}^{-1}$, $\mathsf{z}_{\mathbf{s}} = \mathbf{x_s}\mathsf{z}\mathbf{x_s}^{-1}$. Then, we calculate

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

for some $w \in \Pi_{1,1}''$. By Corollary 6.8.5, the inertia elements $\mathsf{z}_{\mathbf{t}}$ and $\mathsf{z}_{\mathbf{s}}$ 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 $\sigma_m\mathsf{z}_{\mathbf{r}}\sigma_m^{-1}$ is of the form $h\mathsf{z}^{-\nu}\mathsf{z}_{\mathbf{s}}^{\chi(\sigma)}\mathsf{z}^{\nu}h^{-1}$ with $\nu = \nu_{\mathbf{r},\mathbf{s}}^{ml,l^{2n}}(\sigma)$. Since $\langle\mathsf{z}_{\mathbf{r}}\rangle$ is self-centralizing in $\pi_1(E_{\bar{b}} \setminus \{O\}, \overrightarrow{\mathfrak{w}}_{\bar{b}})$ and since $\pi_1(Y_{\bar{b}}^{ml,l^\infty}, \overrightarrow{\mathfrak{w}}_Y) \supset \langle\mathsf{z}_{\mathbf{r}}, \Pi_{1,1}''\rangle$, we see that $\nu = \nu_{\mathbf{r},\mathbf{s}}^{ml,l^{2n}}(\sigma)$ satisfies

$$\mathsf{z}^{-\nu} \equiv \mathsf{z}^{\xi_m(\sigma)}\{G_{\mathbf{r}}(\sigma)\cdot\mathsf{z}\}(\mathbf{x_t}\mathbf{x_s}^{-1}) \bmod \pi_1(Y_{\bar{b}}^{ml,l^{2n}}, \overrightarrow{\mathfrak{w}}_Y). \tag{6.9.3}$$

Then, apply ϑ_{ml} mod l^{2n} to both sides of (6.9.2). Noticing that $\vartheta_{ml}(\mathbf{x_t}\mathbf{x_s}^{-1}) \equiv 0$ mod l^{2n} by Lemma 6.8.4, we find

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

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

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

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

Summing up both sides with $\sum_{i\geq 0} l^{2i}\times(6.9.5)_i$, we obtain

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

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

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

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

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

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 evidences (such as §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).

Proof. Suppose first that (u,v), $(u',v')\in\hat{\mathbb{Z}}^2\setminus(m\hat{\mathbb{Z}})^2$ satisfy $(u,v)\equiv(u',v')$ mod $mM^2 2^\varepsilon$. Then, the congruence $\mathbb{E}_m^{\mathcal{C}}(\sigma;u,v)\equiv\mathbb{E}_m^{\mathcal{C}}(\sigma;u',v')$ mod 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 6.8.5. 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 $u-u'\equiv v-v'\equiv 0$ mod $M^2 2^\varepsilon$. □

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:

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

and depends only on the class of x in $\mathbb{Q}^2/\mathbb{Z}^2$. 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

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

The distribution relation of θ_x in Prop. 4.1.5 ensures that the sequence $\{\boldsymbol{\mu}^{\mathcal{C}}_m(\sigma)\}_{m\in|\mathcal{C}|}$ forms a measure $\boldsymbol{\mu}^{\mathcal{C}}\in\mathbb{Z}_{\mathcal{C}}[[(\mathbb{Z}_{\mathcal{C}})^2]]$ on $\mathbb{Z}^2_{\mathcal{C}}$ with no constant term (i.e., the image by the augmentation map $\varepsilon:\mathbb{Z}_{\mathcal{C}}[[(\mathbb{Z}_{\mathcal{C}})^2]]\to\mathbb{Z}_{\mathcal{C}}$ vanishes): $\varepsilon(\boldsymbol{\mu}^{\mathcal{C}})=0$. Note also that, by Prop. 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*

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

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 them, we obtain the equation

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

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 on $\mathbf{a}\in(\mathbb{Z}/m\mathbb{Z})^2\setminus\{0\}$, while the RHS (set $Y_m(\sigma)$) does not depend on $\mathbf{a}$. Hence, for any prime power $l^i\in|\mathcal{C}|$, we obtain $l^2Y_{ml^{i+1}}(\sigma)=Y_{ml^i}(\sigma)$. 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

$$\mathcal{E}_m(\sigma,\mathbf{a})=\begin{cases}\boldsymbol{\mu}^{\mathcal{C}}_m(\sigma,\mathbf{a})=\boldsymbol{\mu}^{\mathcal{C}}_m(\sigma,-\mathbf{a}), & (\mathbf{a}\neq0),\\ \frac{1}{12}\rho_\Delta(\sigma)-\rho_m(\sigma), & (\mathbf{a}=0).\end{cases}\tag{6.10.5}$$

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

Proof of Proposition 3.6.5. By using the composition law (3.5.8) repeatedly, in general, we have for $\sigma,\tau\in\pi_1(S,\bar{b})$ and $\epsilon\in\mathrm{GL}_2(\mathbb{Z}_{\mathcal{C}})$,

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

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

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

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

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 from the definition of twisted invariants in §3.5. If $\rho(\sigma)^{-1} = (\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix})$, then, calculations with (3.5.2) yields:

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

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

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

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 statement of proposition. □

Proof of Proposition 5.7.3. We have only to show that the restriction of Weierstrass tangential section $s_{\vec{\mathfrak{w}}} : \pi_1(M^\omega_{1,1}, \bar{q}) \to \pi_1(M_{1,2}, \overrightarrow{\mathfrak{w}}_{\bar{q}})$ to geometric part maps $\tau_1, \tau_2 \in \hat{B}_3$ to those in $\hat{B}_4$ respectively. Since the image of $s_{\vec{\mathfrak{w}}}$ is in the normalizer of $\langle \mathsf{z} \rangle$, without loss of generality, we may set $s_{\vec{\mathfrak{w}}}(\tau_1) = \tau_1\mathbf{z}^{c_1}$, $s_{\vec{\mathfrak{w}}}(\tau_2) = \tau_2\mathbf{z}^{c_2}$ for some $c_1, c_2 \in \mathbb{Z}$. The commutativity of $\mathsf{z} = (\omega_3)^2\omega_4^{-1}$ and the braid relation $\tau_1\tau_2\tau_1 = \tau_2\tau_1\tau_2$ allows 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 $s_{\vec{\mathfrak{w}}}(\sigma) = (\tau_1\tau_2)^6\mathbf{z}^{6c} = \mathbf{z}^{1+6c}\omega_4$. 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 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 shall 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 $B_3 = \langle \tau_1, \tau_2 | \tau_1\tau_2\tau_1 = \tau_2\tau_1\tau_2 \rangle$, whose generators τ_1, τ_2 are given standard identification as elements of $\pi_1(M^\omega_{1,1}(\mathbb{C}), \bar{q})$ (§5.4-7). For any given full class of finite groups $\mathcal{C}$, we have a pair of elementary characters:

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

Recall that, in our setting of notational conventions, $\rho^{\mathcal{C}}$ maps τ_1, τ_2 to $(\begin{smallmatrix}1 & 0 \\ -1 & 1\end{smallmatrix})$, $(\begin{smallmatrix}1 & 1 \\ 0 & 1\end{smallmatrix})$ 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 part of the congruence kernel $\pi_1(M_{1,1}^{\omega,\mathcal{C}},\bar{q}^{\mathcal{C}})=\ker(\rho^{\mathcal{C}})$ must be annihilated by ρ_Δ. But if we restrict the range of σ to the discrete fundamental group $B_3=\pi_1(M_{1,1}^{\omega}(\mathbb{C})^{an},\bar{q})$, $(\subset \hat{B}_3)$, 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 computing $\mathbb{E}_m(\sigma;u,v)$ for $\sigma\in B_3$ and $(u,v)\in\mathbb{Z}^2$.

7.2. **Generalized Dedekind sum formula.** In the beautiful work [St87], G.Stevens gave interpretation of the Rademacher function on $\mathrm{GL}_2(\mathbb{Q})^+$ and its generalizations by using 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 of weight 2 in our notation. (A generalization to higher weights and its arithmetic properties is also discussed in [N03], which we hope to continue to work in a subsequent work to this paper.)

Definition 7.2.1. The generalized Rademacher function of weigh 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

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

so that it factors through $\mathrm{PSL}_2(\mathbb{Z})$ for the case $c<0$. Here, P_1 and P_2 are the periodic Bernoulli functions same as in §4.3. The last term in the above description for the case $c>0$ is called 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 has in general 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 $[x]^o$, $\mathsf{P}_1^{\vdash}(x)$ denote respectively the "mild Gaussian symbol", the "right continuous periodic sawtooth function" defined by

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

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

$$K_x(A):=C_x-C_{xA},$$

where

$$C_x:=\frac{1}{2}+\frac{x_2(x_1-1)}{2}-\mathsf{P}_1^{\vdash}(x_2)\cdot[x_1]^o.$$

The main result of this section is the following

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

$$\mathbb{E}_m(\sigma;r_1,r_2)=K_x(A_\sigma)-\Phi_x^{(2)}(A_\sigma)-\frac{1}{12}\rho_\Delta(\sigma),$$

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 details later in Proposition 7.5.1.

Most part of this section will be devoted to the proof of the above theorem. Our basic policy 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 $\frac{\mathbf{r}}{m}\to\frac{\mathbf{s}}{m}$ modulo m^2M^2 becomes 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 argue the evaluation of $\mathbb{E}_m(\sigma;u,v)$ in the complex analytic model §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 $(r_1,r_2)=(i-4,j-4)\in[-3,3]^2(\subset\mathbb{Z}^2)$:

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

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

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

The consequent right hand side of 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 σ is, in fact, equal to $\tau_1^{-2}\tau_2^6\tau_1^2\tau_2(\tau_1\tau_2)^{-3}$) is then:

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

By Theorem 7.2.3, we conclude that the components of the above matrix coincide with those of $(\mathbf{E}_3(\sigma, ; i-4, j-4))_{i,j=1}^7$, except for $\frac{*}{4}$ at (i,j)-components with $i-1 \equiv j-1 \equiv 0$ mod $m=3$. Generally, exceptional gaps between both sides of 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 Theorem 6.2.1, we need to identify the branch of power roots of Siegel units $g_x(\tau)$ $x=(x_1,x_2) \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ in the complex model. This can be attained by identifying the branch of $\log g_x$, which, in view of the equation (4.3.4), requests us to determine a suitable constant term for the indefinite integral of the Eisenstein series $E_2^{(\mathbf{x})}$ of weight 2 ($\mathbf{x} = x$ mod $\mathbb{Z}$). 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

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

Comparing this with the infinite product form of g_x (cf. §4.2), we obtain the following relation between them:

$$g_x(\tau) = e^{\pi i} e^{\pi i x_2(x_1-1)} \eta_x(\tau) e^{-2\pi i [x_1](x_2-\frac{1}{2})} \left[e^{\pi i P_1(x_2)}\right]^{\delta_{x_1\in\mathbb{Z}}}, \tag{7.3.3}$$

where $\delta_{x_1\in\mathbb{Z}} = 1, 0$ according as $x_1 \in \mathbb{Z}$ or not 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 a "half of G.Stevens' lift" given in his book [St82] (cf. §2.3, Def. 2.3.1) as follows:

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

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

In view of (7.3.3), in the home region $x = (x_1, x_2) \in (0,1)^2$, $g_x(\tau)$ 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 take a principle so as 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 along $\mathbf{x}_2^{r_2}$ first and then along $\mathbf{x}_1^{r_1}$ afterwards". For this purpose, we shall choose a branch of $\log g_x(\tau)$ so as to be continuous on the following region (the complex plane minus $((-\infty,0)\cup(1,+\infty))\times\mathbb{Z}$ with limits from the right (above) in $\lim\limits_{\varepsilon\to 0+} \log g_{x_2+\varepsilon}$ for $x_1 \notin \mathbb{Z}$, $x_2 \in \mathbb{Z}$.

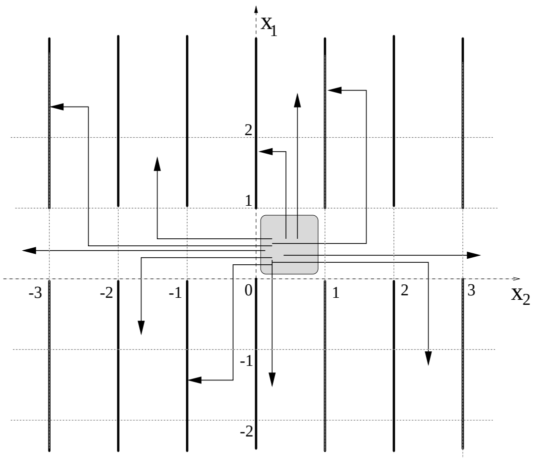


Figure 3

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 loose 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 $\psi^{St}(\tau)$ is counted as

$$-\sum_k e^{2\pi i x_2 k} + \sum_k e^{-2\pi i x_2 k} = \log(1 - e^{2\pi i x_2 k}) - \log(1 - e^{-2\pi i x_2 k}) = 2\pi i(x_2 - \frac{1}{2}).$$

Therefore, to keep continuity of our lift $\log g_x(\tau)$, everytime x_1 goes up across an integer value, we need to add extra $-2\pi i(x_2 - \frac{1}{2})$. This explains the term $-2\pi i(x_2 - \frac{1}{2})[x_1]$. 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 value of upper or lower limits at every discontinuous point. Finally, after reaching the nearest unit square, one may want to arrive at destination with $x_2 \in \mathbb{Z}$ from above. So we substitute $\mathsf{P}_1^{\vdash}(x_2)$ for $P_1(x_2)$. Consequently, our choice of logarithm of Siegel units can be summarized as

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

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 settle 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 $x = (\frac{r_1}{m}, \frac{r_2}{m})$, $y = (\frac{s_1}{m}, \frac{s_2}{m})$ 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 have now

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

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

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

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

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

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 the 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 $\rho(\sigma)=\binom{a\,b}{c\,d}\in\mathrm{SL}_2(\mathbb{Z})$ and for $(k_1,k_2)\in\mathbb{Z}^2$, we have*

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

Observe in the last term of the above expression that $k_1(ack_1+a-c-1)+k_2(bdk_2+b-d+1)$ always has a value of an even integer, since a and c (resp. b and d) have different parity from $ad-bc=1$.

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

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

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

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

where $A={}^t\rho(\sigma)=\binom{a\,c}{b\,d}$. It is easy to see that terms of $K_{(\frac{u+1}{m},\frac{v}{m})}(A)-K_{(\frac{1}{m},\frac{0}{m})}(A)$ can be classified into three family: a quadratic form in k_1, k_2, a linear form in k_1 and a linear form in k_2. After simple computation, we obtain from it those terms of the RHS of the proposition formula together with $-(ak_1+bk_2)\left\lfloor\frac{c}{m}\right\rfloor$ which is cancelled out 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 $\mathbb{E}_m(\sigma;, u, v)$ on $(u, v) \in \mathbb{Z}^2$ by means of their original definition given in §3. These examples are also useful to check 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 the action of the Weierstrass lift $s_{\vec{\varpi}}(\sigma)$ 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

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

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

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

Case $\sigma = \tau_2^\alpha$ $(\alpha \in \mathbb{Z})$. In this case, the Weierstrass lift $s_{\vec{\varpi}}(\sigma)$ acts by $\mathbf{x}_1 \mapsto \mathbf{x}_1$ and $\mathbf{x}_2 \mapsto \mathbf{x}_2\mathbf{x}_1^\alpha$, and hence $\mathcal{S}_{uv}(\sigma) = (\mathbf{x}_2\mathbf{x}_1^\alpha)^{-v}\mathbf{x}_1^{\alpha v}\mathbf{x}_2^v$. From this 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 $(m\hat{\mathbb{Z}})^2$ yields then:

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

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 $(u,v)\in[-6,6]^2$:

$$
\Big(\mathbb{E}_3(\tau_2,i-7,j-7)\Big)_{i,j=1}^{13}=\begin{bmatrix}
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3\\
-1&-1&-1&0&0&0&0&0&0&-1&-1&-1&-3
\end{bmatrix}.
$$

Case $\sigma=\tau_1\tau_2\tau_1$. In this case, the Weierstrass lift $s_{\vec{\mathfrak{w}}}(\sigma)$ 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 it holds that

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

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

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

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

$$
\Big(\mathbb{E}_3(\tau_1\tau_2\tau_1,i-7,j-7)\Big)_{i,j=1}^{13}=\begin{bmatrix}
6&6&6&3&3&3&0&0&0&-3&-3&-3&-6\\
4&4&4&2&2&2&0&0&0&-2&-2&-2&-4\\
4&4&4&2&2&2&0&0&0&-2&-2&-2&-4\\
4&4&4&2&2&2&0&0&0&-2&-2&-2&-4\\
2&2&2&1&1&1&0&0&0&-1&-1&-1&-2\\
2&2&2&1&1&1&0&0&0&-1&-1&-1&-2\\
2&2&2&1&1&1&0&0&0&-1&-1&-1&-2\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0\\
-2&-2&-2&-1&-1&-1&0&0&0&1&1&1&2\\
-2&-2&-2&-1&-1&-1&0&0&0&1&1&1&2\\
-2&-2&-2&-1&-1&-1&0&0&0&1&1&1&2
\end{bmatrix}.
$$

Case $\sigma = \tau_1\tau_2$. In this case, the Weierstrass lift $s_{\vec{\mathfrak{w}}}(\sigma)$ 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 taking integration over $(m\hat{\mathbb{Z}})^2$, we find:

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

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

$$\Big(\mathbb{E}_3(\tau_1\tau_2, i-7, j-7)\Big)_{i,j=1}^{13} = \begin{bmatrix} 3 & 3 & 3 & 2 & 2 & 2 & 0 & 0 & 0 & -3 & -3 & -3 & -7\\ 1 & 3 & 3 & 1 & 2 & 2 & 0 & 0 & 0 & -2 & -3 & -3 & -5\\ 1 & 1 & 3 & 1 & 1 & 2 & 0 & 0 & 0 & -2 & -2 & -3 & -5\\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & -2 & -2 & -2 & -5\\ -1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & -1 & -2 & -2 & -3\\ -1 & -1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & -1 & -2 & -3\\ -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -3\\ -3 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1 & -1\\ -3 & -3 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & -1\\ -3 & -3 & -3 & -1 & -1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & -1\\ -5 & -3 & -3 & -2 & -1 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 1\\ -5 & -5 & -3 & -2 & -2 & -1 & 0 & 0 & 0 & 1 & 1 & 0 & 1\\ -5 & -5 & -5 & -2 & -2 & -2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Errata for [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 for [N99]
On p.204, p.213 figures should be inserted
(same ones as §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}

References

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

[As01] M.Asada, The faithfulness of the monodromy representations associated with certain families of algebraic curves, J. Pure and Applied Algebra, **159**, 123-147.

[BK06] K.Bannai, S.Kobayashi, Algebraic theta functions and the p-adic interpolation of Eisenstein-Kronecker numbers, arXiv:math/0610163.

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

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

[BL94] A.Beilinson, A.Levin, Elliptic Polylogarithms, in "Motives" (U.Jannsen, L.Steven, J.-P.Serre eds.), Proc. Symp. in Pure Math. **55**, Parts 2, 123–192.

[C89] R.Coleman, Anderson-Ihara theory: Gauss sums and circular units, Adv. Stud. in Pure Math. **17** (1989), 55–72.

[De89] P.Deligne, Le Groupe Fondamental de la Droite Projective Moins Trois Points, in "Galois group over $\mathbb{Q}$" (Y.Ihara, K.Ribet, J.-P.Serre eds.), MSRI Publ. Vol. 16 (1989), 79–297.

[Dr90] V.G.Drinfeld, On quasitriangular quasi-Hopf algebras and a group closely connected with $Gal(\bar{Q}/Q)$, Algebra i Analiz **2** (1990), 149–181 (in Russian); *English transl. in* Leningrad Math. J. **2(4)** (1991) 829–860.

[Fr1916] R. Fricke, Die Elliptische Funktionen und ihre Anwendungen, Erster Teil, Teubner in Leipzig, 1916.

[F10] H. Furusho, Pentagon and hexagon equations, Ann. of Math., **171** (2010), 545-556.

[GR71] A.Grothendieck, M. Raynaud, Revêtement Etales et Groupe Fondamental (SGA1), Lecture Note in Math. **224**, Springer, Berlin Heidelberg New York 1971.

[GM71] A. Grothendieck, J.P. Murre, The tame fundamental group of a formal neighborhood of a divisor with normal crossings on a scheme, Lect. Notes in Math. **208** Springer (1971).

[G84] A.Grothendieck, Esquisse d'un Programme, 1984 *in Geometric Galois Actions I, P.Lochak, L.Schneps (eds.)* London Math. Soc. Lect. Note Ser. **242** (1997) 5–48.

[Ha97] R.Hain, Infinitesimal presentations of the Torelli groups, J. Amer. Math. Soc. **10** (1997), 597-651.

[Ho09] Y.Hoshi, On the fundamental groups of log configuration schemes, Math. J. Okayama Univ. **51** (2009), 1–26.

[Ih86a] Y.Ihara, Profinite braid groups, Galois representations, and complex multiplications, Ann. of Math. **123** (1986), 43–106.

[Ih86b] Y.Ihara, On Galois representations arising from towers of coverings of $\mathbf{P}^1 - \{0, 1, \infty\}$, Invent. Math. **86** (1986), 427–459.

[IKY87] Y.Ihara, M.Kaneko, A.Yukinari, On some properties of the universal power series for Jacobi sums, in "Galois Representations and Arithmetic Algebraic Geometry", Advanced Studies in Pure Math. **12** (1987), 65–86.

[Ih90] Y.Ihara, Braids, Galois groups, and some arithmetic functions, Proc. Intern. Congress of Math. Kyoto 1990, 99–120.

[IM95] Y. Ihara, M. Matsumoto, On Galois actions on profinite completions of braid groups, in "Recent Development on the Inverse Galois Problem", M. Fried et al (eds.), Contemp. Math., **186** (1995), 173–200.

[IN97] Y. Ihara, H. Nakamura, On deformation of maximally degenerate stable marked curves and Oda's problem, J. Reine Angew. Math. **487** (1997), 125–151.

[Ih99-00] Y.Ihara, On beta and gamma functions associated with the Grothendieck-Teichmüller modular group *in Aspects of Galois Theory (H. Voelklein et.al (eds.))* London Math. Soc. Lect. Note Ser. **256** (1999) 144–179; Part II, J. reine angew. Math. **527** (2000) 1–11.

[Ih02] Y.Ihara, *Some arithmetic aspects of Galois actions in the pro-p fundamental group of* $\mathbb{P}^1 - \{0, 1, \infty\}$, Proc. Symp. Pure Math. (AMS) **70** (2002) 247–273.

[K76] N.Katz, p-adic interpolation of real analytic Eisenstein series, Ann. of Math., **104** (1976), 459–571.

[KM85] N.Katz, B.Mazur, Arithmetic Moduli of Elliptic Curves, Annals of Mathematics Studies **108**, Princeton 1985.

[Ki07] M.Kim, p-adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication, arXiv:math/0710.5290.

[KL81] D.Kubert, S.Lang, Modular Units, Springer 1981

[L87] S.Lang, Elliptic Functions, 2nd Edition, Graduate Texts in Mathematics **112**, Springer 1987.

[LS06] P.Lochak, L.Schneps, Open problems in Grothendieck-Teichmüller theory. in "Problems on mapping class groups and related topics", Proc. Sympos. Pure Math., **74** (2006), 165–186.

[Ma96] M. Matsumoto, Galois representations on profinite braid groups on curves, J. reine angew. Math. **474** (1996), 169–219.

[Ma97] M.Matsumoto, Galois group $G_{\mathbb{Q}}$, singularity E_7 and moduli M_3, in "Geometric Galois Actions, 2" (P.Lochak, L.Schneps eds.) London Math. Soc. Lect. Note Ser. **243** (1997) 179–218.

[Mum83] D.Mumford, Tata Lectures on Theta I, Birkhäuser 1983.

[Moc99] S.Mochizuki, Extending families of curves over log regular schemes, J. Reine. Angew. Math. **511** (1999), 43-71.

[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.

[Mor93] S.Morita, The extension of Johnson's homomorphism from the Torelli group to the mapping class group, Invent. Math. **111** (1993), 197–224.

[MS03] W.G.McCallum, R.Sharifi, A cup product in the Galois cohomology of number fields, Duke Math. J., **120** (2003), 269–310.

[N94] H.Nakamura, Galois rigidity of pure sphere braid groups and profinite calculus, J. Math. Sci. Univ. Tokyo **1** (1994), 71–136.

[N95] ———, On exterior Galois representations associated with open elliptic curves, J. Math. Sci., Univ. Tokyo **2** (1995), 197–231.

[N97] ———, Galois representations in the profinite Teichmüller modular groups, in 'Geometric Galois Actions I' (L.Schneps, P.Lochak eds.) London Math. Soc. Lect. Note Series 242 (1997), pp. 159–173.

[N99] ———, Tangential base points and Eisenstein power series, in "Aspects of Galois Theory" (H. Völkein, D.Harbater, P.Müller, J.G.Thompson, eds.) London Math. Soc. Lect. Note Ser. **256** (1999), 202–217.

[N99-02] ———, Limits of Galois representations in fundamental groups along maximal degeneration of marked curves, I , Amer. J. Math. **121** (1999) 315–358. ; Part II, Proc. Symp. Pure Math. **70** (2002) 43–78.

[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, (in Japanese), RIMS Kokyuroku **1281** (2002), 176–183.

[N03j] ———, On Magnus representation arising from elliptic curves and Eisenstein power series (in Japanese), in "Report Collection of 47th Algebra Symposium in 2002" (A.Tamagawa, S.Yoshihara eds.), 143-149.

[N03] ——— Generalized Rademacher functions and some congruence properties, in "Galois Theory and Modular Forms" (K.Hashimoto, K.Miyake, H.Nakamura eds.), Development of Math. **11** (2003), 375–394.

[NS00] H.Nakamura, 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.

[NT03-06] H.Nakamura, H.Tsunogai, Harmonic and equianharmonic equations in the Grothendieck-Teichmüller group, Forum Math. **15** (2003) 877–892; Part II, *in "Primes and Knots" (T.Kohno, M.Morishita eds.)* AMS Contemporary Mathematics **416** (2006), 197–211.

[NTY10] H.Nakamura, H.Tsunogai, S.Yasuda, Harmonic and equianharmonic equations in the Grothendieck-Teichmüller group, III, J. Inst. Math. Jussieu (in press).

[Od95] Takayuki Oda, A note on ramification of the Galois representation on the fundamental group of an algebraic curve, II, J. Number Theory, **53** (1995), 342-355.

[Rad73] H.Rademacher, Topics in Analytic Number Theory, Springer 1973.

[Sch74] B.Schoeneberg, Elliptic Modular Functions, An Introduction, Springer 1974.

[Sh71] G.Shimura, Introduction to Arithmetic Theory of Automorphic Functions, Iwanami Shoten and Princeton University Press, 1971.

[St82] G.Stevens, Arithmetic on modular curves, Progresses in Math. **20**, Birkhäuser 1982.

[St85] G.Stevens, The cuspidal group and special values of L-functions, Trans. AMS **291** (1985), 519–550.

[St87] G.Stevens, The Eisenstein measure and real quadratic fields, in "Proceedings of the International Conference on Number Theory (Quebec, PQ, 1987)", (1987) 887–927, de Gruyter, Berlin.

[Sti08] J.Stix, On cuspidal sections of algebraic fundamental groups, preprint, Philadelphia-Bonn, August 2008.

[Ta97] A.Tamagawa, The Grothendieck conjecture for affine curves, Compositio math., **109** (1997), 135–194.

[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.

[Tsu95b] H.Tsunogai, On some derivations of Lie algebras related to Galois representations, Publ. RIMS, Kyoto Univ. **31** (1995), 113–134.

[Tsu03] H.Tsunogai, The stable derivation algebras for higher genera, Israel J. Math. **136** (2003), 221–250.

[Woj04] Z.Wojtkowiak, On a torsor of paths of an elliptic curve minus a point, J. Math. Sci. Univ. Tokyo, **11** (2004), 353–399.

Hiroaki Nakamura: Department of Mathematics, Faculty of Science, Okayama University, Okayama 700-8530, Japan

E-mail address: `h-naka@math.okayama-u.ac.jp`