©2020 The Mathematical Society of Japan
J. Math. Soc. Japan
Vol. 72, No. 2 (2020) pp. 333–412
doi: 10.2969/jmsj/78327832

μ-type subgroups of $J_1(N)$ and application to cyclotomic fields

By Masami Ohta

(Received June 25, 2017)

Abstract. Let p be an odd prime number, and N a positive integer prime to p. We prove that μ-type subgroups of the modular Jacobian variety $J_1(N)$ or $J_1(Np)$ of order a power of p and defined over some abelian extensions of $\mathbb{Q}$ are trivial, under several hypotheses. For the proof, we use the method of Vatsal. As application, we show that a conjecture of Sharifi is valid in some cases.

Introduction.

Let $J_0(N)$ and $J_1(N)$ be the Jacobian varieties of the modular curves $X_0(N)$ and $X_1(N)$, all defined over $\mathbb{Q}$, attached to the congruence subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$ of $SL_2(\mathbb{Z})$, respectively. The purpose of this paper is to study the μ-type subgroups of $J_1(N)$. In general, we say that a commutative group scheme over some scheme is a *μ-type group* if it is finite, flat and Cartier dual to a constant group scheme, following Mazur [**Ma**].

As for $J_0(N)$, when $N \geq 5$ is a prime number, Mazur proved, among others, the following two results which had been conjectured by Ogg, in his celebrated paper [**Ma**, Chapter III, Section 1]:

- The rational torsion subgroup $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ is a cyclic group of order $n := (N-1)/(N-1, 12)$, which is generated by the class of the cuspidal divisor $(0) - (\infty)$.

- The maximal μ-type subgroup of $J_0(N)$ over $\mathbb{Q}$ is the Shimura subgroup $\mathrm{Ker}(J_0(N) \to J_1(N))$, which is again of order n.

These two results were proved via the detailed study of the Eisenstein ideal in the Hecke algebra acting on $J_0(N)$ or the space of cusp forms of weight two on $\Gamma_0(N)$. As remarked by Mazur [**Ma**, loc. cit.], if one disregards the two-torsion part, the study of $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ is much easier than that of the μ-type subgroups. Indeed, the latter required a deep result on the Hecke algebra, the Gorenstein property.

It is possible to extend this method of the Eisenstein ideal to study the rational torsion subgroups of other modular Jacobian varieties, in the "easier" case, i.e. disregarding the two-torsion part (and sometimes the three-torsion part also), cf. [**O6**], [**O7**]. However, it seems rather difficult to extend it to study the μ-type subgroups of, for example, $J_1(N)$. In addition, in view of the application we expect, we wish to obtain the result not only over $\mathbb{Q}$, but also over some (abelian) extensions of $\mathbb{Q}$.

2010 *Mathematics Subject Classification.* Primary 11G18; Secondary 14G05, 11R23.
Key Words and Phrases. modular Jacobian variety $J_1(N)$, μ-type subgroup, cyclotomic field.

On the other hand, in [**V**] (in which the terminology "multiplicative" is used instead of "μ-type"), Vatsal has found a completely different approach to the study of the μ-type subgroups of modular Jacobians. He proved the following result which considerably generalizes Mazur's result for non-two-torsion μ-type subgroups of $J_0(N)$ with N not necessarily prime, cf. [**V**, Theorem 1.1]:

- Let p be an odd prime number, and W a μ-type subgroup of $J_0(N)$ over $\mathbb{Q}$ of order a power of p. If $J_0(N)$ has semi-stable reduction at p (which is the case if p^2 does not divide N), then W is contained in the Shimura subgroup.

It is the method of Vatsal we are going to follow. To state the main result of this paper, we use the following notation: We let $\mathbb{Q}(\zeta_p)$ be the cyclotomic field of p-th roots of unity, and identify the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ with $(\mathbb{Z}/p\mathbb{Z})^\times$ in the usual manner. Thus for a subgroup A of $(\mathbb{Z}/p\mathbb{Z})^\times$, we can consider the fixed field $\mathbb{Q}(\zeta_p)^A$. We will prove the following theorem (Part II, Theorem (5.1.4) in the text):

Theorem. *Let p be an odd prime number, and assume that $N\varphi(N)$ is not divisible by p, where φ denotes the Euler function. Let k_0 be a fixed finite abelian extension of $\mathbb{Q}$ such that $[k_0 : \mathbb{Q}]$ is prime to p, and p is unramified in k_0. For a subgroup A of $(\mathbb{Z}/p\mathbb{Z})^\times$, we set*

$$k_A := k_0\mathbb{Q}(\zeta_p)^A.$$

Assume that $A \neq \{1\}$. If G is a μ-type subgroup of $J_1(Np)$ over k_A of order a power of p on which the diamond action $\langle a\rangle_p$ of each $a \in A \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$ is the identity, then G is necessarily trivial.

Although this formulation of our main theorem is also convenient for our application to cyclotomic fields, we actually prove it in a slightly different form. We consider the quotient curve $X_1(Np; A)$ of $X_1(Np)$ by the action of A through $\langle\ \rangle_p$, and its Jacobian variety $J_1(Np; A)$ over $\mathbb{Q}$. Then, under the same assumptions as above, our theorem can be restated as follows: $J_1(Np; A)$ has no non-trivial μ-type subgroup of order a power of p over k_A (Part II, Theorem (5.1.7) in the text). An advantage of considering $X_1(Np; A)$ is that it has semi-stable reduction over $\mathbb{Q}(\zeta_p)^A$ at the prime above p, whose ramification index is strictly smaller than $p-1$ when $A \neq \{1\}$; while this method in turn necessitates our assumption on the A-invariance of G in the above theorem. On the other hand, one easily obtains from this a result in the prime-to-p level case; i.e. for N, p and A as above, $J_1(N)$ has no non-trivial μ-type subgroup of order a power of p over k_A (Part II, Corollary (5.1.5) in the text). We also remark that the same results as above obviously hold for μ-type subgroups over any subfield of k_A, notably over $\mathbb{Q}$.

We next describe an application of our theorem to the theory of cyclotomic fields, which in fact motivated our study of the μ-type subgroups. We let N and p be as in the theorem above, and assume moreover that $p \geq 5$ in the following application. Fix an even Dirichlet character θ of conductor N or Np, for which we assume that $\theta\omega(p) \neq 1$ when $\theta\mid_{(\mathbb{Z}/p\mathbb{Z})^\times} = \omega^{-1}$, ω being the Teichmüller character modulo p. Let $\mathfrak{r}$ be the ring generated by the values of θ over $\mathbb{Z}_p$. To state our result, we need a rather lengthy list of terminologies. We refer the reader to Part II, 6.1 in the text for more details, and mention here only the following:

- $\Lambda_{\mathfrak{r}} := \mathfrak{r}[[1+p\mathbb{Z}_p]]$ is the completed group algebra of the multiplicative group $1+p\mathbb{Z}_p$, the Iwasawa algebra.
- X is the ordinary part of the projective limit of the étale cohomology groups $H^1(X_1(Np^r)\otimes_{\mathbb{Q}}\overline{\mathbb{Q}}, \mathbb{Z}_p)\otimes_{\mathbb{Z}_p}\mathfrak{r}$ for $r \geq 1$, localized at an appropriate Eisenstein maximal ideal attached to θ.
- $\mathfrak{h}^*$ is Hida's Hecke algebra acting on X, which is a finite and flat $\Lambda_{\mathfrak{r}}$-algebra.
- $\mathfrak{I}^*$ is the Eisenstein ideal of $\mathfrak{h}^*$.
- A decomposition $X = X_- \oplus X_+$ as an $\mathfrak{h}^*$-module, where X_+ is the fixed subspace under the action of the inertia group at p (with respect to a fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$). Here, X_+ is known to be a free $\mathfrak{h}^*$-module of rank one, whereas X_- is isomorphic to $\mathrm{Hom}_{\Lambda_{\mathfrak{r}}}(\mathfrak{h}^*, \Lambda_{\mathfrak{r}})$ as an $\mathfrak{h}^*$-module.
- F is the imaginary abelian extension of $\mathbb{Q}$ corresponding to $\theta\omega$.
- F_∞ is the cyclotomic $\mathbb{Z}_p$-extension of F.
- L_∞ is the maximal abelian unramified pro-p-extension of F_∞.
- $\mathrm{Gal}(L_\infty/F_\infty)_{(\theta\omega)^{-1}}$ is the $(\theta\omega)^{-1}$-part of the Galois group.

We obtain from the natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on X the map

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Hom}_{\mathfrak{h}^*}(X_+, X_-) \cong X_-$$

where we have fixed an $\mathfrak{h}^*$-basis of X_+ to obtain the isomorphism in the right hand side. It is known that, when reduced modulo $\mathfrak{I}^*$, this gives rise to a *representation*:

$$\mathrm{Gal}(L_\infty/F_\infty)_{(\theta\omega)^{-1}} \to X_-/\mathfrak{I}^* X_-. \tag{$*$}$$

In [**Sha**], Sharifi conjectured that this is in fact an isomorphism, as a part of more precise conjectures. We will prove (Part II, Theorem (6.2.2) in the text):

THEOREM. *Assume that the kernel of the restriction of θ to $(\mathbb{Z}/p\mathbb{Z})^\times$ is non-trivial. Then the homomorphism $(*)$ is an isomorphism.*

(One has to modify the $\Lambda_{\mathfrak{r}}$-module structure of X_- (arising from the $\Lambda_{\mathfrak{r}}$-algebra structure of $\mathfrak{h}^*$) by an involutive automorphism of $\Lambda_{\mathfrak{r}}$ to make $(*)$ as an isomorphism of $\Lambda_{\mathfrak{r}}$-modules; cf. Part II, 6.1 in the text.)

As we already said, we will prove our main theorem by following Vatsal's article [**V**], in which he used the following results:

(I) Hida's non-vanishing modulo p result for the values of Hecke L-functions attached to Hecke characters of imaginary quadratic fields; cf. [**H1**], [**H2**], [**H3**].

(II) Rubin's proof of the Iwasawa main conjecture for imaginary quadratic fields; cf. [**Ru1**], [**Ru2**].

(III) Surjectivity of the supersingular reduction of CM points on $X_0(M)$, due to Vatsal and Cornut; cf. [**C**].

(IV) Ihara's theorem on modular curves over finite fields; cf. [**I**].

An important feature of the modular curves $X_0(M)$, $X_1(M)$ etc. is that they contain many CM points, corresponding to elliptic curves with complex multiplication. The method of Vatsal makes essential use of arithmetic properties of such points, as we will see below.

We now explain how the proof of our main theorem proceeds: Let $X_1(Np;A)$ be, as above, the quotient of the curve $X_1(Np)$ by the action via $\langle\ \rangle_p$ of A. Assume that there is a non-trivial G as in our main theorem, equivalently a non-trivial μ-type subgroup of $J_1(Np;A)$ of order a power of p over k_A. Then there is a $\mathbb{Z}/p\mathbb{Z}$-torsor (= an étale Galois covering with Galois group $\mathbb{Z}/p\mathbb{Z}$) Z over $X_1(Np;A) \otimes_{\mathbb{Q}} k_A =: X_1(Np;A)_{/k_A}$ with Z geometrically irreducible over k_A. To rule out such possibility, we want to choose a good prime number q, such that the primes of k_A above q are of degree at most two, to obtain a $\mathbb{Z}/p\mathbb{Z}$-torsor

$$Z_{/\mathbb{F}_{q^2}} \to X_1(Np;A)_{/\mathbb{F}_{q^2}}$$

over $\mathbb{F}_{q^2}$ by reduction. We assume that $q \equiv \pm 1 \bmod Np$ in which case supersingular points of $X_1(Np;A)_{/\mathbb{F}_{q^2}}$ are rational over $\mathbb{F}_{q^2}$. In choosing q, we further require that all points of $Z_{/\mathbb{F}_{q^2}}$ above these points are rational over $\mathbb{F}_{q^2}$. However, Ihara's theorem (IV) asserts that such an étale covering cannot exist. Our aim is thus to show that a prime q having the above properties really exists (when non-trivial G exists).

It is therefore important to know what points of $X_1(Np;A)$ (or $X_1(Np)$) are mapped by reduction to supersingular points in positive characteristic fibres, and how the fibres of such points via $Z \to X_1(Np;A)_{/k_A}$ behave. As in [**V**], we take an imaginary quadratic field K (in which prime factors of Np all split) and a prime number l not dividing Np, and consider points (corresponding to elliptic curves) having complex multiplication by orders of l-power conductor of K. For $X_0(Np)$, these are the points called Heegner points and rational over the ring class fields of l-power conductor of K. We will consider the points of $X_1(Np;A)$ (or $X_1(Np)$) lying above such points, which are rational over the anticyclotomic $\mathbb{Z}_l$-extension of some abelian extension of K. If q is a prime number ($q \nmid Npl$) which is inert in K, the result (III) of Vatsal and Cornut asserts that Heegner points reduce surjectively onto the supersingular points of $X_0(Np)_{/\mathbb{F}_{q^2}}$. It follows from this that a similar result holds for $X_1(Np;A)$ (or $X_1(Np)$) and the above mentioned CM points on it by reduction to characteristic q for certain $q(\equiv \pm 1 \bmod Np)$; cf. Part II, 3.2.

The most important step for the proof of our main theorem is to show that the "growth" of the inverse images of the CM points of $X_1(Np;A)_{/k_A}$ in Z is moderate. Precisely, we show that there is a finite extension of K such that all points of Z above such CM points are rational over the composite of this field and the anticyclotomic $\mathbb{Z}_l$-extension of K, which will enable us to choose "good" primes q. After the study of ramifications in the fibres of $Z \to X_1(Np;A)_{/k_A}$ in Part II, Section 4, this reduces to an analogue of Washington's theorem [**W**] for anticyclotomic $\mathbb{Z}_l$-extensions of abelian extensions of K. We will prove such a result under rather restrictive assumptions on the abelian extensions of K (cf. Part II, 2.1), but it is sufficient for our purpose. (It has been done by Vatsal for the tower of ring class fields of l-power conductor using (I) and (II).)

To do this, aside from (II), we need an improvement of (I) for Hecke characters of K *whose conductor is divisible by primes above p.* This occupies Part I of this paper (and also a part of Part II, Section 1). The proof depends heavily on Hida's ideas, especially on his Zariski density result of CM points, but we first followed Katz's article [**Ka2**] to study the Hecke L-values of K, and tried to be as self-contained as possible. See the Introduction to Part I for our result in this direction.

Part I. A result on the non-vanishing of Hecke L-values modulo p.

0. Introduction to Part I.

Let K be an imaginary quadratic field with its ring of integers $\mathfrak{o}$. Let

$$\lambda : K_{\mathbb{A}}^{\times}/K^{\times} \to \mathbb{C}^{\times}$$

be a Hecke character of K, $K_{\mathbb{A}}^{\times}$ being the idele group of K. We assume that its infinity component λ_∞ satisfies

$$\lambda_\infty(x) = x^k \text{ for } x \in (K \otimes_{\mathbb{Q}} \mathbb{R})^{\times} = \mathbb{C}^{\times}$$

with an integer k.

Let l be a prime number, and $\mathfrak{o}_n := \mathbb{Z} + l^n\mathfrak{o}$ the order of conductor l^n of K for $n \geq 0$. Let Cl_n be the group of proper $\mathfrak{o}_n$-ideal classes, and set $\mathrm{Cl}_\infty := \varprojlim_{n\geq 0} \mathrm{Cl}_n$. Let $\widehat{\mathrm{Cl}}_\infty^{\mathrm{lc}} = \varinjlim_{n\geq 0} \mathrm{Hom}(\mathrm{Cl}_n, \overline{\mathbb{Q}}^{\times})$ be the set of $\overline{\mathbb{Q}}^{\times}$-valued characters of Cl_∞ that factor through some Cl_n ($n < \infty$). We may consider each $\varepsilon \in \widehat{\mathrm{Cl}}_\infty^{\mathrm{lc}}$ as a Hecke character of K of finite order. Here and below, $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$.

Let p be an odd prime number different from l. We fix an embedding of $\overline{\mathbb{Q}}$ into an algebraic closure of $\mathbb{Q}_p$, and let $\mathfrak{P}$ be the prime of $\overline{\mathbb{Q}}$ corresponding to this embedding. We assume that p splits as $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in K and assume that $\mathfrak{p}$ is the prime lying below $\mathfrak{P}$.

Let $\mathfrak{c}$ be the conductor of λ. We will assume the following conditions:

$$\begin{cases} k \geq 2, \\ \mathfrak{c} \text{ is prime to } l, \\ \mathfrak{c} \text{ is a product of primes that split in } K/\mathbb{Q}. \end{cases}$$

Note that we do not assume that $\mathfrak{c}$ is prime to p. Let e (resp. $\overline{e}$) be the exponent of $\mathfrak{p}$ (resp. $\overline{\mathfrak{p}}$) dividing $\mathfrak{c}$. Let $\chi_{\mathfrak{p}} : (\mathfrak{o}/\mathfrak{p}^e)^{\times} = (\mathbb{Z}/p^e\mathbb{Z})^{\times} \to \overline{\mathbb{Q}}^{\times}$ be the character induced from λ.

With these notation and assumptions, we will prove:

Theorem I. *There is a non-zero complex number Ω_∞ with which the following assertion holds*:

$$p^{e(k-1)}(k-1)!g(e^{2\pi i/p^e}, \chi_{\mathfrak{p}})L^{(l)}(0, \lambda\varepsilon)/\Omega_\infty^k \in \overline{\mathbb{Q}}$$

and moreover these values are $\mathfrak{P}$-integral for all $\varepsilon \in \widehat{\mathrm{Cl}}_\infty^{\mathrm{lc}}$. Further, except for a finite number of ε, these values are $\mathfrak{P}$-adic units.

Here, $g(e^{2\pi i/p^e}, \chi_{\mathfrak{p}})$ is the Gauss sum, $L(s, \lambda\varepsilon)$ is the Hecke L-function, and the superscript "$^{(l)}$" indicates the exclusion of the Euler factors at primes dividing l.

When $\mathfrak{c}$ is prime to p, this is a special case of Hida's much more general result; cf. [**H1**, Theorem 1.1], [**H2**, Theorem 4.3] and [**H3**, Theorems 8.17 and 8.31]. Actually, we will prove this theorem under additional assumptions:

$$\begin{cases} e \geq \overline{e}, \\ \mathfrak{c} \neq (1) \text{ when } k = 2, \end{cases}$$

in this Part I. In the first section of Part II, we will remove these assumptions after recalling p-adic properties of Hecke L-values. (The case where $k = 2$ and $\mathfrak{c} = (1)$ is already covered in Hida's theorem; but we avoided the use of non-holomorphic Eisenstein series in Part I for simplicity.)

The algebraicity of the special values of Hecke L-functions was first established by Shimura [**Shi2**]. Katz [**Ka2**], [**Ka3**] then studied further the integrality and p-adic properties of such L-values. As cited above, Hida obtained the non-vanishing modulo p result for the L-values in [**H1**]–[**H3**]. All these results are proved for general CM fields using Hilbert modular forms.

As noted in the introduction, we need the non-vanishing modulo p result for Hecke L-values of imaginary quadratic fields when the conductor of the Hecke character is divisible by primes above p, to prove our main result. The purpose of this Part I is thus to supply such a result, and we will neither touch the general CM fields nor the differential operators of Maass, Shimura and Katz. We basically follow the method of Katz and Hida. The method of the proof of the above non-vanishing result is entirely due to Hida [**H1**]–[**H3**].

1. Level structures on elliptic curves and test objects.

1.1. Basic level structures.

We first recall terminologies from Katz [**Ka2**, Chapter II]. Let M and T be positive integers.

Definition (1.1.1). Let E be an elliptic curve over a base scheme S.

(i) A $\Gamma(M)^{\text{naive}}$-*structure* on E/S is an isomorphism

$$\alpha_M : \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z} \xrightarrow{\sim} E[M]$$

of group schemes over S, where $E[M]$ denotes the kernel of multiplication by M on E.

(ii) A $\Gamma(M)^{\text{arith}}$-*structure* on E/S is an isomorphism

$$\beta_M : \boldsymbol{\mu}_M \times \mathbb{Z}/M\mathbb{Z} \xrightarrow{\sim} E[M]$$

of group schemes over S which satisfies

$$e_{M,E}(\beta_M(\zeta_1, m), \beta_M(\zeta_2, n)) = \zeta_1^n/\zeta_2^m.$$

Here, $e_{M,E}(\ ,\ )$ is the e_M-pairing on E, and ζ_1 and ζ_2 (resp. m and n) are sections of $\boldsymbol{\mu}_M$ (resp. $\mathbb{Z}/M\mathbb{Z}$) over an S-scheme.

(iii) A $\Gamma_0(T)$-*structure* C_T on E/S is a finite flat S-subgroup scheme of order T of E which is cyclic.

(iv) When T is prime to M, a $\Gamma(M)^{\text{naive}} \cap \Gamma_0(T)$-*structure* on E/S is a pair (α_M, C_T) of $\Gamma(M)^{\text{naive}}$- and $\Gamma_0(T)$-structures. Similarly for a $\Gamma(M)^{\text{arith}} \cap \Gamma_0(T)$-*structure.*

(v) A pair (E, α_M) as in (i) is called a $\Gamma(M)^{\text{naive}}$-*curve* over S. Similarly for a $\Gamma(M)^{\text{arith}}$-*curve*, a $\Gamma(M)^{\text{naive}} \cap \Gamma_0(T)$-*curve* and so on.

We remark that a $\Gamma(M)^{\text{naive}}$-structure on E/S exists only when M is invertible in S. As for a $\Gamma_0(T)$-structure, we will consider it only when T is invertible in S, in which case C_T is étale over S and the meaning of cyclicity is the obvious one.

Let E be an elliptic curve over a $\mathbb{Z}[1/M]$-scheme S. If α_M is a $\Gamma(M)^{\text{naive}}$-structure on E/S, we define its determinant by

$$\det(\alpha_M) := e_{M,E}\left(\alpha_M\begin{pmatrix}1\\0\end{pmatrix}, \alpha_M\begin{pmatrix}0\\1\end{pmatrix}\right) \in \boldsymbol{\mu}_M^{\text{prim}}(S) \tag{1.1.2}$$

where $\boldsymbol{\mu}_M^{\text{prim}}$ is the scheme of primitive M-th roots of unity. There is a bijection [**Ka2**, 2.0.8]:

$$\begin{gathered}\{\Gamma(M)^{\text{naive}}\text{-structures on } E/S\} \xrightarrow{\sim} \boldsymbol{\mu}_M^{\text{prim}}(S) \times \{\Gamma(M)^{\text{arith}}\text{-structures on } E/S\} \qquad (1.1.3)\\ \alpha_M \mapsto (\det(\alpha_M), \beta_{\alpha_M})\end{gathered}$$

where we define β_{α_M} by:

$$\beta_{\alpha_M}(\det(\alpha_M)^m, n) := \alpha_M(m, n). \tag{1.1.4}$$

There is a natural right action of $GL_2(\mathbb{Z}/M\mathbb{Z})$ on the set of $\Gamma(M)^{\text{naive}}$-structures on E/S:

$$\alpha_M \mapsto \alpha_M \circ \gamma \ \text{ for } \gamma \in GL_2(\mathbb{Z}/M\mathbb{Z}). \tag{1.1.5}$$

It is easy to see that

$$\det(\alpha_M \circ \gamma) = \det(\alpha_M)^{\det(\gamma)}; \text{ and} \tag{1.1.6}$$

$$\beta_{\alpha_M \circ \gamma}(\zeta^m, n) = \beta_{\alpha_M}(\zeta^{\det(\gamma)^{-1}(am+bn)}, cm + dn) \tag{1.1.7}$$

if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Especially, $\beta_{\alpha_M \circ \gamma} = \beta_{\alpha_M}$ if and only if γ is of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$.

We can consider the relatively representable moduli problems $[\Gamma(M)^{\text{naive}}]$ and $[\Gamma(M)^{\text{arith}}]$ in the sense of Katz and Mazur [**KM**, (4.2), (4.13)]. $[\Gamma(M)^{\text{naive}}]$ is finite and étale over $(\text{Ell}/\mathbb{Z}[1/M])$, and $[\Gamma(M)^{\text{arith}}]$ is affine and étale over (Ell) in the sense of [**KM**, (4.5)]. When $M \geq 3$, they are rigid [**KM**, (4.4)], and these moduli problems are represented by an affine and smooth curve $\mathfrak{M}(\Gamma(M)^{\text{naive}})$ over $\mathbb{Z}[1/M]$ and an affine and smooth curve $\mathfrak{M}(\Gamma(M)^{\text{arith}})$ over $\mathbb{Z}$, respectively [**KM**, Corollary 4.7.1]. (1.1.3) shows that $\mathfrak{M}(\Gamma(M)^{\text{naive}}) = \mathfrak{M}(\Gamma(M)^{\text{arith}}) \otimes_{\mathbb{Z}} \mathbb{Z}[1/M, \zeta_M]$, where $\zeta_M \in \overline{\mathbb{Q}}$ is a primitive M-th root of unity. Also, it follows from (1.1.7) and the subsequent remark that $\mathfrak{M}(\Gamma(M)^{\text{arith}}) \otimes_{\mathbb{Z}} \mathbb{Z}[1/M]$ is the quotient of $\mathfrak{M}(\Gamma(M)^{\text{naive}})$ by the subgroup of $GL_2(\mathbb{Z}/M\mathbb{Z})$

consisting of matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}$. Similarly for the "simultaneous moduli problems" (1.1.1), (iv). Especially, for $M \geq 3$, $\mathfrak{M}(\Gamma(M)^{\mathrm{arith}} \cap \Gamma_0(T))$ is an affine and smooth curve over $\mathbb{Z}[1/T]$, and another important property is that it is geometrically irreducible over $\mathbb{Z}[1/T]$.

Definition (1.1.8). A triple (E, ω, β_M) consisting of a $\Gamma(M)^{\mathrm{arith}}$-curve (E, β_M) over S and a nowhere-vanishing invariant differential ω on E/S is called a $\Gamma(M)^{\mathrm{arith}}$-*test object* over S. Similarly for other moduli problems.

1.2. Relation with isogenies.

Let M be, as in 1.1, a positive integer. In this subsection, we assume that we are given elliptic curves E and F over S, and an isogeny over S

$$\pi : E \to F \text{ with its degree } \deg(\pi) \text{ prime to } M. \tag{1.2.1}$$

If α_M is a $\Gamma(M)^{\mathrm{naive}}$-structure on E, then $\pi \circ \alpha_M : \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z} \overset{\sim}{\to} F[M]$ is obviously a $\Gamma(M)^{\mathrm{naive}}$-structure on F. We have $e_{M,F}\left(\pi \circ \alpha_M\begin{pmatrix}1\\0\end{pmatrix}, \pi \circ \alpha_M\begin{pmatrix}0\\1\end{pmatrix}\right) = e_{M,E}\left(\alpha_M\begin{pmatrix}1\\0\end{pmatrix}, \alpha_M\begin{pmatrix}0\\1\end{pmatrix}\right)^{\deg(\pi)}$, i.e.

$$\det(\pi \circ \alpha_M) = \det(\alpha_M)^{\deg(\pi)}. \tag{1.2.2}$$

On the other hand, when β_M is a $\Gamma(M)^{\mathrm{arith}}$-structure on E, $\pi \circ \beta_M$ may not be a $\Gamma(M)^{\mathrm{arith}}$-structure on F, since the second condition in (1.1.1), (ii) does not hold in general.

Definition (1.2.3). With the notation as above, we define

$$(\pi \circ \beta_M)^{\sim} : \boldsymbol{\mu}_M \times \mathbb{Z}/M\mathbb{Z} \overset{\sim}{\to} F[M] \text{ by :}$$
$$(\pi \circ \beta_M)^{\sim}(\zeta, n) := \pi \circ \beta_M(\zeta^{\deg(\pi)^{-1}}, n).$$

(Here, of course, $\deg(\pi)^{-1}$ is the inverse of $\deg(\pi) \in (\mathbb{Z}/M\mathbb{Z})^{\times}$.)

It is easy to check that $(\pi \circ \beta_M)^{\sim}$ is in fact a $\Gamma(M)^{\mathrm{arith}}$-structure.

Lemma (1.2.4). *Assume that S is a $\mathbb{Z}[1/M]$-scheme, and we are given a $\Gamma(M)^{\mathrm{naive}}$-structure α_M on E/S. Then, using the notation* (1.1.4), *we have*

$$(\pi \circ \beta_{\alpha_M})^{\sim} = \beta_{\pi \circ \alpha_M}.$$

Proof. We have $\pi \circ \alpha_M(m, n) = \beta_{\pi\circ\alpha_M}(\det(\pi \circ \alpha_M)^m, n)$ by (1.1.4), and this is equal to $\beta_{\pi\circ\alpha_M}(\det(\alpha_M)^{m\deg(\pi)}, n)$ by (1.2.2). On the other hand the left hand side is also equal to $\pi \circ \beta_{\alpha_M}(\det(\alpha_M)^m, n)$ by (1.1.4) again, and this is equal to $(\pi \circ \beta_{\alpha_M})^{\sim}(\det(\alpha_M)^{m\deg(\pi)}, n)$ by the above definition. □

Corollary (1.2.5). *Under the same situation, the following diagram commutes*:

$$\begin{tikzcd}
E \arrow[r, "\pi"] & F \\
\boldsymbol{\mu}_M \times \mathbb{Z}/M\mathbb{Z} \arrow[u, "\beta_{\alpha_M}"] \arrow[r, "\deg(\pi)\times\mathrm{id}"'] & \boldsymbol{\mu}_M \times \mathbb{Z}/M\mathbb{Z}. \arrow[u, "\beta_{\pi\circ\alpha_M}"']
\end{tikzcd}$$
□

Next suppose that the degree of the isogeny $\pi : E \to F$ is prime to T. Then π induces an isomorphism $E[T] \overset{\sim}{\to} F[T]$ of group schemes over S. Thus if C_T is a $\Gamma_0(T)$-structure on E, we can consider its image $\pi(C_T)$ by this isomorphism, which defines a $\Gamma_0(T)$-structure on F.

1.3. $\boldsymbol{\Gamma(l^\infty)^{\mathrm{naive}}}$-structures and $\boldsymbol{\Gamma(l^\infty)^{\mathrm{arith}}}$-structures.

For our purpose, it is convenient to consider also the following variants of $\Gamma(M)^{\mathrm{naive}}$- and $\Gamma(M)^{\mathrm{arith}}$-structures. We fix a prime number l.

Definition (1.3.1). Let E be an elliptic curve over S. By definition, a $\Gamma(l^\infty)^{\mathrm{naive}}$-structure $\alpha_{l^\infty} = (\alpha_{l^n})_{n\geq 1}$ on E/S is a system of $\Gamma(l^n)^{\mathrm{naive}}$-structures α_{l^n} on E/S for which the following diagram commutes for all $m \geq n$:

$$\begin{tikzcd}
\mathbb{Z}/l^m\mathbb{Z} \times \mathbb{Z}/l^m\mathbb{Z} \arrow[r, "\alpha_{l^m}", "\sim"'] \arrow[d, "\mathrm{canon.}"'] & E[l^m] \arrow[d, "l^{m-n}"] \\
\mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z} \arrow[r, "\sim", "\alpha_{l^n}"'] & E[l^n].
\end{tikzcd}$$

We define a $\Gamma(l^\infty)^{\mathrm{arith}}$-structure $\beta_{l^\infty} = (\beta_{l^n})_{n\geq 1}$ similarly as a compatible system of $\Gamma(l^n)^{\mathrm{arith}}$-structures.

Thus if we define the projective systems of finite flat group schemes by

$$\begin{cases} \underline{\mathbb{Z}}_l := (\mathbb{Z}/l^n\mathbb{Z})_{n\geq 1}, \\ \underline{\mathbb{Z}}_l(1) := (\boldsymbol{\mu}_{l^n})_{n\geq 1}, \\ \underline{T}_l(E) := (E[l^n])_{n\geq 1} \end{cases} \tag{1.3.2}$$

(with obvious transition morphisms), a $\Gamma(l^\infty)^{\mathrm{naive}}$-structure (resp. a $\Gamma(l^\infty)^{\mathrm{arith}}$-structure) on E/S is an isomorphism $\alpha_{l^\infty} : \underline{\mathbb{Z}}_l \times \underline{\mathbb{Z}}_l \overset{\sim}{\to} \underline{T}_l(E)$ (resp. $\beta_{l^\infty} : \underline{\mathbb{Z}}_l(1) \times \underline{\mathbb{Z}}_l \overset{\sim}{\to} \underline{T}_l(E)$) of projective systems over S. (When l is invertible in S, it may be also considered as an isomorphism of smooth $\mathbb{Z}_l$-sheaves on the étale site of S.)

From now on, we assume that l is invertible in S. The pairings $e_{l^n,E}$ on $E[l^n]$ induce a pairing

$$e_{l^\infty,E} : \underline{T}_l(E) \times \underline{T}_l(E) \to \underline{\mathbb{Z}}_l(1). \tag{1.3.3}$$

If α_{l^∞} is a $\Gamma(l^\infty)^{\mathrm{naive}}$-structure on E/S, its determinant is defined by

$$\det(\alpha_{l^\infty}) := (\det(\alpha_{l^n}))_{n\geq 1}. \tag{1.3.4}$$

Also, if $\alpha_{l^\infty} = (\alpha_{l^n})_{n\geq 1}$ is a $\Gamma(l^\infty)^{\mathrm{naive}}$-structure on E/S, we can define a $\Gamma(l^\infty)^{\mathrm{arith}}$-

structure $\beta_{\alpha_{l^\infty}}$ by

$$\beta_{\alpha_{l^\infty}} := (\beta_{\alpha_{l^n}})_{n \geq 1} \tag{1.3.5}$$

cf. (1.1.4). It is obtained from α_{l^∞} and the isomorphism $\underline{\mathbb{Z}}_l \overset{\sim}{\to} \underline{\mathbb{Z}}_l(1)$ determined by the projective system $\det(\alpha_{l^\infty})$ of primitive l^n-th roots of unity.

Lemma (1.3.6). *Let $\pi : E \to E'$ be an isogeny of elliptic curves* (*whose degree need not be prime to l*) *over a $\mathbb{Z}[1/l]$-scheme S. Suppose that we are given $\Gamma(l^\infty)^{\mathrm{naive}}$-structures α_{l^∞} and α'_{l^∞} on E and E', respectively, and a matrix $g \in GL_2(\mathbb{Q}_l) \cap M_2(\mathbb{Z}_l)$ for which the following diagram commutes*:

$$\begin{tikzcd}
\underline{\mathbb{Z}}_l \times \underline{\mathbb{Z}}_l \arrow[r, "\alpha_{l^\infty}", "\sim"'] \arrow[d, "g"'] & \underline{T}_l(E) \arrow[d, "\underline{T}_l(\pi)"] \\
\underline{\mathbb{Z}}_l \times \underline{\mathbb{Z}}_l \arrow[r, "\sim", "\alpha'_{l^\infty}"'] & \underline{T}_l(E').
\end{tikzcd}$$

Then we have

$$\det(\alpha_{l^\infty})^{\deg(\pi)} = \det(\alpha'_{l^\infty})^{\det(g)}.$$

(Here we have used the multiplicative notation for $\underline{\mathbb{Z}}_l(1)$.)

Proof. The values $\det(\alpha_{l^\infty})$ and $\det(\alpha'_{l^\infty})$ are constant on each connected component of S. We are thus reduced to the case where S is the spectrum of an algebraically closed field of characteristic different from l, and may replace $\underline{\mathbb{Z}}_l$ (resp. $\underline{T}_l(E)$) in the above diagram by the "genuine" $\mathbb{Z}_l$ (resp. the usual Tate module $T_l(E)$).

Write α and e (resp. α' and e') for α_{l^∞} and $e_{l^\infty,E}$ (resp. α'_{l^∞} and $e_{l^\infty,E'}$) for simplicity. Then since $e'(\pi(x), \pi(y)) = e(x,y)^{\deg(\pi)}$, we have

$$\det(\alpha)^{\deg(\pi)} = e'\left(\pi \circ \alpha \begin{pmatrix}1\\0\end{pmatrix}, \pi \circ \alpha \begin{pmatrix}0\\1\end{pmatrix}\right) = e'\left(\alpha' \circ g \begin{pmatrix}1\\0\end{pmatrix}, \alpha' \circ g \begin{pmatrix}0\\1\end{pmatrix}\right) = \det(\alpha')^{\det(g)}.$$

□

Corollary (1.3.7). *Let the notation be as in* (1.3.6). *If* $\deg(\pi) = \det(g)$, *we have* $\det(\alpha_{l^\infty}) = \det(\alpha'_{l^\infty})$. □

Definition (1.3.8). Let M and T be relatively prime positive integers, and l a prime number not dividing MT. A $\Gamma(l^\infty M)^{\mathrm{arith}} \cap \Gamma_0(T)$-*curve* (resp. a $\Gamma(l^\infty M)^{\mathrm{arith}} \cap \Gamma_0(T)$-*test object*) is a triple $(E, \beta_{l^\infty M}, C_T)$ (resp. a quadruple $(E, \omega, \beta_{l^\infty M}, C_T)$). Here, $\beta_{l^\infty M} = (\beta_{l^\infty}, \beta_M)$ is a pair of $\Gamma(l^\infty)^{\mathrm{arith}}$- and $\Gamma(M)^{\mathrm{arith}}$-structures on E, and other symbols have the same meaning as in (1.1.8). Similarly for the $\Gamma(l^\infty)^{\mathrm{naive}}$-structure.

2. Modular forms.

2.1. Algebraic theory.

We recall basic terminologies on the algebraic theory of modular forms from Katz [**Ka2**, Chapter II]. As in Section 1, we fix positive integers M and T such that $(M,T)=1$, and set

$$\Gamma_{M,T} := \Gamma(M)^{\mathrm{arith}} \cap \Gamma_0(T) \tag{2.1.1}$$

for the simplicity of notation. Recall (1.1.8) that a $\Gamma_{M,T}$-test object (E,ω,β_M,C_T) over a scheme S consists of an elliptic curve E over S, a nowhere-vanishing invariant differential ω on E/S, and a $\Gamma(M)^{\mathrm{arith}}$-structure (resp. a $\Gamma_0(T)$-structure) β_M (resp. C_T) on E/S.

Definition (2.1.2). Let B be a $\mathbb{Z}[1/T]$-algebra, and k an integer. A *$\Gamma_{M,T}$-modular form F* of weight k over B is a rule which assigns an element $F(E,\omega,\beta_M,C_T)\in B'$ to every $\Gamma_{M,T}$-test object (E,ω,β_M,C_T) over a B-algebra B', which satisfies the following two conditions:

(i) Let (E,ω,β_M,C_T) over B' be as above. If $\varphi; B'\to B''$ is a homomorphism of B-algebras, and $(E,\omega,\beta_M,C_T)\otimes_{B'} B'' \cong (E',\omega',\beta'_M,C'_T)$ over B'', then

$$F(E',\omega',\beta'_M,C'_T) = \varphi(F(E,\omega,\beta_M,C_T)).$$

(ii) For any $\lambda \in B'^{\times}$,

$$F(E,\lambda^{-1}\omega,\beta_M,C_T) = \lambda^k F(E,\omega,\beta_M,C_T).$$

The B-module consisting of all such forms is denoted by $R^k(B,\Gamma_{M,T})$.

When B is also a $\mathbb{Z}[1/M]$-algebra, one can define the notion of $\Gamma(M)^{\mathrm{naive}}\cap\Gamma_0(T)$-modular forms of weight k over B in the same way.

To consider the Tate curve and the q-expansions of modular forms, we prefer to use $q^{1/M}$ instead q in [**Ka2**] to be consistent with the classical terminology. We thus let $q^{1/M}$ be a variable and set $q=(q^{1/M})^M$, and consider the Tate curve $\mathrm{Tate}(q)$ = "$\mathbb{G}_m/q^{\mathbb{Z}}$" over $\mathbb{Z}((q))$. We remind of us that there is a canonical isomorphism $\widehat{\mathrm{Tate}(q)} \cong \widehat{\mathbb{G}}_m$ of formal Lie groups over $\mathbb{Z}((q))$. On the other hand, for any positive integer n, $\mathrm{Tate}(q)[n]$ "is" $\mathbb{G}_m/q^{\mathbb{Z}}[n]$. Precisely, $\mathrm{Tate}(q)[n]$ is isomorphic to the group scheme $T[n]$ in [**KM**, (8.7)], and $T[n](R)=(R^{\times}/q^{\mathbb{Z}})[n]$ for any $\mathbb{Z}((q))$-algebra R. Thus for $r\in R^{\times}$ with $r^n\in q^{\mathbb{Z}}$, we use the symbol r "mod $q^{\mathbb{Z}}$" to denote the corresponding element in $\mathrm{Tate}(q)[n](R)$. Over $\mathbb{Z}((q^{1/M}))$, $\mathrm{Tate}(q)$ carries the following structures:

$$\begin{cases} \bullet\ \text{canonical invariant differential } \omega_{\mathrm{can}} = \text{“}dx/x\text{”, where } x \text{ is the standard} \\ \quad \text{parameter on } \mathbb{G}_m, \\ \bullet\ \text{canonical } \Gamma(M)^{\mathrm{arith}}\text{-structure } \beta_{M,\mathrm{can}} : \boldsymbol{\mu}_M \times \mathbb{Z}/M\mathbb{Z} \xrightarrow{\sim} \mathrm{Tate}(q)[M] \\ \quad \text{satisfying } \beta_{M,\mathrm{can}}(\zeta,n) = \zeta q^{n/M} \text{ “mod } q^{\mathbb{Z}}\text{”}, \\ \bullet\ \text{canonical } \Gamma_0(T)\text{-structure } C_{T,\mathrm{can}} = \boldsymbol{\mu}_T \text{ “mod } q^{\mathbb{Z}}\text{”}. \end{cases} \tag{2.1.3}$$

We can then define the q-expansion map

$$\begin{aligned} R^k(B, \Gamma_{M,T}) &\to B \otimes_{\mathbb{Z}} \mathbb{Z}((q^{1/M})) \subseteq B((q^{1/M})) \\ F &\mapsto F((\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{M,\mathrm{can}}, C_{T,\mathrm{can}})_B) =: F_q, \end{aligned} \tag{2.1.4}$$

where the subscript "$_B$" indicates the base extension from $\mathbb{Z}((q^{1/M}))$ to $B \otimes_{\mathbb{Z}} \mathbb{Z}((q^{1/M}))$; but when there is no fear of confusion, we express F_q simply by $F(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{M,\mathrm{can}}, C_{T,\mathrm{can}})$. The usual q-expansion principle (cf. [**Ka2**, 2.2]) holds for this map thanks to the geometric irreducibility of $\mathfrak{M}(\Gamma_{M,T})$ over $\mathbb{Z}[1/T]$; cf. 1.1.

2.2. Situation over $\mathbb{C}$.

As for classical modular forms over $\mathbb{C}$, we follow the formulation of Katz [**Ka2**, Chapter I], which we now recall.

Set

$$GL^+ := \{(\omega_1, \omega_2) \in \mathbb{C}^2 \mid \mathrm{Im}(\omega_2/\omega_1) > 0\}. \tag{2.2.1}$$

Via the map $(\omega_1, \omega_2) \mapsto L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, GL^+ corresponds bijectively with the set of lattices in $\mathbb{C}$ with oriented bases.

The group $SL_2(\mathbb{Z})$ acts on GL^+ from the right, and

$$\mathcal{L} := GL^+/SL_2(\mathbb{Z}) \tag{2.2.2}$$

is the set of lattices in $\mathbb{C}$. To $L \in \mathcal{L}$ corresponds a pair $(\mathbb{C}/L, dz)$ where z is a variable on $\mathbb{C}$, to which then corresponds a pair (E, ω) consisting of an elliptic curve E over $\mathbb{C}$ and a nowhere-vanishing invariant differential ω on it. Precisely, the Weierstrass theory gives an isomorphism $\mathbb{C}/L \xrightarrow{\sim} E(\mathbb{C})$, through which dz and ω correspond. This establishes a bijection between $\mathcal{L}$ and the set of isomorphism classes of $(\mathbb{C}/L, dz)$, and also that of (E, ω) over $\mathbb{C}$. In what follows, we will sometimes identify $(\mathbb{C}/L, dz)$ and (E, ω), especially $\mathbb{C}/L$ and $E(\mathbb{C})$, when their correspondence is obvious.

Set

$$a(L) := \frac{1}{2i}(\overline{\omega}_1\omega_2 - \omega_1\overline{\omega}_2) \text{ with } (\omega_1, \omega_2) \text{ an oriented basis of } L \tag{2.2.3}$$

where the bar indicates the complex conjugation. Then the e_M-pairing on $E[M] = (1/M)L/L$ is given by

$$e_M\left(\frac{\ell_1}{M}, \frac{\ell_2}{M}\right) = \exp\left(\frac{\pi}{Ma(L)}(\overline{\ell}_1\ell_2 - \ell_1\overline{\ell}_2)\right). \tag{2.2.4}$$

$\mathbb{C}^\times$ acts on GL^+ as $\lambda : (\omega_1, \omega_2) \mapsto (\lambda\omega_1, \lambda\omega_2)$, and we have an isomorphism

$$GL^+/\mathbb{C}^\times \xrightarrow{\sim} H := \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\} \tag{2.2.5}$$

by $(\omega_1, \omega_2) \mapsto \tau = \omega_2/\omega_1$. The action of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ on the left hand side commutes with the action $\tau \mapsto (d\tau + b)/(c\tau + a)$ on the right hand side via this isomorphism.

A function $F : GL^+ \to \mathbb{C}$ is said to have weight $k \in \mathbb{Z}$ if it satisfies

$$F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-k}F(\omega_1, \omega_2) \text{ for all } \lambda \in \mathbb{C}^\times. \tag{2.2.6}$$

If a holomorphic function $F : GL^+ \to \mathbb{C}$ is invariant under the action of $\left(\begin{smallmatrix}1 & M\\ 0 & 1\end{smallmatrix}\right)$, i.e. $F(\omega_1, \omega_2 + M\omega_1) = F(\omega_1, \omega_2)$, then the function on H, $\tau \mapsto F(2\pi i, 2\pi i\tau)$ has the Fourier expansion

$$F(2\pi i, 2\pi i\tau) = \sum_{n\in\mathbb{Z}} a_n q^{n/M} \text{ with } q^{1/M} = e^{2\pi i\tau/M}. \tag{2.2.7}$$

If moreover F has weight k, F is uniquely determined by this q-expansion:

$$F(\omega_1, \omega_2) = \left(\frac{2\pi i}{\omega_1}\right)^k \sum_{n\in\mathbb{Z}} a_n \mathrm{exp}\left(\frac{2\pi i\omega_2}{M\omega_1}\cdot n\right). \tag{2.2.8}$$

Definition (2.2.9). Let $\Gamma(M)$ and $\Gamma_0(T)$ be the usual congruence subgroups of $SL_2(\mathbb{Z})$. A holomorphic function $F : GL^+ \to \mathbb{C}$ is called a modular form of weight k on $\Gamma(M) \cap \Gamma_0(T)$ if it satisfies:

$$\begin{cases} \bullet\ F \text{ is invariant under } \Gamma(M) \text{ and } \Gamma_0(T), \\ \bullet\ F \text{ has weight } k, \\ \bullet\ \text{Every transform of } F \text{ by an element of } SL_2(\mathbb{Z}) \text{ has the } q\text{-expansion (2.2.7)} \\ \quad \text{in } \mathbb{C}((q^{1/M})). \end{cases}$$

Proposition (2.2.10) ([**Ka2**, 2.4]). *For an element F of $R^k(\mathbb{C}, \Gamma_{M,T})$, define the function F^{an} on GL^+ by*:

$$F^{\mathrm{an}}(\omega_1, \omega_2) := F\left(\frac{\mathbb{C}}{\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2}, dz, \beta(e^{2\pi ia/M}, b) = \frac{a\omega_1 + b\omega_2}{M}, C = \left\langle \frac{\omega_1}{M} \right\rangle\right).$$

Then the correspondence $F \mapsto F^{\mathrm{an}}$ gives an isomorphism of $R^k(\mathbb{C}, \Gamma_{M,T})$ to the space of modular forms of weight k on $\Gamma(M) \cap \Gamma_0(T)$ in the sense of (2.2.9).

This isomorphism preserves q-expansions: *the q-expansion* (2.2.7) *of $F^{\mathrm{an}}(2\pi i, 2\pi i\tau)$ coincides with $F((\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{M,\mathrm{can}}, C_{T,\mathrm{can}})_{\mathbb{C}})$*. □

2.3. Modular forms on $\Gamma(l^\infty M)^{\mathrm{arith}} \cap \Gamma_0(T)$.

We fix a prime number l not dividing MT.

From now on, we fix l^n-th roots q^{1/l^nM} of $q^{1/M}$ in such a way that $(q^{1/l^mM})^{l^{m-n}} = q^{1/l^nM}$ for all $m \geq n$. Then the Tate curve Tate(q) considered over $\mathbb{Z}((q^{1/l^nM}))$ carries, in addition to the data (2.1.3), the canonical $\Gamma(l^n)^{\mathrm{arith}}$-structure (to be precise, with respect to this choice)

$$\beta_{l^n,\mathrm{can}} : \boldsymbol{\mu}_{l^n} \times \mathbb{Z}/l^n\mathbb{Z} \xrightarrow{\sim} \mathrm{Tate}(q)[l^n]; \quad (\eta, b) \mapsto \eta q^{b/l^n} \text{ “mod } q^{\mathbb{Z}}\text{”} \tag{2.3.1}$$

and further over $\varinjlim_n \mathbb{Z}((q^{1/l^nM}))$, the canonical $\Gamma(l^\infty)^{\mathrm{arith}}$-structure

$$\beta_{l^\infty,\mathrm{can}} := (\beta_{l^n,\mathrm{can}})_{n\geq 1}. \tag{2.3.2}$$

By means of (2.3.1), with $\beta_{l^n M,\mathrm{can}} = (\beta_{l^n,\mathrm{can}}, \beta_{M,\mathrm{can}})$, we can define the injective q-expansion map

$$R^k(B, \Gamma_{l^n M,T}) \to B \otimes_{\mathbb{Z}} \mathbb{Z}((q^{1/l^n M})) \tag{2.3.3}$$

as in (2.1.4).

When $m \geq n$, there is an obvious correspondence ($\Gamma_{l^m M,T}$-test objects over S)$\to$ ($\Gamma_{l^n M,T}$-test objects over S) for any $\mathbb{Z}[1/T]$-scheme S. Thus for any $\mathbb{Z}[1/T]$-algebra B, we obtain a homomorphism

$$R^k(B, \Gamma_{l^n M,T}) \to R^k(B, \Gamma_{l^m M,T}). \tag{2.3.4}$$

The q-expansion maps clearly commute with this map

$$\begin{tikzcd}
R^k(B, \Gamma_{l^n M,T}) \arrow[r] \arrow[d] & B \otimes_{\mathbb{Z}} \mathbb{Z}((q^{1/l^n M})) \arrow[d, "\mathrm{incl.}"] \\
R^k(B, \Gamma_{l^m M,T}) \arrow[r] & B \otimes_{\mathbb{Z}} \mathbb{Z}((q^{1/l^m M}))
\end{tikzcd} \tag{2.3.5}$$

and especially (2.3.4) is injective.

Definition (2.3.6). Let B be a $\mathbb{Z}[1/T]$-algebra. A modular form F over B of weight k on

$$\Gamma_{l^\infty M,T} := \Gamma(l^\infty M)^{\mathrm{arith}} \cap \Gamma_0(T)$$

is a rule which assigns to each $\Gamma_{l^\infty M,T}$-test object (1.3.8), $(E, \omega, \beta_{l^\infty M}, C_T)$ over a B-algebra B', an element $F(E, \omega, \beta_{l^\infty M}, C_T) \in B'$ satisfying the same properties as (2.1.2), (i) and (ii). We denote by $R^k(B, \Gamma_{l^\infty M,T})$ the B-module of all such forms.

We have a natural homomorphism

$$\varinjlim_n R^k(B, \Gamma_{l^n M,T}) \to R^k(B, \Gamma_{l^\infty M,T}) \tag{2.3.7}$$

in a similar manner as (2.3.4).

Lemma (2.3.8). *The above homomorphism* (2.3.7) *is an isomorphism.*

Proof. Giving an element $F \in R^k(B, \Gamma_{l^n M,T})$ is equivalent to giving a rule f which assigns to each $\Gamma_{l^n M,T}$-curve $(E, \beta_{l^n M}, C_T)$ over a B-scheme S an element $f(E, \beta_{l^n M}, C_T) \in H^0(S, \underline{\omega}^{\otimes k})$ compatibly with Cartesian squares, where $\underline{\omega}$ is the direct image of $\Omega^1_{E/S}$ to S. The correspondence $F \leftrightarrow f$ is given by

$$F(E, \omega, \beta_{l^n M}, C_T)\omega^{\otimes k} = f(E, \beta_{l^n M}, C_T)$$

cf. [**Ka1**, 1.1, 1.2]. From this point of view, when $l^n M \geq 3$ so that the $\Gamma_{l^n M,T}$-moduli problem is representable, the "evaluation at the universal object" gives a canonical isomorphism

$$R^k(B,\Gamma_{l^nM,T}) \cong H^0(\mathfrak{M}(\Gamma_{l^nM,T})_{/B}, \underline{\omega}_n^{\otimes k})$$

where $\underline{\omega}_n$ is defined as above for $\mathfrak{M}(\Gamma_{l^nM,T})_{/B}$ and the universal elliptic curve over it.

On the other hand, for $m \geq n$, the natural morphisms $\mathfrak{M}(\Gamma_{l^mM,T}) \to \mathfrak{M}(\Gamma_{l^nM,T})$ are affine, and there is the projective limit

$$\mathfrak{M}(\Gamma_{l^\infty M,T}) := \varprojlim_n \mathfrak{M}(\Gamma_{l^nM,T})$$

in the category of $\mathbb{Z}[1/T]$-schemes. (Explicitly it is $\mathrm{Spec}(\varinjlim_n A_n)$ if $\mathfrak{M}(\Gamma_{l^nM,T}) = \mathrm{Spec}(A_n)$.) This scheme represents the functor

$$(\text{schemes}/\mathbb{Z}[1/T]) \to (\text{isomorphism classes of } \Gamma_{l^\infty M,T}\text{-curves}).$$

Therefore for the same reason as above, we have an isomorphism

$$R^k(B,\Gamma_{l^\infty M,T}) \cong H^0(\mathfrak{M}(\Gamma_{l^\infty M,T})_{/B}, \underline{\omega}_\infty^{\otimes k})$$

with the obvious definition of $\underline{\omega}_\infty$. Our claim is then equivalent to the isomorphy of

$$\varinjlim_n H^0(\mathfrak{M}(\Gamma_{l^nM,T})_{/B}, \underline{\omega}_n^{\otimes k}) \to H^0(\mathfrak{M}(\Gamma_{l^\infty M,T})_{/B}, \underline{\omega}_\infty^{\otimes k})$$

which is clear. □

Corollary (2.3.9). *We have the injective q-expansion map*

$$R^k(B,\Gamma_{l^\infty M,T}) \to B \otimes_{\mathbb{Z}} \varinjlim_n \mathbb{Z}((q^{1/l^nM})). \qquad \square$$

By (2.3.8), we may consider $R^k(B,\Gamma_{l^nM,T})$ as a subspace of $R^k(B,\Gamma_{l^\infty M,T})$. This allows us to apply the operators "$|\,g$" studied below (cf. (3.3.6)) for elements of $R^k(B,\Gamma_{l^nM,T})$ (though the image may not have the same level).

3. Some operators on test objects and modular forms.

3.1. Nebentypus.

Each element $(a,b) \in (\mathbb{Z}/M\mathbb{Z})^\times \times (\mathbb{Z}/M\mathbb{Z})^\times$ determines an automorphism of $\boldsymbol{\mu}_M \times \mathbb{Z}/M\mathbb{Z}$ by the rule $(\zeta, n) \mapsto (\zeta^a, bn)$. If β_M is a $\Gamma(M)^{\mathrm{arith}}$-structure on an elliptic curve E over S, $\beta_M \circ (a,b) : \boldsymbol{\mu}_M \times \mathbb{Z}/M\mathbb{Z} \xrightarrow{\sim} E[M]$ is a $\Gamma(M)^{\mathrm{arith}}$-structure on E/S if and only if $b = a^{-1}$. We thus set

$$h_a := (a, a^{-1}) \ \text{ for } \ a \in (\mathbb{Z}/M\mathbb{Z})^\times \tag{3.1.1}$$

and make the following:

Definition (3.1.2). When $(E, \omega, \beta_M, C_T)$ is a $\Gamma_{M,T}$-test object, we set

$$h_a(E, \omega, \beta_M, C_T) := (E, \omega, \beta_M \circ h_a, C_T).$$

When $F \in R^k(B, \Gamma_{M,T})$, we define $F \,|\, h_a \in R^k(B, \Gamma_{M,T})$ by

$$(F \,|\, h_a)(E, \omega, \beta_M, C_T) := F(h_a(E, \omega, \beta_M, C_T)).$$

If $\rho : (\mathbb{Z}/M\mathbb{Z})^\times \to B^\times$ is a homomorphism, we say that $F \in R^k(B, \Gamma_{M,T})$ has the character ρ if

$$F \,|\, h_a = \rho(a) F \;\text{ for all }\; a \in (\mathbb{Z}/M\mathbb{Z})^\times.$$

3.2. Degeneracy operators.

Let d be a positive integer prime to MT. Consider a $\Gamma_{M,dT}$-test object $(E, \omega, \beta_M, C_{dT})$ over a $\mathbb{Z}[1/dT]$-scheme S. Here, C_{dT} is a cyclic subgroup scheme of order dT of E, and hence we have $C_{dT} = C_T \times_S C_d$ with $C_T = C_{dT}[T]$ and $C_d = C_{dT}[d]$.

Definition (3.2.1). With the notation as above, we define

$$[d]_{M,T} = [d] : (\Gamma_{M,dT}\text{-test objects over } S) \to (\Gamma_{M,T}\text{-test objects over } S),$$
$$[d](E, \omega, \beta_M, C_{dT}) = (E', \omega', \beta'_M, C'_T)$$

as follows:

- $E' := E/C_d$ with $\pi : E \to E'$ the quotient morphism,
- $\omega' := \check{\pi}^* \omega$, where $\check{\pi}$ is the isogeny dual to π,
- $\beta'_M := (\pi \circ \beta_M)^\sim$, cf. (1.2.3),
- $C'_T := \pi(C_T)$.

When B is a $\mathbb{Z}[1/dT]$-algebra, we define

$$R^k(B, \Gamma_{M,T}) \to R^k(B, \Gamma_{M,dT})$$
$$F \mapsto F \,|\, [d]_{M,T} = F \,|\, [d]$$

by $(F \,|\, [d])(E, \omega, \beta_M, C_{dT}) := F([d](E, \omega, \beta_M, C_{dT}))$.

Proposition (3.2.2). *Let F be an element of $R^k(B, \Gamma_{M,T})$ with B a $\mathbb{Z}[1/dT]$-algebra. Let*

$$F_q = F((\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{M,\mathrm{can}}, C_{T,\mathrm{can}})_B) = \sum_n a_n q^{n/M}$$

be the q-expansion (2.1.4) *of F. Then we have*

$$(F \mid [d])_q = \sum_n a_n q^{dn/M}.$$

Proof. We consider the effect of $[d]$ on $(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{M,\mathrm{can}}, C_{dT,\mathrm{can}})$ over $\mathbb{Z}[1/dT]((q^{1/M}))$.

First, $\mathrm{Tate}(q)/C_{d,\mathrm{can}} = \mathrm{Tate}(q)/\boldsymbol{\mu}_d = \mathrm{Tate}(q^d)$, the isogeny $\pi : \mathrm{Tate}(q) \to \mathrm{Tate}(q^d)$ corresponds to the d-th power homomorphism on $\mathbb{G}_m$, and $\check{\pi}^* \omega_{\mathrm{can}} = \omega_{\mathrm{can}}$ on $\mathrm{Tate}(q^d)$, cf. [**Ka1**, pages Ka-22 and Ka-23].

Then, since $\pi \circ \beta_{M,\mathrm{can}}(\eta, b) = \eta^d q^{db/M}$ "mod $q^{d\mathbb{Z}}$", it follows from the definition (1.2.3) that $(\pi \circ \beta_{M,\mathrm{can}})^{\sim}(\eta, b) = \eta q^{bd/M}$ "mod $q^{d\mathbb{Z}}$", i.e. $(\pi \circ \beta_{M,\mathrm{can}})^{\sim} = \beta_{M,\mathrm{can}}$ on $\mathrm{Tate}(q^d)$. It is clear that $\pi(C_{T,\mathrm{can}}) = C_{T,\mathrm{can}}$ on $\mathrm{Tate}(q^d)$.

Therefore, if $\varphi_d : \mathbb{Z}[1/dT]((q^{1/M})) \to \mathbb{Z}[1/dT]((q^{1/M}))$ is the $\mathbb{Z}[1/dT]$-algebra homomorphism sending $q^{1/M}$ to $q^{d/M}$, the quadruple computed above is the base extension of $(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{M,\mathrm{can}}, C_{T,\mathrm{can}})$ by φ_d. Our claim follows from the property (2.1.2), (i). □

Corollary (3.2.3). *Let d and d' be positive integers prime to MT. Then, for any $\mathbb{Z}[1/dd'T]$-algebra B, the following diagram commutes*

$$\begin{tikzcd}
R^k(B, \Gamma_{M,T}) \arrow[r, "|[d]"] \arrow[d, "|[d']"'] & R^k(B, \Gamma_{M,dT}) \arrow[d, "|[d']"] \\
R^k(B, \Gamma_{M,d'T}) \arrow[r, "|[d]"'] & R^k(B, \Gamma_{M,dd'T})
\end{tikzcd}$$

and the composites of the consecutive arrows in fact coincide with $[dd']$.

Proof. This follows from (3.2.2) and the q-expansion principle. □

3.3. Action of $GL_2(\mathbb{Q}_l)$ and its subgroup $G(l)$.

We return to the situation considered in 1.3 and 2.3.

Lemma (3.3.1). *Let (E, α_{l^∞}) be a $\Gamma(l^\infty)^{\mathrm{naive}}$-curve over a $\mathbb{Z}[1/l]$-scheme S. For a matrix $g \in GL_2(\mathbb{Q}_l) \cap M_2(\mathbb{Z}_l)$, there is an elliptic curve E'/S, a $\Gamma(l^\infty)^{\mathrm{naive}}$-structure α'_{l^∞} on it, and an S-isogeny $\pi : E \to E'$ whose degree is a power of l, making the following diagram commutative*:

$$\begin{tikzcd}
\underline{\mathbb{Z}}_l \times \underline{\mathbb{Z}}_l \arrow[r, "\alpha_{l^\infty}", "\sim"'] \arrow[d, "g"'] & \underline{T}_l(E) \arrow[d, "\underline{T}_l(\pi)"] \\
\underline{\mathbb{Z}}_l \times \underline{\mathbb{Z}}_l \arrow[r, "\sim", "\alpha'_{l^\infty}"'] & \underline{T}_l(E').
\end{tikzcd}$$

The triple $(E', \alpha'_{l^\infty}, \pi)$ is unique up to canonical isomorphisms over S.

Proof. Let $\underline{\mathbb{Q}_l/\mathbb{Z}_l}$ (resp. $E(l)$) be the constant l-divisible (Barsotti–Tate) group of height one (resp. the l-divisible group attached to E). Then giving a $\Gamma(l^\infty)^{\mathrm{naive}}$-structure α_{l^∞} on E/S, defined as an isomorphism of projective systems in (1.3.1), is equivalent to giving an isomorphism of l-divisible groups $\underline{\mathbb{Q}_l/\mathbb{Z}_l} \times \underline{\mathbb{Q}_l/\mathbb{Z}_l} \overset{\sim}{\to} E(l)$ over S which we denote by the same symbol α_{l^∞}. Our claim is then equivalent to the existence of the following commutative diagram for the l-divisible groups over S:

$$\begin{tikzcd}
\underline{\mathbb{Q}_l/\mathbb{Z}_l} \times \underline{\mathbb{Q}_l/\mathbb{Z}_l} \arrow[r, "\alpha_{l^\infty}", "\sim"'] \arrow[d, "g"'] & E(l) \arrow[d, "\pi"] \\
\underline{\mathbb{Q}_l/\mathbb{Z}_l} \times \underline{\mathbb{Q}_l/\mathbb{Z}_l} \arrow[r, "\sim"] & E'(l).
\end{tikzcd} \qquad (**)$$

Now given g, $g^{-1}(\mathbb{Z}_l \times \mathbb{Z}_l)/(\mathbb{Z}_l \times \mathbb{Z}_l)$ determines a finite subgroup scheme F_g of E/S of order a power of l via α_{l^∞}. If we set $E' := E/F_g$ and let $\pi : E \to E'$ be the quotient morphism, there is the unique isomorphism at the bottom horizontal arrow making the diagram $(**)$ commutative, which gives α'_{l^∞}.

Conversely, if we have the commutative diagram in our claim, π, whose degree is assumed to be a power of l, must be the quotient morphism by F_g, and the $\Gamma(l^\infty)^{\mathrm{naive}}$-structure α'_{l^∞} is uniquely determined by π. □

With the above notation, we write $g(E, \alpha_{l^\infty})$ for (the isomorphism class of) (E', α'_{l^∞}).

Corollary (3.3.2). *Let g and g' be two elements of $GL_2(\mathbb{Q}_l) \cap M_2(\mathbb{Z}_l)$. Then we have*

$$g'(g(E, \alpha_{l^\infty})) \cong (g'g)(E, \alpha_{l^\infty}).$$

This action of the semigroup $GL_2(\mathbb{Q}_l) \cap M_2(\mathbb{Z}_l)$ uniquely extends to the action of $GL_2(\mathbb{Q}_l)$ on the set of isomorphism classes of $\Gamma(l^\infty)^{\mathrm{naive}}$-curves over S.

Proof. Let us denote by $F_1(S)$ the set of isomorphism classes of $\Gamma(l^\infty)^{\mathrm{naive}}$-curves over S. The uniqueness in (3.3.1) implies that $(E, \alpha_{l^\infty}) \mapsto g(E, \alpha_{l^\infty})$ in fact gives the action of $GL_2(\mathbb{Q}_l) \cap M_2(\mathbb{Z}_l)$ on $F_1(S)$. But $l = \begin{pmatrix} l & 0 \\ 0 & l \end{pmatrix}$ acts trivially on $F_1(S)$, and hence the latter claim follows. □

Remark (3.3.3). Let $F_2(S)$ be the set of isomorphism classes of the pair consisting of an elliptic curve up to isogeny of l-power degree, $E \otimes \mathbb{Z}[1/l]$, and an isomorphism of $\mathbb{Q}_l$-sheaves $\underline{\mathbb{Q}}_l \times \underline{\mathbb{Q}}_l \xrightarrow{\sim}$ (the $\mathbb{Q}_l$-sheaf associated with $\underline{T}_l(E)$) on the étale site of S. Then according to Deligne('s argument) [**D**, Corollaire 3.5], the natural map $F_1(S) \to F_2(S)$ is bijective. The action of $GL_2(\mathbb{Q}_l)$ on $F_1(S)$ we have just described is nothing but the one corresponding to the obvious action on $F_2(S)$. We have preferred the above rather elementary description.

We now choose and fix a system $(\zeta_{l^n})_{n \geq 1} \subset \overline{\mathbb{Q}}^\times$ of primitive l^n-th roots of unity satisfying $\zeta_{l^{n+1}}^l = \zeta_{l^n}$ for all $n \geq 1$. Let S be a $\mathbb{Z}[1/l, \zeta_{l^\infty}] := \mathbb{Z}[1/l, \zeta_{l^n}\ (n \geq 1)]$-scheme. The choice of $(\zeta_{l^n})_{n \geq 1}$ determines isomorphisms $\boldsymbol{\mu}_{l^n} \cong \mathbb{Z}/l^n\mathbb{Z}$ ($\zeta_{l^n} \leftrightarrow 1 \bmod l^n$) and $\underline{\mathbb{Z}}_l(1) \cong \underline{\mathbb{Z}}_l$ over S. For an elliptic curve E/S, we identify a $\Gamma(l^\infty)^{\mathrm{arith}}$-structure β_{l^∞} with a $\Gamma(l^\infty)^{\mathrm{naive}}$-structure α_{l^∞} of determinant $(\zeta_{l^n})_{n \geq 1}$ by means of this latter isomorphism, cf. (1.3.5), and similarly for $\Gamma(l^n)^{\mathrm{arith}}$- and $\Gamma(l^n)^{\mathrm{naive}}$-structures. Set

$$G(l) := \{g \in GL_2(\mathbb{Q}_l) \mid \det(g) \text{ is a power of } l\}. \tag{3.3.4}$$

Let g be an element of $G(l) \cap M_2(\mathbb{Z}_l)$. If (E, α_{l^∞}) is a $\Gamma(l^\infty)^{\mathrm{naive}}$-curve over S and $g(E, \alpha_{l^\infty}) = (E', \alpha'_{l^\infty})$, it follows from (1.3.7) that $\det(\alpha_{l^\infty}) = \det(\alpha'_{l^\infty})$. We can therefore consider the action of $G(l)$ on the set of isomorphism classes of $\Gamma(l^\infty)^{\mathrm{arith}}$-curves over S via the above identification which we write as $(E, \beta_{l^\infty}) \mapsto g(E, \beta_{l^\infty})$.

Now let M and T be relatively prime positive integers, and assume that l does not divide MT. Let S be a $\mathbb{Z}[1/lT, \zeta_{l^\infty}]$-scheme.

Proposition (3.3.5). *Let the notation and the assumption be as above. Then there is the unique action of $G(l)$ on the set of isomorphism classes of $\Gamma_{l^\infty M,T}$-test objects over S (cf. (1.3.8)), described as follows: Let $X = (E, \omega, \beta_{l^\infty}, \beta_M, C_T)$ be such an object. Let g be an element of $G(l) \cap M_2(\mathbb{Z}_l)$, and $g(E, \beta_{l^\infty}) = (E', \beta'_{l^\infty})$ with the quotient morphism $\pi : E \to E'$. Then we have*

$$gX := (E', \check{\pi}^*\omega, \beta'_{l^\infty}, (\pi \circ \beta_M)^{\sim}, \pi(C_T)).$$

Proof. Take $g, g' \in G(l) \cap M_2(\mathbb{Z}_l)$. For (E, β_{l^∞}), let (E', β'_{l^∞}) and $\pi : E \to E'$ be as above, and define $g'(E', \beta'_{l^\infty}) = (E'', \beta''_{l^\infty})$ and $\pi' : E' \to E''$ similarly. To show that $g'(gX) \cong (g'g)X$, the only non-obvious point is the relation

$$(\pi' \circ (\pi \circ \beta_M)^{\sim})^{\sim} = ((\pi' \circ \pi) \circ \beta_M)^{\sim}$$

which follows from the computation

$$(\pi' \circ (\pi \circ \beta_M)^{\sim})^{\sim}(\eta, b) \overset{(1.2.3)}{=} \pi' \circ (\pi \circ \beta_M)^{\sim}(\eta^{\deg(\pi')^{-1}}, b) \overset{(1.2.3)}{=} (\pi' \circ \pi) \circ \beta_M(\eta^{\deg(\pi' \circ \pi)^{-1}}, b).$$

When $g = \left(\begin{smallmatrix} l^a & 0 \\ 0 & l^a \end{smallmatrix}\right)$ $(a \geq 0)$, $\pi : E \to E' = E$ is multiplication by l^a so that

$$(\pi \circ \beta_M)^{\sim}(\eta, b) = l^a \beta_M(\eta^{l^{-2a}}, b) = \beta_M \circ h_{l^{-a}}(\eta, b)$$

(cf. 3.1.1). We therefore have

$$\begin{pmatrix} l^a & 0 \\ 0 & l^a \end{pmatrix} (E, \omega, \beta_{l^\infty}, \beta_M, C_T) = (E, l^a\omega, \beta_{l^\infty}, \beta_M \circ h_{l^{-a}}, C_T).$$

This action of $\left(\begin{smallmatrix} l^a & 0 \\ 0 & l^a \end{smallmatrix}\right)$ is bijective on the set of isomorphism classes of $\Gamma_{l^\infty M,T}$-test objects over S (in which l is invertible). We can thus extend the action of $G(l) \cap M_2(\mathbb{Z}_l)$ to the whole group $G(l)$. □

Definition (3.3.6). Let B be a $\mathbb{Z}[1/lT, \zeta_{l^\infty}]$-algebra. For $F \in R^k(B, \Gamma_{l^\infty M,T})$ (cf. (2.3.6)) and $g \in G(l)$, we define $F \,|\, g \in R^k(B, \Gamma_{l^\infty M,T})$ by

$$(F \,|\, g)(X) := F(gX)$$

for all $\Gamma_{l^\infty M,T}$-test objects X over B-algebras.

Actually, in our later applications, we only need the action of the following matrices in $G(l)$ with $i, j \in \mathbb{Z}$:

$$\begin{cases} \begin{pmatrix} l^a & 0 \\ 0 & l^a \end{pmatrix} \text{ which we have already described,} \\ a_{r,i} := \begin{pmatrix} 1 & -iM \\ 0 & l^r \end{pmatrix}; \text{ and } A_{r,i} := l^{-r}a_{r,i} = \begin{pmatrix} 1/l^r & -iM/l^r \\ 0 & 1 \end{pmatrix}, \\ b_{r,j} := \begin{pmatrix} l^r & -jM \\ 0 & l^r \end{pmatrix}; \text{ and } B_{r,j} := l^{-r}b_{r,j} = \begin{pmatrix} 1 & -jM/l^r \\ 0 & 1 \end{pmatrix}. \end{cases} \tag{3.3.7}$$

PROPOSITION (3.3.8). *Let F be an element of $R^k(B, \Gamma_{l^\infty M,T})$ with its q-expansion $F_q = \sum_n a_n q^{n/l^c M}$ for some positive integer c. With the same notation as in* (3.3.6) *and* (3.3.7)*, we have*

$$(F \mid A_{r,i})_q = \sum_n a_n (\zeta_{l^{c+r}}^i q^{1/l^{c+r}M})^n,$$

$$(F \mid B_{r,j})_q = \sum_n a_n (\zeta_{l^{c+r}}^j q^{1/l^c M})^n.$$

PROOF (cf. [**Ka1**, 1.11]). We give the proof only for the second formula, since the first one is similar. We consider the effect of $B_{r,j}$ on the Tate quintuple $(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{l^\infty,\mathrm{can}}, \beta_{M,\mathrm{can}}, C_{T,\mathrm{can}})$ over $\varinjlim_m \mathbb{Z}[1/lT, \zeta_{l^\infty}]((q^{1/l^m M})) =: R_\infty$. Write

$$B_{r,j}(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{l^\infty,\mathrm{can}}, \beta_{M,\mathrm{can}}, C_{T,\mathrm{can}}) = (E', \omega', \beta'_{l^\infty}, \beta'_M, C'_T).$$

Recall that $\beta_{l^m,\mathrm{can}}$ on $\mathrm{Tate}(q)$ is defined by (2.3.1), and we have identified $\boldsymbol{\mu}_{l^m}$ with $\mathbb{Z}/l^m\mathbb{Z}$ by our chosen ζ_{l^m} . Recall also that the action of $l^{-r} = \begin{pmatrix} l^{-r} & 0 \\ 0 & l^{-r} \end{pmatrix}$ was described in the proof of (3.3.5). Since $b_{r,j}^{-1} = \begin{pmatrix} 1/l^r & jM/l^{2r} \\ 0 & 1/l^r \end{pmatrix}$, we see from the proof of (3.3.1) that E' is the quotient by $H_{r,j} := \langle \zeta_{l^r}, \zeta_{l^{2r}}^{jM} q^{1/l^r}$ “mod $q^{\mathbb{Z}}$”$\rangle$.

The quotient of $\mathrm{Tate}(q)$ by $\langle \zeta_{l^r}$ “mod $q^{\mathbb{Z}}$”$\rangle$ is isomorphic to $\mathrm{Tate}(q^{l^r})$, and the quotient homomorphism $\pi_1 : \mathrm{Tate}(q) \to \mathrm{Tate}(q^{l^r})$ corresponds to the l^r-th power homomorphism on $\mathbb{G}_m$. The image of $H_{r,j}$ by π_1 is the subgroup $\langle \zeta_{l^r}^{jM} q$ “mod $q^{l^r\mathbb{Z}}$”$\rangle$, and the quotient of $\mathrm{Tate}(q^{l^r})$ by this subgroup is $\mathrm{Tate}(\zeta_{l^r}^{jM} q)$. Let $\pi_2 : \mathrm{Tate}(q^{l^r}) \to \mathrm{Tate}(\zeta_{l^r}^{jM} q)$ be the quotient homomorphism. We may therefore identify $E' = \mathrm{Tate}(q)/H_{r,j}$ with $\mathrm{Tate}(\zeta_{l^r}^{jM} q)$, and the quotient morphism π with $\pi_2 \circ \pi_1$. We have:

- $\check{\pi}^* \omega_{\mathrm{can}} = \check{\pi}_2^* \circ \check{\pi}_1^* \omega_{\mathrm{can}} = \check{\pi}_2^* \omega_{\mathrm{can}} = l^r \omega_{\mathrm{can}}$, so that $\omega' = \omega_{\mathrm{can}}$.
- $\beta'_{l^\infty} = (\beta'_{l^m})_{m \geq 1}$ is the unique compatible system of $\Gamma(l^m)^{\mathrm{arith}}$-structures making the following diagram commutative, for all $m \geq 1$:

$$\begin{tikzcd}
\mathbb{Z}/l^m\mathbb{Z} \times \mathbb{Z}/l^m\mathbb{Z} \arrow[r, "\sim"] \arrow[d, "b_{r,j}"'] & \boldsymbol{\mu}_{l^m} \times \mathbb{Z}/l^m\mathbb{Z} \arrow[r, "\beta_{l^m,\mathrm{can}}", "\sim"'] \arrow[d] & \mathrm{Tate}(q)[l^m] \arrow[d, "\pi"] \\
\mathbb{Z}/l^m\mathbb{Z} \times \mathbb{Z}/l^m\mathbb{Z} \arrow[r, "\sim"] & \boldsymbol{\mu}_{l^m} \times \mathbb{Z}/l^m\mathbb{Z} \arrow[r, "\sim", "\beta'_{l^m}"'] & \mathrm{Tate}(\zeta_{l^r}^{jM} q)[l^m].
\end{tikzcd}$$

The element (a, b) in the top left group is sent to $\zeta_{l^m}^{al^r} q^{bl^r/l^m}$ “mod $(\zeta_{l^r}^{jM} q)^{\mathbb{Z}}$” in the bottom right group, if we go clockwise. So, one easily checks that $\beta'_{l^m}(\eta, b) := \eta(\zeta_{l^{m+r}}^{jM} q^{1/l^m})^b$ “mod $(\zeta_{l^r}^{jM} q)^{\mathbb{Z}}$” for $m \geq 1$ give the desired system.

- Since

$$\begin{aligned}
(\pi \circ \beta_{M,\mathrm{can}})^{\sim}(\eta, b) &= \eta^{l^{-r}} q^{l^r b/M} \text{ “mod } (\zeta_{l^r}^{jM} q)^{\mathbb{Z}}\text{”} \\
&= \eta^{l^{-r}} (\zeta_{l^r}^j q^{1/M})^{l^r b} \text{ “mod } (\zeta_{l^r}^{jM} q)^{\mathbb{Z}}\text{”},
\end{aligned}$$

we have

$$\beta'_M(\eta, b) = \eta(\zeta_{l^r}^j q^{1/M})^b \text{ “mod } (\zeta_{l^r}^{jM} q)^{\mathbb{Z}}\text{”}.$$

- We clearly have $\pi(C_{T,\mathrm{can}}) = \boldsymbol{\mu}_T$.

Now the $\mathbb{Z}[1/lT, \zeta_{l^\infty}]$-algebra automorphisms of $\mathbb{Z}[1/lT, \zeta_{l^\infty}]((q^{1/l^m M}))$ sending $q^{1/l^m M}$ to $\zeta_{l^{m+r}}^j q^{1/l^m M}$ for $m \geq 1$ give rise to an automorphism of the ring R_∞. The above argument shows that $B_{r,j}$ sends the Tate quintuple to the one obtained by the base extension by this ring automorphism, and hence our conclusion follows. □

3.4. Hecke operator $U(l^r)$ on $R^k(B, \Gamma_{M,l^sT})$.

Let M, T and l be as in the previous subsection. Let E be an elliptic curve over a $\mathbb{Z}[1/lT]$-scheme S. If α_{l^s} (resp. β_{l^s}) is a $\Gamma(l^s)^{\mathrm{naive}}$-(resp. a $\Gamma(l^s)^{\mathrm{arith}}$-) structure on E/S, we call $C_{l^m} := \alpha_{l^s}(l^{s-m}\mathbb{Z}/l^s\mathbb{Z} \times \{0\})$ (resp. $\beta_{l^s}(\boldsymbol{\mu}_{l^m})$) the $\Gamma_0(l^m)$-structure associated with α_{l^s} (resp. β_{l^s}) for $1 \leq m \leq s$. Via the correspondence $\beta_{l^s} \mapsto C_{l^s}$, we have a q-expansion preserving injection

$$R^k(B, \Gamma_{M,l^sT}) \to R^k(B, \Gamma_{l^sM,T}) \tag{3.4.1}$$

as (2.3.4), for any $\mathbb{Z}[1/lT]$-algebra B. By means of this, we will consider $R^k(B, \Gamma_{M,l^sT})$ as a subspace of $R^k(B, \Gamma_{l^sM,T})$ or $R^k(B, \Gamma_{l^\infty M,T})$.

We now consider the Hecke operators $U(l^r)$ for $r \geq 1$ (which are well-known for modular forms on $\Gamma_0(N)$ or $\Gamma_1(N)$) on $R^k(B, \Gamma_{M,l^sT})$ for $s \geq 1$.

Let $X = (E, \omega, \beta_M, C_{l^sT})$ be a Γ_{M,l^sT}-test object over a B-algebra B'. There is a faithfully flat B'-algebra B'' over which E admits a $\Gamma(l^r)^{\mathrm{naive}}$-structure α_{l^r} whose associated $\Gamma_0(l)$-structure is $C_{l^sT}[l]$. The cyclic subgroups of $\mathbb{Z}/l^r\mathbb{Z} \times \mathbb{Z}/l^r\mathbb{Z}$ of order l^r which have trivial intersection with $\mathbb{Z}/l^r\mathbb{Z} \times \{0\}$ (equivalently with $l^{r-1}\mathbb{Z}/l^r\mathbb{Z} \times \{0\}$) are given by the subgroups $\left\langle \binom{iM}{1} \right\rangle$, $0 \leq i \leq l^r - 1$; and note that these correspond to subgroups $a_{r,i}^{-1}(\mathbb{Z}_l \times \mathbb{Z}_l)/(\mathbb{Z}_l \times \mathbb{Z}_l)$ of $(1/l^r)\mathbb{Z}/\mathbb{Z} \times (1/l^r)\mathbb{Z}/\mathbb{Z}$ in the notation (3.3.7). Set $K_{r,i} := \alpha_{l^r}\left(\left\langle \binom{iM}{1} \right\rangle\right) \subseteq E[l^r]$, $E_i := E/K_{r,i}$, and let $\pi_i : E \to E_i$ be the quotient homomorphism. We can then consider the Γ_{M,l^sT}-test object

$$X_i := (E_i, l^{-r}\check{\pi}_i^* \omega, (\pi_i \circ \beta_M)^\sim \circ h_{l^r}, \pi_i(C_{l^sT})).$$

For $F \in R^k(B, \Gamma_{M,l^sT})$, we define

$$(F \,|\, U(l^r))(X) := l^{-r} \sum_{i=0}^{l^r-1} F(X_i). \tag{3.4.2}$$

Proposition (3.4.3). *Let the notation be as above. Then $F \,|\, U(l^r)$ belongs to $R^k(B, \Gamma_{M,l^sT})$. If F has the q-expansion $F_q = \sum_n a_n q^{n/M}$, we have*

$$(F \,|\, U(l^r))_q = \sum_n a_{nl^r} q^{n/M}.$$

Proof. Set $S := \mathrm{Spec}(B')$. The universal situation giving the above α_{l^r} is as follows: Let $[\Gamma_0(l)]$ and $[\Gamma(l^r)^{\mathrm{naive}}] = [\Gamma(l^r)]$ be as in [**KM**, (5.1)]. Then to the $\Gamma_0(l)$-structure $C_{l^sT}[l]$ on E/S corresponds a section $S \to [\Gamma_0(l)]_{E/S}$. Form the fibre product

$[\Gamma(l^r)^{\mathrm{naive}}]_{E/S} \times_{[\Gamma_0(l)]_{E/S}} S =: \widetilde{S} = \mathrm{Spec}(\widetilde{B})$ with respect to the "associating the $\Gamma_0(l)$-structure" morphism $[\Gamma(l^r)^{\mathrm{naive}}]_{E/S} \to [\Gamma_0(l)]_{E/S}$. There is the tautological $\Gamma(l^r)^{\mathrm{naive}}$-structure $\widetilde{\alpha}_{l^r}$ on $E/\widetilde{S}$, and the above α_{l^r} is the base extension of $\widetilde{\alpha}_{l^r}$ by the unique B-algebra homomorphism $\widetilde{B} \to B''$. We may thus take $\widetilde{B}$ and $\widetilde{\alpha}_{l^r}$ for B'' and α_{l^r}.

Now $\widetilde{S}/S$ is a torsor under the group $\{g \in GL_2(\mathbb{Z}/l^r\mathbb{Z}) \mid g \bmod l$ is upper triangular$\}$. The value (3.4.2), a priori lying in $\widetilde{B}$, is easily seen to be invariant under the action of this group, and hence belongs to B'. It is straightforward to see that the rule $F \mid U(l^r)$ thus obtained satisfies (2.1.2), (i) and (ii), so that it belongs to $R^k(B, \Gamma_{M,l^sT})$.

On the other hand, we considered $R^k(B, \Gamma_{M,l^sT})$ as embedded in $R^k(B, \Gamma_{l^\infty M,T})$, and it is further embedded into the bigger space $R^k(B \otimes_{\mathbb{Z}[1/lT]} \mathbb{Z}[1/lT, \zeta_{l^\infty}], \Gamma_{l^\infty M,T})$, in the notation of the previous subsection. Being considered in this last space, we have defined $F \mid U(l^r)$ as

$$F \mid U(l^r) = l^{-r} \sum_{i=0}^{l^r-1} F \mid A_{r,i}$$

(cf. (3.3.5)–(3.3.7)), and hence our claim on the q-expansion follows from (3.3.8). □

4. CM test objects over $\mathbb{C}$.

4.1. Preliminaries on imaginary quadratic fields.

In this section, we fix an imaginary quadratic field K, and denote by $\mathfrak{o}$ its ring of integers. We also fix a prime number l, and denote by

$$\mathfrak{o}_n := \mathbb{Z} + l^n\mathfrak{o} \tag{4.1.1}$$

the order of conductor l^n of K for $n \geq 0$. Let I_n be the group of proper (fractional) $\mathfrak{o}_n$-ideals, and Cl_n the group of proper $\mathfrak{o}_n$-ideal classes. If $\mathfrak{a}$ is a proper $\mathfrak{o}_n$-ideal, we denote by $\{\mathfrak{a}\}_n$ the class of $\mathfrak{a}$ in Cl_n. We have the well-known formula

$$|\,\mathrm{Cl}_n| = |\,\mathrm{Cl}_0| \cdot l^n |\,\mathfrak{o}^\times : \mathfrak{o}_n^\times|^{-1} \left(1 - \left(\frac{K}{l}\right) l^{-1}\right) \quad \text{for } n \geq 1. \tag{4.1.2}$$

Here, $(K/l) = +1, -1$ or 0 according as l splits, remains prime or ramifies in K, respectively.

Let $K_{\mathbb{A}}^\times$ be the idele group of K, and $K_\infty^\times$ (resp. $K_{\mathbb{A},0}^\times$) its infinite (resp. finite) part. For $x \in K_{\mathbb{A}}^\times$ and a prime number q, we denote by $x_q \in (K \otimes_{\mathbb{Q}} \mathbb{Q}_q)^\times$ the q-component of x. When $\mathfrak{a}$ is a lattice in K and $x \in K_{\mathbb{A}}^\times$, we let $x\mathfrak{a}$ be the unique lattice in K such that $(x\mathfrak{a})_q = x_q\mathfrak{a}_q$ for all q, the subscript "$_q$" for lattices meaning the completion at q. Thus, if we let $\widehat{\mathbb{Z}}$ be the profinite completion of $\mathbb{Z}$ and $\widehat{\mathfrak{a}} := \mathfrak{a} \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$, we have $x\mathfrak{a} = x\widehat{\mathfrak{a}} \cap K$. We have the canonical isomorphism

$$K_{\mathbb{A}}^\times / K_\infty^\times \widehat{\mathfrak{o}}_n^\times = K_{\mathbb{A},0}^\times / \widehat{\mathfrak{o}}_n^\times \cong I_n \text{ by } x \mapsto x\mathfrak{o}_n \tag{4.1.3}$$

which in turn induces

$$K_{\mathbb{A}}^\times / K_\infty^\times \widehat{\mathfrak{o}}_n^\times K^\times \cong \mathrm{Cl}_n. \tag{4.1.4}$$

Denote by $\|\cdot\|$ the idele norm quasi-character of $K_{\mathbb{A}}^{\times}$. For any $n \geq 0$ and $\mathfrak{a} = a\mathfrak{o}_n$ with $a \in K_{\mathbb{A},0}^{\times}$, we can define its norm by

$$N(\mathfrak{a}) := \|a\|^{-1}. \tag{4.1.5}$$

If $n = 0$, this is of course the usual norm, and $N(\mathfrak{a}) = N(\mathfrak{a}\mathfrak{o})$ in general.

When n and m are non-negative integers, we have the obvious commutative diagram with exact horizontal lines

$$\begin{tikzcd}
0 \arrow[r] & K_\infty^\times \widehat{\mathfrak{o}}_{n+m}^\times K^\times \arrow[r] \arrow[d, "\text{incl.}"'] & K_{\mathbb{A}}^\times \arrow[r] \arrow[d, equal] & \mathrm{Cl}_{n+m} \arrow[r] \arrow[d, "p_n^{n+m}"] & 0 \\
0 \arrow[r] & K_\infty^\times \widehat{\mathfrak{o}}_n^\times K^\times \arrow[r] & K_{\mathbb{A}}^\times \arrow[r] & \mathrm{Cl}_n \arrow[r] & 0.
\end{tikzcd} \tag{4.1.6}$$

It follows that the kernel of the natural homomorphism $p_n^{n+m} : \mathrm{Cl}_{n+m} \to \mathrm{Cl}_n$ is canonically isomorphic to $K_\infty^\times \widehat{\mathfrak{o}}_n^\times K^\times / K_\infty^\times \widehat{\mathfrak{o}}_{n+m}^\times K^\times \cong \mathfrak{o}_{n,l}^\times / \mathfrak{o}_{n+m,l}^\times \mathfrak{o}_n^\times$, where as above the subscript "$_l$" means the l-adic completion. When $n \geq 1$, $\mathfrak{o}_n^\times = \{\pm 1\}$, and hence this group is equal to $\mathfrak{o}_{n,l}^\times / \mathfrak{o}_{n+m,l}^\times$, and it has order l^m.

It also follows from (4.1.3) that the kernel of the natural homomorphism $I_{n+m} \to I_n$ is canonically isomorphic to $\mathfrak{o}_{n,l}^\times / \mathfrak{o}_{n+m,l}^\times$.

Proposition (4.1.7). *Choose a complete set $\{e_0, \ldots, e_{l^m-1}\}$ of representatives of $\mathfrak{o}_{n,l}^\times / \mathfrak{o}_{n+m,l}^\times$ for fixed $n \geq 1$ and $m \geq 0$. Let $\mathfrak{a} = a\mathfrak{o}_n$ be a proper $\mathfrak{o}_n$-ideal with $a \in K_{\mathbb{A}}^\times$, and set $\mathfrak{a}_i := l^{-m} e_i a \mathfrak{o}_{n+m}$.*

(1) $(p_n^{n+m})^{-1}(\{\mathfrak{a}\}_n) = \{\{\mathfrak{a}_0\}_{n+m}, \ldots, \{\mathfrak{a}_{l^m-1}\}_{n+m}\}$.

(2) *$\mathfrak{a}_i$ contains $\mathfrak{a}$, and $\mathfrak{a}_i/\mathfrak{a}$ is a cyclic group of order l^m for each i. Further, these groups constitute all cyclic subgroups of $K/\mathfrak{a}$ of order l^m which have trivial intersection with the cyclic subgroup $\mathfrak{a}\mathfrak{o}_{n-1}/\mathfrak{a}$ of order l.*

Proof. The first assertion is clear from (4.1.6).

It is easy to see that $\mathfrak{a}_i \supseteq \mathfrak{a}$, and we further have

$$\mathfrak{a}_i/\mathfrak{a} \cong \widehat{\mathfrak{a}}_i/\widehat{\mathfrak{a}} \cong l^{-m} e_i \widehat{\mathfrak{o}}_{n+m}/\widehat{\mathfrak{o}}_n \cong l^{-m}\mathfrak{o}_{n+m}/\mathfrak{o}_n$$

which is cyclic of order l^m. On the other hand,

$$\mathfrak{a}\mathfrak{o}_{n-1}/\mathfrak{a} \cong a\widehat{\mathfrak{o}}_{n-1}/a\widehat{\mathfrak{o}}_n \cong \mathfrak{o}_{n-1}/\mathfrak{o}_n \cong \mathbb{Z}/l\mathbb{Z}.$$

Thus, if $\mathfrak{a}_i/\mathfrak{a}$ has non-trivial intersection with $\mathfrak{a}\mathfrak{o}_{n-1}/\mathfrak{a}$, we must have $\mathfrak{a}\mathfrak{o}_{n-1} \subseteq \mathfrak{a}_i$. This implies that $l^m \mathfrak{o}_{n-1} \subseteq \mathfrak{o}_{n+m}$, which is impossible.

It is clear that $\mathfrak{a}_i/\mathfrak{a} \neq \mathfrak{a}_{i'}/\mathfrak{a}$ if $i \neq i'$. Since there are exactly l^m cyclic subgroups of $K/\mathfrak{a}$ of order l^m that have trivial intersection with $\mathfrak{a}\mathfrak{o}_{n-1}/\mathfrak{a}$ (cf. 3.4), the assertion (2) follows. □

Let $\{w, 1\}$ be a $\mathbb{Z}$-basis of $\mathfrak{o}$ so that $\mathfrak{o}_n = \mathbb{Z}l^n w + \mathbb{Z}$. We consider $\{l^n w, 1\}$ also as a $\mathbb{Z}_l$-basis of $\mathfrak{o}_{n,l} = \mathfrak{o}_n \otimes_{\mathbb{Z}} \mathbb{Z}_l$. In the following, we fix a positive integer M prime to l and set

$$e_{n,i} := 1 + il^n Mw \in \mathfrak{o}_{n,l}^{\times} \text{ for } i \in \mathbb{Z}. \tag{4.1.8}$$

Proposition (4.1.9). *Let the notation be as in* (4.1.7).

(1) *The elements $e_{n,i}$ for $0 \le i \le l^m - 1$ form a complete set of representatives of $\mathfrak{o}_{n,l}^{\times}/\mathfrak{o}_{n+m,l}^{\times}$. If we define $\mathfrak{a}_i$ from $\mathfrak{a} = a\mathfrak{o}_n$ using $e_i = e_{n,i}$ as in* (4.1.7)*, then $\mathfrak{a}_{i,l}$ is a free $\mathbb{Z}_l$-module with basis $\{a_l l^n w, a_l l^{-m}(1 + il^n Mw)\}$.*

(2) $e_{n,i}$ mod $\mathfrak{o}_{n+m,l}^{\times}$ *depends only on* i mod l^m. *When $n \ge m$, we have an isomorphism of groups*

$$\mathfrak{o}_{n,l}^{\times}/\mathfrak{o}_{n+m,l}^{\times} \xrightarrow{\sim} \mathbb{Z}/l^m\mathbb{Z} \ \ by \ \ e_{n,i} \mapsto i.$$

Proof. (1) We first prove the second assertion. For this, it is enough to treat the case $a_l = 1$. We thus want to show that

$$\mathfrak{a}_{i,l} = l^{-m} e_{n,i} \mathfrak{o}_{n+m,l} = \mathbb{Z}_l(l^n w) + \mathbb{Z}_l(l^{-m}(1 + il^n Mw)) =: \mathfrak{b}_{i,l}.$$

The left hand side is a free $\mathbb{Z}_l$-module with a basis consisting of $l^{-m}e_{n,i}$ and $l^{-m}e_{n,i}(l^{n+m}w) = l^n w + il^{2n}Mw^2$. Since $\mathfrak{b}_{i,l}$ contains 1 and $w^2 = aw + b$ with $a, b \in \mathbb{Z}$, we see that $\mathfrak{a}_{i,l} \subseteq \mathfrak{b}_{i,l}$. But both $\mathfrak{a}_{i,l}$ and $\mathfrak{b}_{i,l}$ contain $\mathfrak{a}_l$ as a submodule of index l^m, and hence $\mathfrak{a}_{i,l} = \mathfrak{b}_{i,l}$.

It follows from this that all $\mathfrak{a}_{i,l}$ $(0 \le i \le l^m - 1)$ are different, and hence $e_{n,i}$ in the same range are different mod $\mathfrak{o}_{n+m,l}^{\times}$.

(2) Since

$$1 + il^n Mw + l^{n+m}c \equiv 1 + il^n Mw \mod \mathfrak{o}_{n+m,l}^{\times} \text{ for any } c \in \mathfrak{o}_l,$$

$e_{n,i}$ mod $\mathfrak{o}_{n+m,l}^{\times}$ depends only on i mod l^m. If $n \ge m$, it also follows that

$$(1 + il^n Mw)(1 + i'l^n Mw) \equiv 1 + (i + i')l^n Mw \mod \mathfrak{o}_{n+m,l}^{\times}$$

for any $i, i' \in \mathbb{Z}$. □

4.2. CM test objects over $\mathbb{C}$.

We let M and T be positive integers such that $(M,T) = 1$ and $(l, MT) = 1$, which are subject to the following data on which our construction below depends.

$$\left\{\begin{array}{l} \bullet \text{ There is an integral ideal } \mathfrak{f} \text{ of } K \text{ such that } (\mathfrak{f}, \bar{\mathfrak{f}}) = 1 \text{ and } M = N(\mathfrak{f}) \\ \quad \text{(so that all prime factors of } M \text{ splits in } K\text{),} \\ \bullet \text{ There are prime ideals } \mathfrak{t}_1, \ldots, \mathfrak{t}_t \text{ of } K \text{ and } T = N(\mathfrak{t}_1 \cdots \mathfrak{t}_t) \text{ is square free} \\ \quad \text{(so that each } \mathfrak{t}_i \text{ splits or ramifies over } \mathbb{Q}\text{).} \end{array}\right. \tag{4.2.1}$$

Let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$-ideal for some $n \ge 0$. In general, when $\mathfrak{b}$ is an integral $\mathfrak{o}$-ideal prime to l, we say that $\mathfrak{a}$ is prime to $\mathfrak{b}$ if $\mathfrak{a}\mathfrak{o}$ is prime to $\mathfrak{b}$ in the usual sense. We assume that $\mathfrak{a}$ is prime to M (i.e. prime to $M\mathfrak{o}$) in the following. Thus $\mathfrak{a}_q = \mathfrak{o}_{n,q} = \mathfrak{o}_q$ for all prime numbers q dividing M, and we have $\mathfrak{a}/M\mathfrak{a} \cong \mathfrak{o}/M\mathfrak{o}$ canonically. Now to the lattice $\mathfrak{a}$ corresponds pairs

$$(\mathbb{C}/\mathfrak{a}, dz) \text{ and } (E(\mathfrak{a}), \omega_\infty(\mathfrak{a})), \quad (\mathbb{C}/\mathfrak{a} = E(\mathfrak{a})(\mathbb{C}),\ dz \leftrightarrow \omega_\infty(\mathfrak{a})) \tag{4.2.2}$$

as in 2.2, which we will often identify. Under the fixed data (4.2.1), we equip $E(\mathfrak{a})$ with the following level structures:

We define the $\Gamma(M)^{\text{naive}}$-structure

$$\alpha_M(\mathfrak{a}) : \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z} \overset{\sim}{\to} E(\mathfrak{a})[M] = \frac{1}{M}\mathfrak{a}/\mathfrak{a} \tag{4.2.3}$$

as the inverse of the composite of canonical isomorphisms

$$\frac{1}{M}\mathfrak{a}/\mathfrak{a} \overset{\sim}{\to} \mathfrak{a}/M\mathfrak{a} \overset{\sim}{\to} \mathfrak{o}/M\mathfrak{o} \overset{\sim}{\to} \mathfrak{o}/\mathfrak{f} \times \mathfrak{o}/\bar{\mathfrak{f}} \overset{\sim}{\to} \mathbb{Z}/M \times \mathbb{Z}/M.$$

We define the $\Gamma(M)^{\text{arith}}$-structure

$$\beta_M(\mathfrak{a}) : \boldsymbol{\mu}_M \times \mathbb{Z}/M\mathbb{Z} \overset{\sim}{\to} E(\mathfrak{a})[M] \text{ by } \beta_M(\mathfrak{a}) := \beta_{\alpha_M(\mathfrak{a})}, \text{ cf. (1.1.4).} \tag{4.2.4}$$

We define the $\Gamma_0(T)$-structure by

$$C_T(\mathfrak{a}) := \bigoplus_{i=1}^{t} E(\mathfrak{a})[\mathfrak{t}_{i,n}] = \bigoplus_{i=1}^{t} \mathfrak{t}_{i,n}^{-1}\mathfrak{a}/\mathfrak{a} \text{ with } \mathfrak{t}_{i,n} := \mathfrak{t}_i \cap \mathfrak{o}_n. \tag{4.2.5}$$

Finally, when $n \geq 1$, we define the $\Gamma_0(l)$-structure by

$$C_l(\mathfrak{a}) := \mathfrak{a}\mathfrak{o}_{n-1}/\mathfrak{a}, \text{ cf. (4.1.7).} \tag{4.2.6}$$

Definition (4.2.7). With the above notation, we define $\Gamma_{M,T}$- or $\Gamma_{M,lT}$-test objects over $\mathbb{C}$ respectively by

$$\begin{cases} X_{\infty,M,T}(\mathfrak{a}) := (E(\mathfrak{a}), \omega_\infty(\mathfrak{a}), \beta_M(\mathfrak{a}), C_T(\mathfrak{a})), \\ X_{\infty,M,lT}(\mathfrak{a}) := (E(\mathfrak{a}), \omega_\infty(\mathfrak{a}), \beta_M(\mathfrak{a}), C_T(\mathfrak{a}), C_l(\mathfrak{a})). \end{cases}$$

The tuples without differentials

$$\begin{cases} x_{M,T}(\mathfrak{a}) := (E(\mathfrak{a}), \beta_M(\mathfrak{a}), C_T(\mathfrak{a})), \\ x_{M,lT}(\mathfrak{a}) := (E(\mathfrak{a}), \beta_M(\mathfrak{a}), C_T(\mathfrak{a}), C_l(\mathfrak{a})) \end{cases}$$

determine $\mathbb{C}$-valued points of the modular curves $\mathfrak{M}(\Gamma_{M,T})$ and $\mathfrak{M}(\Gamma_{M,lT})$ (cf. 1.1).

Lemma (4.2.8). *Let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$-ideal prime to M. Then we have*

$$\det(\alpha_M(\mathfrak{o})) = \det(\alpha_M(\mathfrak{a}))^{l^n N(\mathfrak{a})}$$

the norm $N(\mathfrak{a})$ being defined by (4.1.5).

Proof. We can express $\mathfrak{a}$ as $\mathfrak{a} = \mathfrak{a}_1\mathfrak{a}_2^{-1}$ with integral proper $\mathfrak{o}_n$-ideals $\mathfrak{a}_1$ and $\mathfrak{a}_2$ prime to M. From the inclusion of lattices

$$\mathfrak{o} \supseteq \mathfrak{o}_n \subseteq \mathfrak{a}_2^{-1} \supseteq \mathfrak{a}$$

we have quotient homomorphisms

$$E(\mathfrak{o}) \leftarrow E(\mathfrak{o}_n) \rightarrow E(\mathfrak{a}_2^{-1}) \leftarrow E(\mathfrak{a})$$

corresponding to the natural $\mathbb{C}/\mathfrak{o} \leftarrow \mathbb{C}/\mathfrak{o}_n$ etc. These homomorphisms commute with the $\Gamma(M)^{\mathrm{arith}}$-structures $\alpha_M(\mathfrak{o}), \alpha_M(\mathfrak{o}_n)$ etc. For example, if we denote by π the morphism $E(\mathfrak{a}) \rightarrow E(\mathfrak{a}_2^{-1})$, it has degree $N(\mathfrak{a}_1)$, and $\pi \circ \alpha_M(\mathfrak{a}) = \alpha_M(\mathfrak{a}_2^{-1})$ so that we have

$$\det(\alpha_M(\mathfrak{a}_2^{-1})) = \det(\alpha_M(\mathfrak{a}))^{N(\mathfrak{a}_1)}$$

by (1.2.2); and similarly for other homomorphisms. Our result then follows. □

4.3. Effect of operators on CM test objects.

We keep the notation of 4.1 and 4.2. We study here the effect of operators considered in Section 3. First we have

Lemma (4.3.1). *Let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$-ideal prime to M with $n \geq 1$.*

i) *For the $\Gamma_{M,lT}$-test object $X_{\infty,M,lT}(\mathfrak{a})$ (cf. (4.2.7)) and the degeneracy operator $[l]$ (cf. (3.2.1)), we have*

$$[l]X_{\infty,M,lT}(\mathfrak{a}) = (E(\mathfrak{a}\mathfrak{o}_{n-1}), l\omega_\infty(\mathfrak{a}\mathfrak{o}_{n-1}), \beta_M(\mathfrak{a}\mathfrak{o}_{n-1}), C_T(\mathfrak{a}\mathfrak{o}_{n-1})),$$

the $\Gamma_{M,T}$-test object $X_{\infty,M,T}(\mathfrak{a}\mathfrak{o}_{n-1})$ with the differential multiplied by l.

ii) *Take a divisor $\mathfrak{s}$ of $\mathfrak{t}_1 \cdots \mathfrak{t}_t$ and set $S := N(\mathfrak{s})$ and $\mathfrak{s}_n := \mathfrak{s} \cap \mathfrak{o}_n$. Then we have*

$$[S]X_{\infty,M,lT}(\mathfrak{a}) = (E(\mathfrak{s}_n^{-1}\mathfrak{a}), S\omega_\infty(\mathfrak{s}_n^{-1}\mathfrak{a}), \beta_M(\mathfrak{s}_n^{-1}\mathfrak{a}), C_{lT/S}(\mathfrak{s}_n^{-1}\mathfrak{a})),$$

the $\Gamma_{M,lT/S}$-test object $X_{\infty,M,lT/S}(\mathfrak{s}_n^{-1}\mathfrak{a})$ with the differential multiplied by S.

Proof. We only give the proof for the first assertion, since the second can be proved similarly.

Set $[l]X_{\infty,M,lT}(\mathfrak{a}) = (E', \omega', \beta'_M, C'_T)$. From the definition (4.2.6), we have $E' = E(\mathfrak{a}\mathfrak{o}_{n-1})$. Let $\pi : E(\mathfrak{a}) \rightarrow E(\mathfrak{a}\mathfrak{o}_{n-1})$ be the quotient homomorphism which has degree l. Then we have

- $\omega' = \check{\pi}^*\omega_\infty(\mathfrak{a}) = l\omega_\infty(\mathfrak{a}\mathfrak{o}_{n-1})$ since $\pi^*\omega_\infty(\mathfrak{a}\mathfrak{o}_{n-1}) = \omega_\infty(\mathfrak{a})$,
- $\beta'_M = (\pi \circ \beta_M(\mathfrak{a}))^\sim \overset{(1.2.4)}{=} \beta_{\pi\circ\alpha_M(\mathfrak{a})} = \beta_M(\mathfrak{a}\mathfrak{o}_{n-1})$,

and it is clear that $C'_T = C_T(\mathfrak{a}\mathfrak{o}_{n-1})$. □

We next consider $\Gamma(l^\infty)^{\mathrm{naive}}$- and $\Gamma(l^\infty)^{\mathrm{arith}}$-structures. In general let $E = \mathbb{C}/L$ be a complex elliptic curve (not necessarily of CM type). Then we may consider a $\Gamma(l^\infty)^{\mathrm{naive}}$-structure α_{l^∞} on E (1.3.1) as an isomorphism of $\mathbb{Z}_l \times \mathbb{Z}_l$ to the l-adic Tate module $T_l(E)$. This is equivalent to fixing a $\mathbb{Z}_l$-basis $\{w_1, w_2\}$ of $T_l(E) = L \otimes_{\mathbb{Z}} \mathbb{Z}_l$; $\alpha_{l^\infty}(a, b) = aw_1 + bw_2$. In the following, we take an oriented basis $\{w_1, w_2\}$ of L itself and use it to define α_{l^∞}. The determinant of such α_{l^∞} is $(e^{2\pi i/l^u})_{u\geq 1}$ (cf. (2.2.4)).

By the action of the matrices given in (3.3.7), we obtain $a_{m,i}(E, \alpha_{l^\infty}) = A_{m,i}(E, \alpha_{l^\infty}) =: (E_{m,i}, \alpha_{l^\infty,m,i})$ which can be described as follows: $E_{m,i} = \mathbb{C}/L_{m,i}$ with $L_{m,i}$ the $\mathbb{Z}$-lattice having basis $\{w_1, l^{-m}(iMw_1 + w_2)\}$, and $\alpha_{l^\infty,m,i}$ is defined by this basis. Here, $L_{m,i}$ and $E_{m,i}$ depend only on the residue class $\bar{i}$ of i mod l^m, and hence we write them $L_{m,\bar{i}}$ and $E_{m,\bar{i}}$. From the matrix relation $B_{m,j}a_{m,i} = a_{m,i+j}$, we obtain

$$B_{m,j}(E_{m,\bar{i}}, \alpha_{l^\infty,m,i}) = (E_{m,\overline{i+j}}, \alpha_{l^\infty,m,i+j}). \tag{4.3.2}$$

We return to elliptic curves with CM. In what follows, we fix an integral basis $\{w, 1\}$ of $\mathfrak{o}$ such that $\mathrm{Im}(w) < 0$ (so that this basis is oriented), and take $\{l^n w, 1\}$ for the basis of $\mathfrak{o}_n$. When $n \geq 1$, non-zero principal $\mathfrak{o}_n$-ideals correspond bijectively with the set $K^\times/\{\pm 1\}$ ($c \leftrightarrow c\mathfrak{o}_n$). We fix a set of representatives of $K^\times/\{\pm 1\}$, which is stable under multiplication by powers of l, and take the generator of each principal $\mathfrak{o}_n$-ideal ($\neq (0)$) from this set.

Now fix integers $n \geq 1$ and $m \geq 0$. We will consider elliptic curves attached to proper $\mathfrak{o}_{n+m}$-ideals belonging to $\mathrm{Ker}(\mathrm{Cl}_{n+m} \to \mathrm{Cl}_n)$. We first take a principal $\mathfrak{o}_n$-ideal $c\mathfrak{o}_n \neq (0)$ and equip with $E(c\mathfrak{o}_n) = \mathbb{C}/c\mathfrak{o}_n$ the $\Gamma(l^\infty)^{\mathrm{naive}}$-structure $\alpha_{l^\infty}(c\mathfrak{o}_n)$ defined by the basis $\{cl^n w, c\}$. Starting with this, we can apply the above construction, and obtain

$$(E(\mathfrak{a}_{m,\bar{i}}), \alpha_{l^\infty}(\mathfrak{a}_{m,\bar{i}})_i) := a_{m,i}(E(c\mathfrak{o}_n), \alpha_{l^\infty}(c\mathfrak{o}_n)) \tag{4.3.3}$$

for each $i \in \mathbb{Z}$. Thus $\mathfrak{a}_{m,\bar{i}}$ has $\{cl^n w, cl^{-m}(1 + iMl^n w)\}$ as its $\mathbb{Z}$-basis, and $\alpha_{l^\infty}(\mathfrak{a}_{m,\bar{i}})_i$ is the $\Gamma(l^\infty)^{\mathrm{naive}}$-structure given by this basis.

Lemma (4.3.4). *Let $e_{n,i} \in \mathfrak{o}_{n,l}^\times$ be as in (4.1.8). Then we have*

$$\mathfrak{a}_{m,\bar{i}} = l^{-m} e_{n,i}(c\mathfrak{o}_{n+m}) \quad \textit{for all } i \in \mathbb{Z}.$$

Proof. We need to show that $(\mathfrak{a}_{m,\bar{i}})_q = (l^{-m} e_{n,i}(c\mathfrak{o}_{n+m}))_q$ for all prime numbers q, the subscript "$_q$" meaning, as before, the q-adic completion. For $q \neq l$, the both sides are equal to $c\mathfrak{o}_q$, while the l-adic completions agree by (4.1.9), (1). □

It follows that, since $\mathrm{Ker}(I_{n+m} \to I_n) \cong \mathfrak{o}_{n,l}^\times/\mathfrak{o}_{n+m,l}^\times$ (cf. 4.1), $\mathfrak{a}_{m,\bar{i}}$ for $\bar{i} \in \mathbb{Z}/l^m\mathbb{Z}$ constitute all proper $\mathfrak{o}_{n+m}$-ideals projecting to $l^{-m}c\mathfrak{o}_n \in I_n$ by (4.1.9). Then when c moves over the fixed representatives of $K^\times/\{\pm 1\}$, the ideals $\mathfrak{a}_{m,\bar{i}}$ range over all proper $\mathfrak{o}_{n+m}$-ideals belonging to $\mathrm{Ker}(\mathrm{Cl}_{n+m} \to \mathrm{Cl}_n)$. We have defined on each elliptic curve $E(\mathfrak{a}_{m,\bar{i}})$ the $\Gamma(l^\infty)^{\mathrm{naive}}$-structures $\alpha_{l^\infty}(\mathfrak{a}_{m,\bar{i}})_i$ for $i \in \bar{i}$. (If $i' = i + al^m \in \bar{i}$, we have $\alpha_{l^\infty}(\mathfrak{a}_{m,\bar{i}})_i = \alpha_{l^\infty}(\mathfrak{a}_{m,\bar{i}})_{i'} \circ \begin{pmatrix} 1 & -aM \\ 0 & 1 \end{pmatrix}$.) All these $\Gamma(l^\infty)^{\mathrm{naive}}$-structures have the same determinant $(e^{2\pi i/l^u})_{u \geq 1}$, and we may identify them with $\Gamma(l^\infty)^{\mathrm{arith}}$-structures, denoted $\beta_{l^\infty}(\mathfrak{a}_{m,\bar{i}})_i$, via the basis $(e^{2\pi i/l^u})_{u \geq 1}$ of $\mathbb{Z}_l(1)$. Similarly $\beta_{l^\infty}(c\mathfrak{o}_n)$ on $E(c\mathfrak{o}_n)$ corresponds to $\alpha_{l^\infty}(c\mathfrak{o}_n)$. Therefore, when c or $\mathfrak{a}_{m,\bar{i}}$ is prime to M, we can consider the $\Gamma_{l^\infty M,T}$-test objects

$$\begin{cases} X_{\infty,l^\infty M,T}(c\mathfrak{o}_n) := (E(c\mathfrak{o}_n), \omega_\infty(c\mathfrak{o}_n), \beta_{l^\infty}(c\mathfrak{o}_n), \beta_M(c\mathfrak{o}_n), C_T(c\mathfrak{o}_n)), \\ X_{\infty,l^\infty M,T}(\mathfrak{a}_{m,\bar{i}})_i := (E(\mathfrak{a}_{m,\bar{i}}), \omega_\infty(\mathfrak{a}_{m,\bar{i}}), \beta_{l^\infty}(\mathfrak{a}_{m,\bar{i}})_i, \beta_M(\mathfrak{a}_{m,\bar{i}}), C_T(\mathfrak{a}_{m,\bar{i}})). \end{cases} \tag{4.3.5}$$

In Section 7, we will need the following rather technical result: Fix, aside from n and m, an integer r such that $0 \le r \le m$, and set

$$\begin{cases} i := jl^{m-r} + k, \\ i' := (j+d)l^{m-r} + k \end{cases}$$

with integers j, d and k.

Lemma (4.3.6). *Assume that $r \le n$. Then we have*

$$e_{n+m-r,d}\mathfrak{a}_{m,\bar{i}} = \mathfrak{a}_{m,\bar{i'}}.$$

When $\mathfrak{a}_{m,\bar{i}}$ is prime to M, we have

$$B_{r,d}X_{\infty,l^\infty M,T}(\mathfrak{a}_{m,\bar{i}})_i = X_{\infty,l^\infty M,T}(\mathfrak{a}_{m,\bar{i'}})_{i'}.$$

Proof. For the first assertion, in view of (4.3.4), we need to show that $e_{n+m-r,d}e_{n,i} \equiv e_{n,i'} \bmod \mathfrak{o}_{n+m,l}^\times$. But a simple computation shows that $e_{n+m-r,d}e_{n,i} = e_{n,i'} + l^{2n+m-r}C$ with $C \in \mathfrak{o}_l$. Since $2n+m-r \ge n+m$, our claim follows.

As for the second, if $c\mathfrak{o}_n$ and $\mathfrak{a}_{m,\bar{i}}$ are related as before, we see, as in the proof of (4.3.1), that $a_{m,i}X_{\infty,l^\infty M,T}(c\mathfrak{o}_n)$ is equal to $X_{\infty,l^\infty M,T}(\mathfrak{a}_{m,\bar{i}})_i$ with the differential $\omega_\infty(\mathfrak{a}_{m,\bar{i}})$ multiplied by l^m, and similarly for $a_{m,i'}X_{\infty,l^\infty M,T}(c\mathfrak{o}_n)$. The conclusion follows from the identity $B_{r,d}a_{m,i} = a_{m,i'}$. □

5. Eisenstein series and their special values.

5.1. Eisenstein series.

We first recall Katz's description [**Ka2**, Chapter III] of the Eisenstein series on $\Gamma(M)^{\mathrm{arith}}$.

Recall that lattices in $\mathbb{C}$ correspond bijectively with (isomorphism classes of) pairs consisting of an elliptic curve and a nowhere-vanishing invariant differential over $\mathbb{C}$ (cf. 2.2). In the following, we let the symbols L and (E,ω) correspond in this sense.

In general, for a function $f : \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z} \to \mathbb{C}$, we define

$$P^{-1}f : \boldsymbol{\mu}_M \times \mathbb{Z}/M\mathbb{Z} \to \mathbb{C} \tag{5.1.1}$$
$$\text{by } (P^{-1}f)(\zeta,m) := \frac{1}{M}\sum_{a \bmod M} f(a,m)\zeta^{-a}$$

(the "inverse partial Fourier transform" of f, [**Ka2**, 3.2.2, 3.6.1]).

Define, for any function $h : (1/M)L/L = E[M] \to \mathbb{C}$, the k-th Epstein zeta function ζ_k and its variant φ_k for $k \in \mathbb{Z}$ by

$$\begin{cases} \zeta_k(s;L,h) = \zeta_k(s;E,\omega,h) := \displaystyle\sum_{\ell\in L}{}' \frac{h(\ell/M)}{(\ell/M)^k|\ell/M|^{2s-k}}, \\ \varphi_k(s;L,h) = \varphi_k(s;E,\omega,h) := \Gamma\left(s+\dfrac{k}{2}\right)\left(\dfrac{a(L)}{M\pi}\right)^{s-k/2}\zeta_k(s;L,h) \end{cases} \tag{5.1.2}$$

where the sum "$\sum'$" is over $\ell \neq 0$ and $a(L)$ is defined by (2.2.3). These functions converge for $\mathrm{Re}(s) > 1$, and extend to entire functions of s on $\mathbb{C}$ when $k > 0$.

Now if $\beta_M : \boldsymbol{\mu}_M \times \mathbb{Z}/M\mathbb{Z} \xrightarrow{\sim} E[M]$ is a $\Gamma(M)^{\mathrm{arith}}$-structure on E, we can consider the $\mathbb{C}$-valued function $P^{-1}f \circ \beta_M^{-1}$ on $E[M]$ for any $f : \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z} \to \mathbb{C}$. Set

$$\begin{aligned} G_{k,s,f}(E,\omega,\beta_M) &:= \frac{(-1)^k}{2}\varphi_k\left(s+\frac{k}{2}; E, \omega, P^{-1}f \circ \beta_M^{-1}\right) \\ &= \frac{(-1)^k}{2}\Gamma(s+k)\left(\frac{a(L)}{M\pi}\right)^s \sum_{\ell \in L}{}' \frac{P^{-1}f \circ \beta_M^{-1}(\ell/M)}{(\ell/M)^k |\ell/M|^{2s}}. \end{aligned} \tag{5.1.3}$$

It converges for $\mathrm{Re}(s) > 1 - k/2$, and extends to an entire function of s if $k > 0$.

Theorem (5.1.4) ([**Ka2**, Theorem 3.6.9]). *Let f be a complex valued function on $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$, and denote by $\mathbb{Q}[f]$ the subring of $\mathbb{C}$ generated by the values of f over $\mathbb{Q}$. Let k be a positive integer, and assume that, when $k = 2$, $\sum_j f(j,0) = \sum_j f(0,j) = 0$. Then $G_{k,0,f} := G_{k,s,f}|_{s=0}$ belongs to $R^k(\mathbb{Q}[f], \Gamma(M)^{\mathrm{arith}})$.*

When $k \geq 2$, its q-expansion $G_{k,0,f}(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{M,\mathrm{can}})$ is given by:

$$\begin{cases} 0 \qquad \text{if } f(-a,-b) = (-1)^{k-1}f(a,b), \\ \dfrac{1}{2}L(1-k, f(n,0)) + \displaystyle\sum_{n \geq 1}\left(\sum_{\substack{n=dd' \\ d,d' \geq 1}} d^{k-1} f(d,d')\right) q^{n/M} \\ \qquad \text{if } f(-a,-b) = (-1)^k f(a,b). \end{cases}$$

Here, $L(s, f(n,0))$ is the L-function continuing $\sum_{n \geq 1} f(n,0)/n^s$ $(\mathrm{Re}(s) > 1)$ analytically. (Katz also computed the q-expansion when $k = 1$, but we will not need it.) □

We next specialize the above general result to the following situation: Let χ_1 and χ_2 be primitive Dirichlet characters defined modulo M and M', respectively, and assume that M' is a divisor of M. As usual, we consider χ_1 and χ_2 as functions on $\mathbb{Z}/M\mathbb{Z}$, and $\mathbb{Z}/M'\mathbb{Z}$, respectively, and also consider χ_2 as a function on $\mathbb{Z}/M\mathbb{Z}$ through the projection to $\mathbb{Z}/M'\mathbb{Z}$. We set

$$f_{\chi_1,\chi_2}(a,b) := \chi_1(a)\chi_2(b). \tag{5.1.5}$$

In general, if χ is a Dirichlet character modulo M and ζ is an M-th root of unity, we define the Gauss sum by

$$g(\zeta,\chi) := \sum_{a \bmod M} \chi(a)\zeta^{-a}. \tag{5.1.6}$$

It follows from the definition (5.1.1) that

$$P^{-1}f_{\chi_1,\chi_2}(\zeta,b) = \frac{1}{M}\chi_2(b)g(\zeta,\chi_1). \tag{5.1.7}$$

On the other hand, let α_M be a $\Gamma(M)^{\mathrm{naive}}$-structure on E, and let β_{α_M} be the

$\Gamma(M)^{\mathrm{arith}}$-structure associated with it, (1.1.4). Let ζ_{α_M} be the determinant of α_M, and write $\alpha_M^{-1}(\ell/M) = (a_\ell, b_\ell)$ for an element $\ell/M \in (1/M)L/L = E[M]$. We then have

$$(P^{-1} f_{\chi_1,\chi_2}) \circ \beta_{\alpha_M}^{-1}(\ell/M) = \frac{1}{M}\overline{\chi}_1(a_\ell)\chi_2(b_\ell) g(\zeta_{\alpha_M}, \chi_1). \tag{5.1.8}$$

Corollary (5.1.9). *Let the notation be as above. We assume that $k \geq 2$, and $\chi_1(-1)\chi_2(-1) = (-1)^k$. When $k = 2$, we also assume that $M > 1$. Then $G_{k,0,f_{\chi_1,\chi_2}}$ belongs to $R^k(\mathbb{Q}[\chi_1,\chi_2], \Gamma(M)^{\mathrm{arith}})$ and we have*

$$G_{k,0,f_{\chi_1,\chi_2}}(E,\omega,\beta_{\alpha_M}) = \frac{(-1)^k}{2} M^{k-1}(k-1)! g(\zeta_{\alpha_M},\chi_1) \sum_{\ell\in L}{}' \left.\frac{\overline{\chi}_1(a_\ell)\chi_2(b_\ell)}{\ell^k |\ell|^{2s}}\right|_{s=0}.$$

It has the following q-expansion

$$\begin{aligned} &G_{k,0,f_{\chi_1,\chi_2}}(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{M,\mathrm{can}}) \\ &\quad = \begin{Bmatrix} \frac{1}{2}L(1-k,\chi_1) & \text{when } \chi_2 = 1 \\ 0 & \text{when } \chi_2 \neq 1 \end{Bmatrix} + \sum_{n\geq 1}\left(\sum_{\substack{n=dd'\\ d,d'\geq 1}} \chi_1(d)\chi_2(d') d^{k-1}\right) q^{n/M}. \quad \square \end{aligned}$$

We note that the sum "$\sum'_{\ell\in L}$" in the above corollary converges for $\mathrm{Re}(s) > -1/2$ when $k \geq 3$. Hence that term is simply the (convergent) sum $\sum'_{\ell\in L} \overline{\chi}_1(a_\ell)\chi_2(b_\ell)/\ell^k$ in this case.

Finally, with the notation (3.1.1), it follows from (5.1.7) that

$$(P^{-1} f_{\chi_1,\chi_2}) \circ h_a^{-1}(\zeta, b) = P^{-1} f_{\chi_1,\chi_2}(\zeta^{a^{-1}}, ab) = \frac{1}{M}\chi_1(a)\chi_2(ab) g(\zeta,\chi_1).$$

Therefore $G_{k,0,f_{\chi_1,\chi_2}}$ has the character $\chi_1\chi_2$ in the sense of 3.1:

$$G_{k,0,f_{\chi_1,\chi_2}} \mid h_a = \chi_1(a)\chi_2(a) G_{k,0,f_{\chi_1,\chi_2}} \quad \text{for all } a \in (\mathbb{Z}/M\mathbb{Z})^\times. \tag{5.1.10}$$

5.2. Eisenstein series $G_{k,\lambda}$ attached to a Hecke character.

We let K be an imaginary quadratic field, and use the same terminology as in 4.1 for K. We start with a Hecke (quasi-)character

$$\lambda : K_{\mathbb{A}}^\times / K^\times \to \mathbb{C}^\times \ \text{ such that } \lambda(a) = a^k \text{ for all } a \in K_\infty^\times = \mathbb{C}^\times \tag{5.2.1}$$

for an integer k. We denote by $\mathfrak{c}$ the conductor of λ, and set $K_{\mathbb{A},0}^\times(\mathfrak{c}) := \{x = (x_v) \in K_{\mathbb{A},0}^\times \mid x_v \equiv 1 \bmod \mathfrak{c}\mathfrak{o}_v \text{ for all } v \mid \mathfrak{c}\}$. Then we have an isomorphism

$$K_{\mathbb{A},0}^\times(\mathfrak{c}) / K_{\mathbb{A},0}^\times(\mathfrak{c}) \cap \widehat{\mathfrak{o}}^\times \xrightarrow{\sim} I(\mathfrak{c}) := (\text{fractional } \mathfrak{o}\text{-ideals prime to } \mathfrak{c}) \tag{5.2.2}$$

by $a \mapsto a\mathfrak{o}$ in the sense of 4.1. The restriction of λ to $K_{\mathbb{A},0}^\times(\mathfrak{c})$ therefore induces a (quasi-)character of $I(\mathfrak{c})$, the ideal character associated with λ, which we hereafter denote by λ^{id}. Thus if $\mathfrak{a} = (a)$ is a principal ideal with $a \in K_{\mathbb{A},0}^\times(\mathfrak{c}) \cap K^\times$, we have $\lambda^{\mathrm{id}}(\mathfrak{a}) = a^{-k}$. Moreover, λ^{id} also induces a character of $K_{\mathbb{A},0}^\times(\mathfrak{c})/K_{\mathbb{A},0}^\times(\mathfrak{c}) \cap \widehat{\mathfrak{o}}_n^\times$ ($\hookrightarrow K_{\mathbb{A},0}^\times/\widehat{\mathfrak{o}}_n^\times \cong I_n$;

cf. (4.1.3)). Therefore for any proper $\mathfrak{o}_n$-ideal $\mathfrak{a} = a\mathfrak{o}_n$ with $a \in K^{\times}_{\mathbb{A},0}(\mathfrak{c})$, we can define $\lambda^{\mathrm{id}}(\mathfrak{a}) := \lambda(a)$. In other words, this left hand side is defined as $\lambda^{\mathrm{id}}(\mathfrak{a}\mathfrak{o})$ with the above terminology.

From now on, we make the following:

Assumption (5.2.3). • $k \geq 2$, and when $k = 2$ we assume that $\mathfrak{c} \neq (1)$;
• $(l, \mathfrak{c}) = (1)$;
• $\mathfrak{c}$ is a product of primes that split in $K/\mathbb{Q}$.

We fix a decomposition $\mathfrak{c} = \mathfrak{f}\mathfrak{f}'$ as a product of integral ideals such that

$$(\mathfrak{f}, \bar{\mathfrak{f}}) = (1), \ \text{ and } \ \mathfrak{f}' \,|\, \bar{\mathfrak{f}} \tag{5.2.4}$$

and set

$$M := N(\mathfrak{f}), \ \text{ and } \ M' := N(\mathfrak{f}') \ \ (\text{so that } M' \,|\, M). \tag{5.2.5}$$

Writing $\mathfrak{o}_{\mathfrak{f}}$ and $\mathfrak{o}_{\mathfrak{f}'}$ the $\mathfrak{f}$-adic and $\mathfrak{f}'$-adic completions of $\mathfrak{o}$, respectively, we have characters

$$\begin{cases} \lambda_{\mathfrak{f}} := \lambda|_{\mathfrak{o}_{\mathfrak{f}}^{\times}} : \mathfrak{o}_{\mathfrak{f}}^{\times} \to (\mathfrak{o}_{\mathfrak{f}}/\mathfrak{f})^{\times} \to \overline{\mathbb{Q}}^{\times}, \\ \lambda_{\mathfrak{f}'} := \lambda|_{\mathfrak{o}_{\mathfrak{f}'}^{\times}} : \mathfrak{o}_{\mathfrak{f}'}^{\times} \to (\mathfrak{o}_{\mathfrak{f}'}/\mathfrak{f}')^{\times} \to \overline{\mathbb{Q}}^{\times}. \end{cases} \tag{5.2.6}$$

Definition (5.2.7). Via the canonical isomorphisms $\mathfrak{o}_{\mathfrak{f}}/\mathfrak{f} \cong \mathbb{Z}/M\mathbb{Z}$ and $\mathfrak{o}_{\mathfrak{f}'}/\mathfrak{f}' \cong \mathbb{Z}/M'\mathbb{Z}$, we let $\chi_{\mathfrak{f}}$ and $\chi_{\mathfrak{f}'}$ be the Dirichlet characters defined modulo M and M' corresponding to $\lambda_{\mathfrak{f}}$ and $\lambda_{\mathfrak{f}'}$, respectively. Letting

$$f(a,b) := \chi_{\mathfrak{f}}(a)\overline{\chi}_{\mathfrak{f}'}(b) \ \text{ for } \ a, b \in \mathbb{Z}/M\mathbb{Z}$$

we define

$$G_{k,\lambda} := G_{k,0,f} \in R^k(\mathbb{Q}[\chi_{\mathfrak{f}}, \chi_{\mathfrak{f}'}], \Gamma(M)^{\mathrm{arith}}).$$

(Though the subscript "$_k$" in $G_{k,\lambda}$ is superfluous, we keep it to emphasis the infinity type of λ and the weight of this Eisenstein series.)

Since $\chi_{\mathfrak{f}}(-1)\chi_{\mathfrak{f}'}(-1) = (-1)^k$, and $M > 1$ when $k = 2$, $G_{k,\lambda}$ is in fact non-zero, and its q-expansion is explicitly given by (5.1.9).

We next consider the special value of this Eisenstein series at CM test objects. To do this, for a proper $\mathfrak{o}_n$-ideal class $\{\mathfrak{a}\}_n \in \mathrm{Cl}_n$, we consider the (partial) L-functions of orders studied by Hida [**H3**, 8.1.5, 8.1.7] and Yoshida [**Y**, Chapter V, Section 3]

$$L^n_{\{\mathfrak{a}\}_n}(s, \lambda) := \sum_{\mathfrak{b}} \lambda^{\mathrm{id}}(\mathfrak{b})N(\mathfrak{b})^{-s} \tag{5.2.8}$$

where the sum ranges over all integral proper $\mathfrak{o}_n$-ideals $\mathfrak{b} \in \{\mathfrak{a}\}_n$ prime to $\mathfrak{c}$ (equivalently, $\mathfrak{b}$ is of the form $b\mathfrak{o}_n$ with $b \in K^{\times}_{\mathbb{A},0}(\mathfrak{c})$). This function converges for $\mathrm{Re}(s) > 1 - k/2$, extends to a meromorphic function on $\mathbb{C}$, and holomorphic at $s = 0$ even when $k = 2$; cf. the proof of the following proposition.

Proposition (5.2.9). *Let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$-ideal prime to M, and consider the $\Gamma(M)^{\mathrm{arith}} = \Gamma_{M,1}$-test object*

$$X_{\infty,M,1}(\mathfrak{a}) = (E(\mathfrak{a}), \omega_\infty(\mathfrak{a}), \beta_M(\mathfrak{a}))$$

cf. (4.2.7). *Then we have*

$$G_{k,\lambda}(X_{\infty,M,1}(\mathfrak{a})) = |\,\mathfrak{o}_n^\times\,| \frac{(-1)^k}{2} M^{k-1}(k-1)!g(\zeta_\mathfrak{a}, \chi_\mathfrak{f})\lambda^{\mathrm{id}}(\mathfrak{a})L^n_{\{\mathfrak{a}^{-1}\}_n}(0,\lambda).$$

Here and henceforth, we set

$$\zeta_\mathfrak{a} := \det(\alpha_M(\mathfrak{a})).$$

Proof. With the same terminology as in (5.1.9), we need to show that

$$\sum_{\ell\in\mathfrak{a}}{}' \left.\frac{\overline{\chi}_\mathfrak{f}(a_\ell)\overline{\chi}_{\mathfrak{f}'}(b_\ell)}{\ell^k|\ell|^{2s}}\right|_{s=0} = |\,\mathfrak{o}_n^\times\,|\,\lambda^{\mathrm{id}}(\mathfrak{a})L^n_{\{\mathfrak{a}^{-1}\}_n}(0,\lambda).$$

By the definition of (4.2.3), we have $\alpha_M(\mathfrak{a})^{-1}(\ell/M) = (\ell \bmod \mathfrak{f}, \ell \bmod \overline{\mathfrak{f}})$, and hence $\overline{\chi}_\mathfrak{f}(a_\ell)\overline{\chi}_{\mathfrak{f}'}(b_\ell)$ is equal to $\overline{\lambda}_\mathfrak{f}(\ell)\overline{\lambda}_{\mathfrak{f}'}(\ell)$ if $\ell \in \mathfrak{o}_\mathfrak{f}^\times$ and $\ell \in \mathfrak{o}_{\mathfrak{f}'}^\times$, and 0 otherwise. Therefore letting $\mathfrak{o}_\mathfrak{c} := \mathfrak{o}_\mathfrak{f} \times \mathfrak{o}_{\mathfrak{f}'}$ and $\lambda_\mathfrak{c} := \lambda_\mathfrak{f} \times \lambda_{\mathfrak{f}'}$, the left hand side is equal to

$$\sum_{\ell\in\mathfrak{a},\ \ell\in\mathfrak{o}_\mathfrak{c}^\times} \left.\frac{\lambda_\mathfrak{c}(\ell)^{-1}}{\ell^k|\ell|^{2s}}\right|_{s=0} = \sum_{\ell\in\mathfrak{a},\ \ell\in\mathfrak{o}_\mathfrak{c}^\times} \left.\frac{\lambda^{\mathrm{id}}((\ell))}{|\ell|^{2s}}\right|_{s=0}$$

since $\lambda(\ell) = 1 = \ell^k\lambda^{\mathrm{id}}((\ell))\lambda_\mathfrak{c}(\ell)$. Here, $\ell \in \mathfrak{a}$ if and only if $\ell\mathfrak{a}^{-1} =: \mathfrak{b}$ is an integral proper $\mathfrak{o}_n$-ideal, and in this case, $\ell \in \mathfrak{o}_\mathfrak{c}^\times$ if and only if $\mathfrak{b}$ is prime to $\mathfrak{c}$. Thus this sum is equal to the one over such $\mathfrak{b}$ each with multiplicity $|\,\mathfrak{o}_n^\times\,|$:

$$|\,\mathfrak{o}_n^\times\,| \sum_\mathfrak{b} \left.\frac{\lambda^{\mathrm{id}}(\mathfrak{a})\lambda^{\mathrm{id}}(\mathfrak{b})}{N(\mathfrak{a})^s N(\mathfrak{b})^s}\right|_{s=0} = |\,\mathfrak{o}_n^\times\,|\ \lambda^{\mathrm{id}}(\mathfrak{a})\sum_\mathfrak{b} \left.\frac{\lambda^{\mathrm{id}}(\mathfrak{b})}{N(\mathfrak{b})^s}\right|_{s=0}. \qquad \square$$

5.3. Modified Eisenstein series $\mathbb{G}_{k,\lambda}$ and its special values.

We keep the notation in 5.1 and 5.2.

Definition (5.3.1). We set

$$\mathbb{G}_{k,\lambda} := G_{k,\lambda} - \overline{\chi}_{\mathfrak{f}'}(l)G_{k,\lambda}\,|\,[l] \in R^k(\mathbb{Q}[\chi_\mathfrak{f}, \chi_{\mathfrak{f}'}], \Gamma_{M,l})$$

where $[l]$ is the degeneracy operator; cf. 3.2.

Proposition (5.3.2). *The q-expansion $\mathbb{G}_{k,\lambda}(\mathrm{Tate}(q), \omega_{\mathrm{can}}, \beta_{M,\mathrm{can}}, C_{l,\mathrm{can}})$ is given by*

$$\sum_{n=1}^\infty \left(\sum_{\substack{n=dd'\\ l\nmid d'}} \chi_\mathfrak{f}(d)\overline{\chi}_{\mathfrak{f}'}(d')d^{k-1}\right)q^{n/M}$$

and $\mathbb{G}_{k,\lambda}$ belongs to $R^k(\mathbb{Z}[\chi_{\mathfrak{f}}, \chi_{\mathfrak{f}'}], \Gamma_{M,l})$.

Proof. The q-expansion of $G_{k,\lambda}$ is given by (5.1.9) with $\chi_1 = \chi_{\mathfrak{f}}$ and $\chi_2 = \overline{\chi}_{\mathfrak{f}'}$, and the q-expansion of $G_{k,\lambda} \,|\, [l]$ is obtained from this by the change of variable $q^{1/M} \mapsto q^{l/M}$ by (3.2.2). The first assertion then follows from a simple calculation. The second assertion follows from this by the q-expansion principle. □

Corollary (5.3.3). *$\mathbb{G}_{k,\lambda}$ is an eigenform of the Hecke operator $U(l)$:*

$$\mathbb{G}_{k,\lambda} \,|\, U(l) = \chi_{\mathfrak{f}}(l) l^{k-1} \mathbb{G}_{k,\lambda}.$$

Proof. This follows from (3.4.3) and the above proposition by comparing the q-expansions of both sides. □

We next consider the special values of $\mathbb{G}_{k,\lambda}$.

Proposition (5.3.4). *Let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$-ideal prime to M with $n \geq 2$, and let*

$$X_{\infty,M,l}(\mathfrak{a}) = (E(\mathfrak{a}), \omega_\infty(\mathfrak{a}), \beta_M(\mathfrak{a}), C_l(\mathfrak{a}))$$

be the $\Gamma_{M,l}$-test object as in (4.2.7). Then we have

$$\begin{aligned} &\mathbb{G}_{k,\lambda}(X_{\infty,M,l}(\mathfrak{a})) \\ &\quad = (-1)^k M^{k-1}(k-1)! g(\zeta_{\mathfrak{a}}, \chi_{\mathfrak{f}}) \lambda^{\mathrm{id}}(\mathfrak{a}) \left(L^n_{\{\mathfrak{a}^{-1}\}_n}(0,\lambda) - \lambda^{\mathrm{id}}((l)) L^{n-1}_{\{\mathfrak{a}^{-1}\mathfrak{o}_{n-1}\}_{n-1}}(0,\lambda) \right). \end{aligned}$$

Proof. The left hand side is equal to $G_{k,\lambda}(X_{\infty,M,l}(\mathfrak{a})) - \overline{\chi}_{\mathfrak{f}'}(l) G_{k,\lambda}([l]X_{\infty,M,l}(\mathfrak{a}))$. The first term is equal to $G_{k,\lambda}(X_{\infty,M,1}(\mathfrak{a}))$ since $G_{k,\lambda}$ is of level M, and it is given by (5.2.9). The second term is equal to $\overline{\chi}_{\mathfrak{f}'}(l) l^{-k} G_{k,\lambda}(X_{\infty,M,1}(\mathfrak{a}\mathfrak{o}_{n-1}))$ by (4.3.1), i), and this is also described by (5.2.9). Since $\lambda^{\mathrm{id}}(\mathfrak{a}\mathfrak{o}_{n-1}) = \lambda^{\mathrm{id}}(\mathfrak{a})$ and $|\,\mathfrak{o}_{n-1}^\times\,| = |\,\mathfrak{o}_n^\times\,| = 2$, our conclusion is equivalent to

$$\overline{\chi}_{\mathfrak{f}'}(l) l^{-k} g(\zeta_{\mathfrak{a}\mathfrak{o}_{n-1}}, \chi_{\mathfrak{f}}) = \lambda^{\mathrm{id}}((l)) g(\zeta_{\mathfrak{a}}, \chi_{\mathfrak{f}}).$$

But it follows from (4.2.8) that $\zeta_{\mathfrak{a}\mathfrak{o}_{n-1}} = \zeta_{\mathfrak{a}}^l$, and hence $g(\zeta_{\mathfrak{a}\mathfrak{o}_{n-1}}, \chi_{\mathfrak{f}}) = \overline{\chi}_{\mathfrak{f}}(l) g(\zeta_{\mathfrak{a}}, \chi_{\mathfrak{f}})$. Since $\overline{\chi}_{\mathfrak{f}'}(l) l^{-k} \overline{\chi}_{\mathfrak{f}}(l) = l^{-k} \lambda_{\mathfrak{c}}(l)^{-1} = \lambda^{\mathrm{id}}((l))$, our conclusion follows. □

Definition and Proposition (5.3.5). *For a proper $\mathfrak{o}_n$-ideal $\mathfrak{a}$ prime to M with $n \geq 2$, we set*

$$\mathbb{G}_{k,\lambda}(\{\mathfrak{a}\}_n)_\infty := \lambda^{\mathrm{id}}(\mathfrak{a})^{-1} \chi_{\mathfrak{f}}(N(\mathfrak{a})^{-1}) \mathbb{G}_{k,\lambda}(X_{\infty,M,l}(\mathfrak{a})).$$

This value depends only on the class $\{\mathfrak{a}\}_n \in \mathrm{Cl}_n$, and we have

$$\mathbb{G}_{k,\lambda}(\{\mathfrak{a}\}_n)_\infty = C(\lambda) \chi_{\mathfrak{f}}(l^n) \left(L^n_{\{\mathfrak{a}^{-1}\}_n}(0,\lambda) - \lambda^{\mathrm{id}}((l)) L^{n-1}_{\{\mathfrak{a}^{-1}\mathfrak{o}_{n-1}\}_{n-1}}(0,\lambda) \right).$$

Here $C(\lambda)$ is a constant depending only on λ and the decomposition $\mathfrak{c} = \mathfrak{f}\mathfrak{f}'$ defined by

$$C(\lambda) := (-1)^k M^{k-1}(k-1)! g(\zeta_{\mathfrak{o}}, \chi_{\mathfrak{f}}).$$

Proof. Let $\alpha \in K^\times$ be prime to M. Then by (5.3.4), we have

$$\mathbb{G}_{k,\lambda}(\{\alpha\mathfrak{a}\}_n)_\infty = \mathbb{G}_{k,\lambda}(\{\mathfrak{a}\}_n)_\infty \times \frac{\lambda^{\mathrm{id}}(\mathfrak{a})\chi_{\mathfrak{f}}(N(\mathfrak{a}))}{\lambda^{\mathrm{id}}(\alpha\mathfrak{a})\chi_{\mathfrak{f}}(N(\alpha\mathfrak{a}))} \frac{g(\zeta_{\alpha\mathfrak{a}}, \chi_{\mathfrak{f}})\lambda^{\mathrm{id}}(\alpha\mathfrak{a})}{g(\zeta_{\mathfrak{a}}, \chi_{\mathfrak{f}})\lambda^{\mathrm{id}}(\mathfrak{a})}.$$

But by (4.2.8), we have

$$\begin{cases} g(\zeta_{\mathfrak{a}}, \chi_{\mathfrak{f}}) = \chi_{\mathfrak{f}}(l^n N(\mathfrak{a}))g(\zeta_{\mathfrak{o}}, \chi_{\mathfrak{f}}), \\ g(\zeta_{\alpha\mathfrak{a}}, \chi_{\mathfrak{f}}) = \chi_{\mathfrak{f}}(l^n N(\alpha\mathfrak{a}))g(\zeta_{\mathfrak{o}}, \chi_{\mathfrak{f}}). \end{cases}$$

Thus the value $\mathbb{G}_{k,\lambda}(\{\mathfrak{a}\}_n)_\infty$ indeed depends only on $\{\mathfrak{a}\}_n$. The remaining assertion is also clear from the above discussion. □

Slightly more generally, we have

Corollary (5.3.6). *Let $\mathfrak{s}$ be a divisor of $\mathfrak{t}_1 \cdots \mathfrak{t}_t$ (cf. (4.2.1)) and set $S = N(\mathfrak{s})$. Let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$-ideal prime to M with $n \geq 2$. Then*

$$(\mathbb{G}_{k,\lambda} \mid [S])(\{\mathfrak{a}\}_n)_\infty := \lambda^{\mathrm{id}}(\mathfrak{a})^{-1}\chi_{\mathfrak{f}}(N(\mathfrak{a})^{-1})(\mathbb{G}_{k,\lambda} \mid [S])(X_{\infty,M,lS}(\mathfrak{a}))$$

depends only on the class $\{\mathfrak{a}\}_n \in \mathrm{Cl}_n$.

Proof. By (4.3.1), ii), we in fact have that the above value is equal to

$$S^{-k}\mathbb{G}_{k,\lambda}(\{\mathfrak{s}_n^{-1}\mathfrak{a}\}_n)_\infty \times \lambda^{\mathrm{id}}(\mathfrak{s})^{-1}\chi_{\mathfrak{f}}(S)^{-1}.$$ □

Proposition (5.3.7). *Let $\varepsilon : \mathrm{Cl}_f \to \overline{\mathbb{Q}}^\times$ be a character for some $f \geq 0$. For $n \geq \max\{f, 1\} + 1$, we have*

$$\sum_{\{\mathfrak{a}\}_n \in \mathrm{Cl}_n} \varepsilon(\mathfrak{a})\mathbb{G}_{k,\lambda}(\{\mathfrak{a}\}_n)_\infty = C(\lambda)\chi_{\mathfrak{f}}(l)^n L^{(l)}(0, \lambda\varepsilon^{-1}).$$

In the right hand side, we consider ε as a character of $K_{\mathbb{A}}^\times$ via (4.1.4), and $L^{(l)}(s, \lambda\varepsilon^{-1})$ is the Hecke L-function with the Euler factor at (the primes dividing) l removed.

Proof. By (5.3.5), the left hand side is the difference of

$$\begin{aligned} \text{(i)} &:= \sum_{\{\mathfrak{a}\} \in \mathrm{Cl}_n} \varepsilon(\mathfrak{a})L^n_{\{\mathfrak{a}^{-1}\}_n}(s, \lambda) \quad \text{and} \\ \text{(ii)} &:= \sum_{\{\mathfrak{a}\} \in \mathrm{Cl}_n} \varepsilon(\mathfrak{a})\lambda^{\mathrm{id}}((l))L^{n-1}_{\{\mathfrak{a}^{-1}\mathfrak{o}_{n-1}\}_{n-1}}(s, \lambda), \end{aligned}$$

multiplied by $C(\lambda)\chi_{\mathfrak{f}}(l)^n$ and evaluated at $s = 0$.

Since $n > f$, $\varepsilon(\mathfrak{b}) = \varepsilon(\mathfrak{a}^{-1})$ for $\mathfrak{b} \in \{\mathfrak{a}^{-1}\}_n$, and we have

$$\text{(i)} = \sum_{\mathfrak{b}} \lambda^{\mathrm{id}}(\mathfrak{b})\varepsilon^{-1}(\mathfrak{b})N(\mathfrak{b})^{-s} = \sum_{b} (\lambda\varepsilon^{-1})(b)\|b\|^s.$$

Here, the first sum is over all integral proper $\mathfrak{o}_n$-ideals $\mathfrak{b}$ prime to $\mathfrak{c}$, and the second is over $(K^\times_{\mathbb{A},0}(\mathfrak{c}) \cap \widehat{\mathfrak{o}}_n)/(K^\times_{\mathbb{A},0}(\mathfrak{c}) \cap \widehat{\mathfrak{o}}_n^\times)$. It has the Euler product

$$\text{(i)} = L^{(l)}(s, \lambda\varepsilon^{-1}) \times L_l^n(s, \lambda\varepsilon^{-1})$$

(cf. [**Y**, Chapter V, Section 3]), where

$$L_l^n(s, \lambda\varepsilon^{-1}) := \sum_{a \in (K_l^\times \cap \mathfrak{o}_{n,l})/\mathfrak{o}_{n,l}^\times} \lambda_l \varepsilon_l^{-1}(a) \|a\|_l^s$$

the subscript "$_l$" indicating the l-factor (i.e. the restriction to $(K \otimes_{\mathbb{Q}} \mathbb{Q}_l)^\times$). Similarly, we have

$$\text{(ii)} = l\lambda^{\mathrm{id}}((l))L^{(l)}(s, \lambda\varepsilon^{-1}) \times L_l^{n-1}(s, \lambda\varepsilon^{-1}).$$

Therefore, since $\lambda^{\mathrm{id}}((l)) = \lambda_l(l)$ and $\varepsilon_l(l) = 1$, our conclusion is equivalent to the equality

$$L_l^n(0, \lambda\varepsilon^{-1}) - l(\lambda_l\varepsilon_l^{-1})(l)L_l^{n-1}(0, \lambda\varepsilon^{-1}) = 1.$$

Since $n > f$, this follows from [**H3**, (8.1.29)] when $f > 0$; and from [**H3**, (8.1.28)] when $f = 0$. □

6. CM test objects over ring of integers, integrality of special values and the measure on Cl_∞.

6.1. CM test objects over $\mathcal{W}_0$.

Let the notation be as in 4.1 and 4.2. We are going to modify the CM test objects defined in 4.2, and consider them over some rings. For this, we fix a prime number p, and also an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$. We will always assume the following:

Assumption (6.1.1). • p is an odd prime not dividing lT,
• p splits completely in K; $(p) = \mathfrak{p}\overline{\mathfrak{p}}$,
• the prime of K induced by the above embedding is $\mathfrak{p}$.

We let

$$\begin{cases} \mathcal{K}_0 := \overline{\mathbb{Q}} \cap \text{(the maximal unramified subextension of } \overline{\mathbb{Q}}_p/\mathbb{Q}_p), \\ \mathcal{W}_0 := \mathcal{K}_0 \cap \text{(the ring of integers of } \overline{\mathbb{Q}}_p). \end{cases} \tag{6.1.2}$$

Thus $\mathcal{W}_0$ is the strict localization of $\mathbb{Z}_{(p)}$, the localization of $\mathbb{Z}$ at (p).

Let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$-ideal. Then it known that $E(\mathfrak{a})$ has a model $E(\mathfrak{a})_{/\mathcal{K}_0}$ defined over $\mathcal{K}_0$ which has good reduction, i.e. there is an elliptic curve $E(\mathfrak{a})_{/\mathcal{W}_0}$ over $\mathcal{W}_0$ whose generic fibre is $E(\mathfrak{a})_{/\mathcal{K}_0}$; cf. Serre and Tate [**ST**, Theorems 8 and 9]. The complex multiplication by $\mathfrak{o}_n$ on $E(\mathfrak{a})_{/\mathcal{K}_0}$ is also defined over $\mathcal{K}_0$, and, as usual, we normalize the embedding $\mathfrak{o}_n \hookrightarrow \mathrm{End}(E(\mathfrak{a})_{/\mathcal{K}_0})$ in such a way that the representation of $\mathfrak{o}_n$ on $\mathrm{Lie}(E(\mathfrak{a})_{/\mathcal{K}_0}) \cong \mathcal{K}_0$ is the inclusion. Since $\mathcal{W}_0$ is strictly local, all points of $E(\mathfrak{a})_{/\mathcal{K}_0}[m]$ are $\mathcal{K}_0$-rational, for any m prime to p. It follows that the above model $E(\mathfrak{a})_{/\mathcal{K}_0}$, and hence $E(\mathfrak{a})_{/\mathcal{W}_0}$ also, is unique. In the following, we will always consider these models over $\mathcal{K}_0$ and $\mathcal{W}_0$.

We have $\mathfrak{o}_{n,p} = \mathfrak{o}_p = \mathfrak{o}_\mathfrak{p} \oplus \mathfrak{o}_{\overline{\mathfrak{p}}}$ for the p-adic completion. Thus for any $\mathfrak{o}_n$-module X, $X_p = X \otimes_\mathbb{Z} \mathbb{Z}_p$ is the direct sum of $X_\mathfrak{p} := X_p \otimes_{\mathfrak{o}_{n,p}} \mathfrak{o}_\mathfrak{p}$ and $X_{\overline{\mathfrak{p}}} := X_p \otimes_{\mathfrak{o}_{n,p}} \mathfrak{o}_{\overline{\mathfrak{p}}}$. Similarly, the finite flat group scheme $E(\mathfrak{a})_{/\mathcal{W}_0}[p^m]$ on which $\mathfrak{o}_n/p^m\mathfrak{o}_n = \mathfrak{o}/p^m\mathfrak{o} = \mathfrak{o}/\mathfrak{p}^m \oplus \mathfrak{o}/\overline{\mathfrak{p}}^m$ acts, is the direct sum of $E(\mathfrak{a})_{/\mathcal{W}_0}[p^m]_\mathfrak{p}$ and $E(\mathfrak{a})_{/\mathcal{W}_0}[p^m]_{\overline{\mathfrak{p}}}$. $E(\mathfrak{a})_{/\mathcal{W}_0}[p^m]_\mathfrak{p}$ is a group scheme of μ-type over $\mathcal{W}_0$, while $E(\mathfrak{a})_{/\mathcal{W}_0}[p^m]_{\overline{\mathfrak{p}}}$ is constant.

DEFINITION (6.1.3). We henceforth take and fix a nowhere vanishing invariant differential $\omega(\mathfrak{o})$ on $E(\mathfrak{o})_{/\mathcal{W}_0}$. We define the complex number Ω_∞ by

$$\omega(\mathfrak{o}) = \Omega_\infty \omega_\infty(\mathfrak{o}),$$

and in general set

$$\omega(\mathfrak{a}) := \Omega_\infty \omega_\infty(\mathfrak{a}).$$

When $\mathfrak{a}$ and $\mathfrak{a}'$ are proper $\mathfrak{o}_n$-ideals such that $\mathfrak{a}' \supseteq \mathfrak{a}$, the natural (quotient) morphism $E(\mathfrak{a}) \to E(\mathfrak{a}')$ induces $E(\mathfrak{a})_{/\mathcal{K}_0} \to E(\mathfrak{a}')_{/\mathcal{K}_0}$ and $E(\mathfrak{a})_{/\mathcal{W}_0} \to E(\mathfrak{a}')_{/\mathcal{W}_0}$ over $\mathcal{K}_0$ and $\mathcal{W}_0$, respectively. When $\mathfrak{a}$ and $\mathfrak{a}'$ are prime to $\mathfrak{p}$ (i.e. $\mathfrak{a}_\mathfrak{p} = \mathfrak{a}'_\mathfrak{p} = \mathfrak{o}_\mathfrak{p}$), the latter morphism is étale. Arguing as in the proof of (4.2.8), it follows that the above defined $\omega(\mathfrak{a})$ is a nowhere vanishing differential on $E(\mathfrak{a})_{/\mathcal{W}_0}$ whenever $\mathfrak{a}$ is prime to $\mathfrak{p}$.

Recall that in 4.2, we started with the data (4.2.1), especially $M\mathfrak{o} = \mathfrak{f}\bar{\mathfrak{f}}$ with $(\mathfrak{f}, \bar{\mathfrak{f}}) = 1$, and used it to define $\alpha_M(\mathfrak{a})$ and $\beta_M(\mathfrak{a})$ etc. From now on we assume

ASSUMPTION (6.1.4). When M is divisible by p, $\mathfrak{p}$ divides $\mathfrak{f}$.

LEMMA (6.1.5). *Let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$-ideal prime to M, and assume* (6.1.4). *Then the $\Gamma(M)^{\mathrm{arith}}$-structure $\beta_M(\mathfrak{a})$ and the $\Gamma_0(lT)$-structure $C_{lT}(\mathfrak{a})$ on $E(\mathfrak{a})$ are defined over $\mathcal{K}_0$. Further, they extend uniquely to the same structures on $E(\mathfrak{a})_{/\mathcal{W}_0}$. Similarly, any $\Gamma(l^\infty)^{\mathrm{naive}}$-structure α_{l^∞} and $\Gamma(l^\infty)^{\mathrm{arith}}$-structure β_{l^∞} on $E(\mathfrak{a})$ are defined over $\mathcal{K}_0$, and extend uniquely to those over $\mathcal{W}_0$.*

PROOF. Write $M = p^c M_0$ with M_0 prime to p. Then we may consider $\beta_M(\mathfrak{a})$ as a pair $(\beta_{p^c}(\mathfrak{a}), \beta_{M_0}(\mathfrak{a}))$ consisting of $\Gamma(p^c)^{\mathrm{arith}}$- and $\Gamma(M_0)^{\mathrm{arith}}$-structures.

As for $\beta_{M_0}(\mathfrak{a})$, it is an isomorphism of $\boldsymbol{\mu}_{M_0} \times \mathbb{Z}/M_0\mathbb{Z}$ to $E(\mathfrak{a})[M_0]$ both of which are already constant groups over $\mathcal{K}_0$. Thus any such morphism is defined over $\mathcal{K}_0$. Also, since $\boldsymbol{\mu}_{M_0} \times \mathbb{Z}/M_0\mathbb{Z}$ and $E(\mathfrak{a})_{/\mathcal{W}_0}[M_0]$ are constant over $\mathcal{W}_0$, any morphism between them on the generic fibre uniquely extends to the one over $\mathcal{W}_0$. Similarly for α_{l^∞} and β_{l^∞}, and the assertion for $C_{lT}(\mathfrak{a})$ is also clear.

It thus remains to consider $\beta_{p^c}(\mathfrak{a}) : \boldsymbol{\mu}_{p^c} \times \mathbb{Z}/p^c\mathbb{Z} \xrightarrow{\sim} E(\mathfrak{a})[p^c]$. By our definition of $\beta_M(\mathfrak{a})$ in 4.2 and our assumption (6.1.4), this is in fact given by the product of

$$\begin{cases} \beta_{p^c}(\mathfrak{a})_\mu : \boldsymbol{\mu}_{p^c} \xrightarrow{\sim} E(\mathfrak{a})[p^c]_\mathfrak{p}, \\ \beta_{p^c}(\mathfrak{a})_{\text{ét}} : \mathbb{Z}/p^c\mathbb{Z} \xrightarrow{\sim} E(\mathfrak{a})[p^c]_{\overline{\mathfrak{p}}}. \end{cases}$$

The latter is defined over $\mathcal{K}_0$, and extends uniquely to $\mathcal{W}_0$, for the same reason as above.

Considering the Cartier dual, the same assertion holds for the former also. □

Let us use the same symbol $\beta_M(\mathfrak{a})$ etc. as in the case over $\mathbb{C}$ for the level structures obtained in the above lemma in the following:

Definition (6.1.6). With the notation as above, for $\mathfrak{a}$ prime to M (resp. prime to $\mathfrak{p}M$), we define the $\Gamma_{M,lT}$-test objects $X_{M,lT}(\mathfrak{a})_{/\mathcal{K}_0}$ over $\mathcal{K}_0$ (resp. $X_{M,lT}(\mathfrak{a})_{/\mathcal{W}_0}$ over $\mathcal{W}_0$) by

$$\begin{cases} X_{M,lT}(\mathfrak{a})_{/\mathcal{K}_0} := (E(\mathfrak{a})_{/\mathcal{K}_0}, \omega(\mathfrak{a}), \beta_M(\mathfrak{a}), C_{lT}(\mathfrak{a})), \\ X_{M,lT}(\mathfrak{a})_{/\mathcal{W}_0} := (E(\mathfrak{a})_{/\mathcal{W}_0}, \omega(\mathfrak{a}), \beta_M(\mathfrak{a}), C_{lT}(\mathfrak{a})). \end{cases}$$

Similarly for $X_{M,T}(\mathfrak{a})_{/\mathcal{K}_0}$ and $X_{M,T}(\mathfrak{a})_{/\mathcal{W}_0}$.

6.2. Integrality of special values.

In 5.2 and 5.3, starting with a Hecke character λ satisfying (5.2.3), we studied special values of Eisenstein series at CM test objects. In doing this, we decomposed the conductor $\mathfrak{c}$ of λ as $\mathfrak{c} = \mathfrak{f}\mathfrak{f}'$ as in (5.2.4) and defined the level by $M = N(\mathfrak{f})$. To apply the result in the previous subsection in which we assumed (6.1.4), the condition (5.2.4) forces us to assume the following:

Condition (6.2.1). Let e (resp. $\overline{e}$) be the exponent of $\mathfrak{p}$ (resp. $\overline{\mathfrak{p}}$) dividing $\mathfrak{c}$. Then

$$e \geq \overline{e}.$$

Conversely, if this condition is satisfied, we can clearly choose $\mathfrak{f}$ and $\mathfrak{f}'$ satisfying (5.2.4) and (6.1.4). We thus henceforth assume that λ satisfies (6.2.1), and fix such a choice. We then set

$$\begin{cases} \mathcal{K} : \text{the field generated over } \mathcal{K}_0 \text{ by the values of } \lambda_{\mathfrak{f}},\ \lambda_{\mathfrak{f}'} \text{ and } \lambda^{\mathrm{id}}, \\ \text{and } |\mathrm{Cl}_1|\text{-st roots of unity}, \\ \mathcal{W} := \mathcal{K} \cap \text{ (the ring of integers of } \overline{\mathbb{Q}}_p), \ \text{ cf. (6.1.2).} \end{cases} \tag{6.2.2}$$

Since $|\mathrm{Cl}_m|/|\mathrm{Cl}_1|$ is a power of l, $\mathcal{W}$ contains all $|\mathrm{Cl}_m|$-th roots of unity, and hence any $\overline{\mathbb{Q}}^{\times}$-valued character of $|\mathrm{Cl}_m|$ takes values in $\mathcal{W}$, for all $m \geq 1$.

Proposition (6.2.3). (1) *Let $\mathfrak{a}$ be a proper $\mathfrak{o}_n$-ideal prime to M with $n \geq 2$. Then the following value belongs to $\mathcal{W}$:*

$$\begin{aligned} \mathbb{G}_{k,\lambda}(\{\mathfrak{a}\}_n) &:= \Omega_\infty^{-k} \mathbb{G}_{k,\lambda}(\{\mathfrak{a}\}_n)_\infty \\ &= C(\lambda)\chi_{\mathfrak{f}}(l^n)\Omega_\infty^{-k}\left(L^{n}_{\{\mathfrak{a}^{-1}\}_n}(0,\lambda) - \lambda^{\mathrm{id}}((l))L^{n-1}_{\{\mathfrak{a}^{-1}\mathfrak{o}_{n-1}\}_{n-1}}(0,\lambda)\right). \end{aligned}$$

(2) *For any character $\varepsilon : \mathrm{Cl}_f \to \overline{\mathbb{Q}}^{\times}$,*

$$C(\lambda)\Omega_\infty^{-k} L^{(l)}(0, \lambda\varepsilon^{-1})$$

also belongs to $\mathcal{W}$.

PROOF. By (5.3.2), $\mathbb{G}_{k,\lambda}$ belongs to $R^k(\mathcal{W}, \Gamma_{M,l})$. To show (1), we may assume that $\mathfrak{a}$ is prime to $\mathfrak{p}$. Then by the very definition of the modular form (2.1.2), we have

$$\mathbb{G}_{k,\lambda}(X_{M,l}(\mathfrak{a})_{/\mathcal{W}}) = \Omega_\infty^{-k}\mathbb{G}_{k,\lambda}(X_{\infty,M,l}(\mathfrak{a})) \in \mathcal{W}$$

and also $\lambda^{\mathrm{id}}(\mathfrak{a})\chi_{\mathfrak{f}}(N(\mathfrak{a})) \in \mathcal{W}^\times$. Our claim follows from (5.3.5).

The second assertion then follows from (5.3.7). □

COROLLARY (6.2.4). *Let the notation and the assumption be as in of* (5.3.6) *and* (6.2.3), (1). *Then the following value also belongs to* $\mathcal{W}$:

$$(\mathbb{G}_{k,\lambda} \,|\, [S])(\{\mathfrak{a}\}_n) := \Omega_\infty^{-k}(\mathbb{G}_{k,\lambda} \,|\, [S])(\{\mathfrak{a}\}_n)_\infty.$$

PROOF. This follows from the same reason as above because $\mathbb{G}_{k,\lambda}|[S] \in R^k(\mathcal{W}, \Gamma_{M,lS})$; cf. 3.2. □

6.3. $\mathcal{W}$-valued measure on Cl_∞ attached to $\mathbb{G}_{k,\lambda}$.

We set

$$\mathrm{Cl}_\infty := \varprojlim_{n \geq 0} \mathrm{Cl}_n \tag{6.3.1}$$

cf. (4.1.6). This group can be decomposed as

$$\mathrm{Cl}_\infty = \Delta \times \mathit{\Gamma} \text{ with } \Delta \text{ a finite group and } \mathit{\Gamma} \cong \mathbb{Z}_l. \tag{6.3.2}$$

PROPOSITION (6.3.3). *There is a unique* $\mathcal{W}$*-valued measure* $\varphi_{k,\lambda} = \varphi_{\mathbb{G}_{k,\lambda}}$ *on* Cl_∞ *enjoying the following property*: *For each locally constant function* $\phi : \mathrm{Cl}_\infty \to \mathcal{W}$ *factoring through* Cl_n $(n \geq 2)$, *we have*

$$\int_{\mathrm{Cl}_\infty} \phi d\varphi_{k,\lambda} = \chi_{\mathfrak{f}}(l)^{-n} \sum_{\{\mathfrak{a}\}_n \in \mathrm{Cl}_n} \phi(\{\mathfrak{a}^{-1}\}_n)\mathbb{G}_{k,\lambda}(\{\mathfrak{a}\}_n).$$

More generally we have

PROPOSITION (6.3.4). *Assume that* $f \in R^k(\mathcal{W}, \Gamma_{M,lT})$ *satisfies the following four conditions for all* $n \geq n_0$ *for a fixed* $n_0 \geq 0$:

i) *For each proper* $\mathfrak{o}_n$*-ideal* $\mathfrak{a}$ *prime to* M, *there is an element* $\gamma(\mathfrak{a}) \in \mathcal{K}^\times$ *such that* $f(\{\mathfrak{a}\}_n) := \gamma(\mathfrak{a})f(X_{M,lT}(\mathfrak{a})_{/\mathcal{K}})$ *depends only on the class* $\{\mathfrak{a}\}_n \in \mathrm{Cl}_n$. *Further,* $\gamma(\mathfrak{a}) \in \mathcal{W}$ *if* $\mathfrak{a}$ *is prime to* $\mathfrak{p}$.

ii) $f|U(l) = \delta f$ *with* $\delta \in \mathcal{W}^\times$.

iii) $f|h_l = \epsilon f$ *with* $\epsilon \in \mathcal{W}^\times$ (*cf.* 3.1).

iv) *For* $\mathfrak{a}$ *as in* i), *let* $\mathfrak{a}_0, \ldots, \mathfrak{a}_{l-1}$ *be as in* (4.1.7) *with* $m = 1$. *Then* $\gamma(\mathfrak{a}_i) = \eta\gamma(\mathfrak{a})$ *with* $\eta \in \mathcal{W}^\times$ *which is independent of* $\mathfrak{a}$ *and* $\mathfrak{a}_i$.

Then there is a unique $\mathcal{W}$*-valued measure* φ_f *on* Cl_∞ *satisfying*

$$\int_{\mathrm{Cl}_\infty} \phi d\varphi_f = (l\epsilon^{-1}\eta\delta)^{-n} \sum_{\{\mathfrak{a}\}_n \in \mathrm{Cl}_n} \phi(\{\mathfrak{a}^{-1}\}_n)f(\{\mathfrak{a}\}_n)$$

for ϕ as in (6.3.3)*.*

We first prove (6.3.4). First of all, $f(\{\mathfrak{a}\}_n) \in \mathcal{W}$ by i). The rule

$$\phi \mapsto b^{-n} \sum_{\{\mathfrak{a}\}_n \in \mathrm{Cl}_n} \phi(\{\mathfrak{a}^{-1}\}_n) f(\{\mathfrak{a}\}_n)$$

($b \in \mathcal{W}^\times$) gives a measure on Cl_∞ if and only if

$$f(\{\mathfrak{a}\}_n) = b^{-1} \sum_{\substack{\{\mathfrak{A}\}_{n+1} \in \mathrm{Cl}_{n+1} \\ \{\mathfrak{A}\}_{n+1} \mapsto \{\mathfrak{a}\}_n}} f(\{\mathfrak{A}\}_{n+1})$$

holds for all $n \geq n_0$ and $\{\mathfrak{a}\}_n \in \mathrm{Cl}_n$ (the distribution relation). If $\{\mathfrak{a}_0, \dots, \mathfrak{a}_{l-1}\}$ is as in iv), the right hand side is equal to $b^{-1} \sum_{i=0}^{l-1} f(\{\mathfrak{a}_i\}_{n+1})$, by (4.1.7), (1).

On the other hand, it follows from i) and ii) that

$$\delta f(\{\mathfrak{a}\}_n) = \gamma(\mathfrak{a})(f|U(l))(X_{M,lT}(\mathfrak{a})_{/\mathcal{K}}).$$

But by (4.1.7), (2) and the definition of $U(l)$ (cf. 3.4), $(f|U(l))(X_{M,lT}(\mathfrak{a})_{/\mathcal{K}}) = l^{-1} \sum_{i=0}^{l-1} f(X_i)$ can be described as follows: Let $\pi_i : E(\mathfrak{a})_{/\mathcal{K}} \to E(\mathfrak{a}_i)_{/\mathcal{K}}$ be the quotient morphism. Then

$$\begin{aligned} X_i &= (E(\mathfrak{a}_i)_{/\mathcal{K}}, l^{-1}\check{\pi}_i^* \omega(\mathfrak{a}), (\pi_i \circ \beta_M(\mathfrak{a}))^\sim \circ h_l, \pi_i(C_{lT}(\mathfrak{a})) \\ &= (E(\mathfrak{a}_i)_{/\mathcal{K}}, \omega(\mathfrak{a}_i), \beta_M(\mathfrak{a}_i) \circ h_l, C_{lT}(\mathfrak{a}_i)). \end{aligned}$$

Therefore iii) implies that

$$(f|U(l))(X_{M,lT}(\mathfrak{a})_{/\mathcal{K}}) = l^{-1}\epsilon \sum_{i=0}^{l-1} f(X_{M,lT}(\mathfrak{a}_i)_{/\mathcal{K}}).$$

We conclude that

$$f(\{\mathfrak{a}\}_n) = l^{-1}\epsilon\gamma(\mathfrak{a})\delta^{-1} \sum_{i=0}^{l-1} f(X_{M,lT}(\mathfrak{a}_i)_{/\mathcal{K}}) = l^{-1}\varepsilon\eta^{-1}\delta^{-1} \sum_{i=0}^{l-1} f(\{\mathfrak{a}_i\}_{n+1})$$

by iv). This completes the proof of (6.3.4).

We next show (6.3.3). When $f = \mathbb{G}_{k,\lambda}$ and $T = 1$, we have:

i) holds with $\gamma(\mathfrak{a}) = \lambda^{\mathrm{id}}(\mathfrak{a})^{-1} \chi_{\mathfrak{f}}(N(\mathfrak{a}))^{-1}$ by (5.3.5) and (6.2.3).

ii) holds with $\delta = \chi_{\mathfrak{f}}(l) l^{k-1}$ by (5.3.3).

iii) holds with $\epsilon = \chi_{\mathfrak{f}}(l)\overline{\chi}_{\mathfrak{f}'}(l)$. Indeed, $G_{k,\lambda}$ has the character $\chi_{\mathfrak{f}}\overline{\chi}_{\mathfrak{f}'}$ by (5.1.10) and (5.2.7), and it follows easily that the same holds for $\mathbb{G}_{k,\lambda}$.

By the definition of $\mathfrak{a}_i$ given in (4.1.7), we have

$$\begin{cases} \lambda^{\mathrm{id}}(\mathfrak{a}_i) = \lambda^{\mathrm{id}}(\mathfrak{a}_i\mathfrak{o}) = \lambda^{\mathrm{id}}(l^{-1}\mathfrak{a}\mathfrak{o}) = \lambda^{\mathrm{id}}((l))^{-1}\lambda^{\mathrm{id}}(\mathfrak{a}), \\ N(\mathfrak{a}_i) = N(\mathfrak{a}_i\mathfrak{o}) = N(l^{-1}\mathfrak{a}\mathfrak{o}) = l^{-2}N(\mathfrak{a}) \end{cases}$$

whence iv) holds with $\eta = \lambda^{\mathrm{id}}((l))\chi_{\mathfrak{f}}(l)^2$.

(6.3.3) is therefore a consequence of (6.3.4), since $\lambda(l) = l^k\lambda^{\mathrm{id}}((l))\chi_{\mathfrak{f}}(l)\overline{\chi}_{\mathfrak{f}'}(l) = 1$.

From (5.3.7) and (6.3.3), we immediately obtain the following:

Corollary (6.3.5). *Let $\varepsilon : \mathrm{Cl}_f \to \overline{\mathbb{Q}}^\times$ be a character, and consider ε also as a character of $K_{\mathbb{A}}^\times$. Then we have*

$$\int_{\mathrm{Cl}_\infty} \varepsilon d\varphi_{k,\lambda} = C(\lambda)L^{(l)}(0,\lambda\varepsilon)/\Omega_\infty^k \in \mathcal{W}. \qquad \square$$

7. Non-vanishing modulo p of Hecke L-values.

7.1. Conjugation of CM test objects.

We keep the notation of previous sections. We begin with an easy

Lemma (7.1.1). *Assume that we are given an open subgroup H of $\prod_{v\in P}\mathfrak{o}_v^\times$ where P is a finite set of finite primes of K. Let n be a non-negative integer. Then for any class in $K_{\mathbb{A}}^\times/K^\times K_\infty^\times$, we can take its representative $a \in K_{\mathbb{A}}^\times$ satisfying*

$$\begin{cases} (a_v)_{v\in P} \in H, \\ a \in K_{\mathbb{A}}^\times \cap (K_\infty^\times \times \widehat{\mathfrak{o}}_n). \end{cases}$$

Proof. We may assume that P contains all primes above l. We may also assume that, for $c \in H$ and v dividing l, $c_v \in \mathfrak{o}_{n,v}^\times$.

Since $K^\times$ is dense in $\prod_{v\in P} K_v^\times$, we can choose a representative $a \in K_{\mathbb{A}}^\times$ satisfying the first condition. Write $a\mathfrak{o} = \mathfrak{a}\mathfrak{b}^{-1}$ with mutually coprime integral ideals $\mathfrak{a}$ and $\mathfrak{b}$. There is a positive integer h such that $\mathfrak{b}^h = (b)$ is principal and $b \in H$. We can then replace a by ab. □

For the moment, we fix a proper $\mathfrak{o}_n$-ideal $\mathfrak{a}$ and $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$. We take an $s \in K_{\mathbb{A}}^\times$ such that $\sigma|_{K_{\mathrm{ab}}} = [s,K]$, the Artin symbol for K. Then the main theorem of complex multiplication (Shimura [**Shi1**, Theorem 5.4]) asserts that

$$E(\mathfrak{a})^\sigma \cong E(s^{-1}\mathfrak{a}) \tag{7.1.2}$$

and we moreover have the commutative diagram

$$\begin{tikzcd} K/\mathfrak{a} \arrow[r, "\xi(\mathfrak{a})"] \arrow[d, "s^{-1}"'] & E(\mathfrak{a})(\mathbb{C}) \arrow[d, "\sigma"] \\ K/s^{-1}\mathfrak{a} \arrow[r, "\xi'"'] & E(\mathfrak{a})^\sigma(\mathbb{C}). \end{tikzcd} \tag{7.1.3}$$

Here, $\xi(\mathfrak{a}) : \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} E(\mathfrak{a})(\mathbb{C})$ is the canonical isomorphism through which we have often identified the both sides (cf. 2.2), and $\xi' : \mathbb{C}/s^{-1}\mathfrak{a} \xrightarrow{\sim} E(\mathfrak{a})^\sigma(\mathbb{C})$ is the (necessarily unique) complex uniformization which makes the diagram commutative. From now on, we assume that $s \in K_{\mathbb{A}}^\times \cap (K_\infty^\times \times \widehat{\mathfrak{o}}_n)$ so that $s^{-1}\mathfrak{a} \supseteq \mathfrak{a}$. Then there is an isogeny $\lambda_s(\mathfrak{a}) : E(\mathfrak{a}) \to E(\mathfrak{a})^\sigma$ which makes the following diagram commutative:

$$\begin{tikzcd}
\mathbb{C}/\mathfrak{a} \arrow[r, "\xi(\mathfrak{a})"] \arrow[d, "\text{canon.}"'] & E(\mathfrak{a})(\mathbb{C}) \arrow[d, "\lambda_s(\mathfrak{a})"] \\
\mathbb{C}/s^{-1}\mathfrak{a} \arrow[r, "\xi'"'] & E(\mathfrak{a})^\sigma(\mathbb{C}).
\end{tikzcd} \tag{7.1.4}$$

The following is a slight generalization of de Shalit [**dS**, Chapter II, 1.5].

Proposition (7.1.5). *Let the assumption be as above. Then $\lambda_s(\mathfrak{a})$ is the unique isogeny $E(\mathfrak{a}) \to E(\mathfrak{a})^\sigma$ having the following properties*:

i) $\mathrm{Ker}(\lambda_s(\mathfrak{a})) = E(\mathfrak{a})[\mathfrak{b}]$ *with* $\mathfrak{b} = s\mathfrak{o}_n$,

ii) *Let* $\mathfrak{c} = c\mathfrak{o}_n$ *be an integral* $\mathfrak{o}_n$*-ideal with* $c \in K_{\mathbb{A}}^\times$ *such that* $s_q \in \mathfrak{o}_{n,q}^\times$ *if* $c_q \notin \mathfrak{o}_{n,q}^\times$ *(so that we can consider the action of* s^{-1} *on* $E(\mathfrak{a})[\mathfrak{c}](\mathbb{C}) = \mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a} = \bigoplus_{q \text{ s.t. } c_q \notin \mathfrak{o}_{n,q}^\times} c_q^{-1}\mathfrak{a}_q/\mathfrak{a}_q$*). Then for any* $t \in E(\mathfrak{a})[\mathfrak{c}](\mathbb{C})$*, we have*

$$t^\sigma = \lambda_s(\mathfrak{a})(s^{-1}t).$$

Proof. The first assertion is obvious, and for $t = \xi(\mathfrak{a})(u) \in E(\mathfrak{a})[\mathfrak{c}](\mathbb{C})$ ($u \in \mathfrak{c}^{-1}\mathfrak{a}/\mathfrak{a}$), we have

$$t^\sigma = \xi(\mathfrak{a})(u)^\sigma = \xi'(s^{-1}u) = \lambda_s(\mathfrak{a})(\xi(\mathfrak{a})(s^{-1}u)) = \lambda_s(\mathfrak{a})(s^{-1}t)$$

which shows ii). Since the points t as above are Zariski dense, the uniqueness of $\lambda_s(\mathfrak{a})$ also follows. □

With the above notation, we define $\Lambda_{\mathfrak{a}}(s) \in \overline{\mathbb{Q}}^\times$ by

$$\lambda_s(\mathfrak{a})^*\omega(\mathfrak{a})^\sigma = \Lambda_{\mathfrak{a}}(s)\omega(\mathfrak{a}). \tag{7.1.6}$$

Lemma (7.1.7). *For fixed σ, s and n, $\Lambda_{\mathfrak{a}}(s)$ does not depend on the proper $\mathfrak{o}_n$-ideal $\mathfrak{a}$. We thus henceforth write it $\Lambda_n(s)$.*

Proof. Let $\mathfrak{a}$ and $\mathfrak{a}'$ be proper $\mathfrak{o}_n$-ideals. To show that $\Lambda_{\mathfrak{a}}(s) = \Lambda_{\mathfrak{a}'}(s)$, we easily reduce to the case where $\mathfrak{a} \subseteq \mathfrak{a}'$, which we now assume. Let $q : E(\mathfrak{a}) \to E(\mathfrak{a}')$ be the quotient morphism. We claim that $q^\sigma \circ \lambda_s(\mathfrak{a}) = \lambda_s(\mathfrak{a}') \circ q$.

Indeed, for any $\mathfrak{c}$ and $t \in E(\mathfrak{a})[\mathfrak{c}](\mathbb{C})$ as in (7.1.5),

$$\begin{cases} q^\sigma \circ \lambda_s(\mathfrak{a})(s^{-1}t) = q^\sigma(t^\sigma) = q(t)^\sigma, \\ \lambda_s(\mathfrak{a}') \circ q(s^{-1}t) = \lambda_s(\mathfrak{a}')(s^{-1}q(t)) = q(t)^\sigma. \end{cases}$$

Zariski density of the points $s^{-1}t$ implies our claim.

From this, we obtain

$$\begin{aligned}(q^\sigma \circ \lambda_s(\mathfrak{a}))^*\omega(\mathfrak{a}')^\sigma &= \lambda_s(\mathfrak{a})^*\omega(\mathfrak{a})^\sigma = \Lambda_{\mathfrak{a}}(s)\omega(\mathfrak{a}) \\ &= (\lambda_s(\mathfrak{a}') \circ q)^*\omega(\mathfrak{a}')^\sigma = q^*(\Lambda_{\mathfrak{a}'}(s)\omega(\mathfrak{a}')) = \Lambda_{\mathfrak{a}'}(s)\omega(\mathfrak{a}).\end{aligned}$$ □

Proposition (7.1.8). *Consider the $\Gamma_{M,lT}$-test object*

$$X_{M,lT}(\mathfrak{a})_{/\mathbb{C}} = (E(\mathfrak{a}), \omega(\mathfrak{a}), \beta_M(\mathfrak{a}), C_T(\mathfrak{a}), C_l(\mathfrak{a}))$$

obtained by base extension to $\mathbb{C}$ *of the one defined in* (6.1.6), *for a proper* $\mathfrak{o}_n$*-ideal* $\mathfrak{a}$. *For* $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$, *take* $s \in K_{\mathbb{A}}^{\times}$ *such that* $\sigma|_{K_{\mathrm{ab}}} = [s, K]$ *and*

$$\begin{cases} s_v \equiv 1 \mod l^{n+1}MT\mathfrak{o}_v \ \textit{for all finite } v \,|\, lMT, \\ s \in K_{\mathbb{A}}^{\times} \cap (K_{\infty}^{\times} \times \widehat{\mathfrak{o}}_n). \end{cases}$$

Then we have

$$(X_{M,lT}(\mathfrak{a})_{/\mathbb{C}})^{\sigma} \cong (E(s^{-1}\mathfrak{a}), \Lambda_n(s)\omega(s^{-1}\mathfrak{a}), \beta_M(s^{-1}\mathfrak{a}), C_T(s^{-1}\mathfrak{a}), C_l(s^{-1}\mathfrak{a})).$$

Proof. Let $\iota : E(\mathfrak{a})^{\sigma} \xrightarrow{\sim} E(s^{-1}\mathfrak{a})$ be the isomorphism such that $\iota \circ \lambda_s(\mathfrak{a})$ is the quotient homomorphism $\pi : E(\mathfrak{a}) \to E(s^{-1}\mathfrak{a})$. Then $\iota \circ \xi' : \mathbb{C}/s^{-1}\mathfrak{a} \to E(s^{-1}\mathfrak{a})(\mathbb{C})$ is the canonical isomorphism $\xi(s^{-1}\mathfrak{a})$.

The relation $(\iota \circ \lambda_s(\mathfrak{a}))^*\omega(s^{-1}\mathfrak{a}) = \pi^*\omega(s^{-1}\mathfrak{a}) = \omega(\mathfrak{a})$ and (7.1.6) imply that $\Lambda_n(s)\iota^*\omega(s^{-1}\mathfrak{a}) = \omega(\mathfrak{a})^{\sigma}$, i.e. via ι, $(E(\mathfrak{a})^{\sigma}, \omega(\mathfrak{a})^{\sigma}) \xrightarrow{\sim} (E(s^{-1}\mathfrak{a}), \Lambda_n(s)\omega(s^{-1}\mathfrak{a}))$.

Further viewing the map labeled $\xi(\mathfrak{a}) : K/\mathfrak{a} \to E(\mathfrak{a})(\mathbb{C})$ above as giving an embedding of the ind-finite constant group scheme $K/\mathfrak{a}$ to $E(\mathfrak{a})$ over $\mathbb{C}$, which we call $\widetilde{\xi}(\mathfrak{a})$, we obtain from (7.1.3) the commutative diagram:

$$\begin{tikzcd}
(1/lMT)\mathfrak{a}/\mathfrak{a} \arrow[r, "\text{incl.}"] \arrow[d, equal] & K/\mathfrak{a} \arrow[r, "\widetilde{\xi}(\mathfrak{a})^{\sigma}"] \arrow[d, "s^{-1}"] & E(\mathfrak{a})^{\sigma} \arrow[d, "\iota"] \\
(1/lMT)s^{-1}\mathfrak{a}/s^{-1}\mathfrak{a} \arrow[r, "\text{incl.}"'] & K/s^{-1}\mathfrak{a} \arrow[r, "\widetilde{\xi}(s^{-1}\mathfrak{a})"'] & E(s^{-1}(\mathfrak{a})).
\end{tikzcd}$$

It follows that $\iota \circ \alpha_M(\mathfrak{a})^{\sigma} = \alpha_M(s^{-1}\mathfrak{a})$, $\iota C_T(\mathfrak{a})^{\sigma} = C_T(s^{-1}\mathfrak{a})$ and $\iota C_l(\mathfrak{a})^{\sigma} = C_l(s^{-1}\mathfrak{a})$. Finally, recall that $\beta_M(\alpha)$ was defined as the $\Gamma(M)^{\mathrm{arith}}$-structure associated with $\alpha_M(\alpha)$, cf. (4.2.4). It is easy to see that $\beta_M(\alpha)^{\sigma}$ is associated with $\alpha_M(\alpha)^{\sigma}$, from which we conclude that $\iota \circ \beta_M(\mathfrak{a})^{\sigma} = \beta_M(s^{-1}\mathfrak{a})$. □

We now return to the situation considered in 6.3.

Corollary (7.1.9). *Let* F *be the extension of* K *generated by the values of* $\chi_{\mathfrak{f}}$, $\chi_{\mathfrak{f}'}$ *and* λ^{id} *together with* $|\mathrm{Cl}_1|$*-st roots of unity. Let* $\varepsilon : \mathrm{Cl}_n \to \overline{\mathbb{Q}}^{\times}$ *be a character. If* σ *is an automorphism of* $\mathcal{K}(= F\mathcal{K}_0$, *cf.* (6.2.2)) *over* F *which induces an automorphism of* $\mathcal{W}$,

$$\int_{\mathrm{Cl}_\infty} \varepsilon d\varphi_{k,\lambda} \in \mathcal{W}^{\times} \ \textit{if and only if} \int_{\mathrm{Cl}_\infty} \varepsilon^{\sigma} d\varphi_{k,\lambda} \in \mathcal{W}^{\times}.$$

Proof. We may assume that $n \geq 2$. The left hand side is equal to

$$\chi_{\mathfrak{f}}(l)^{-n} \sum_{\{\mathfrak{a}\}_n \in \mathrm{Cl}_n} \varepsilon(\{\mathfrak{a}^{-1}\}_n)\lambda^{\mathrm{id}}(\mathfrak{a})^{-1}\chi_{\mathfrak{f}}(N(\mathfrak{a}))^{-1}\mathbb{G}_{k,\lambda}(X_{M,l}(\mathfrak{a})_{/\mathcal{K}})$$

by (5.3.5), (6.2.3) and (6.3.3), where we take $\mathfrak{a}$ to be prime to $\mathfrak{p}M$.

Extend σ to an automorphism of $\mathbb{C}$ and take $s \in K_{\mathbb{A}}^{\times}$ as in (7.1.8). If we set $\mathfrak{b} := s\mathfrak{o}_n$, we see that $(\lambda^{\mathrm{id}}(\mathfrak{a})^{-1}\chi_{\mathfrak{f}}(N(\mathfrak{a}))^{-1}\mathbb{G}_{k,\lambda}(X_{M,l}(\mathfrak{a})_{/\mathcal{K}}))^{\sigma}$ is equal to

$$\Lambda_n(s)^{-k}\lambda^{\mathrm{id}}(\mathfrak{b})^{-1}\chi_{\mathfrak{f}}(N(\mathfrak{b}))^{-1} \times \lambda^{\mathrm{id}}(\mathfrak{b}^{-1}\mathfrak{a})^{-1}\chi_{\mathfrak{f}}(N(\mathfrak{b}^{-1}\mathfrak{a}))^{-1}\mathbb{G}_{k,\lambda}(X_{M,l}(\mathfrak{b}^{-1}\mathfrak{a})_{/\mathcal{K}})$$

by (7.1.8). By (7.1.1), we can assume here that $\mathfrak{b}$, and hence $\deg(\lambda_s(\mathfrak{a}))$ also, is prime to p. Then $\lambda^{\mathrm{id}}(\mathfrak{b})$, as well as the root of unity $\chi_{\mathfrak{f}}(N(\mathfrak{b}))$, belongs to $\mathcal{W}^{\times}$. Further, since $\omega(\mathfrak{a})^{\sigma}$ is a nowhere vanishing differential on $E(\mathfrak{a})^{\sigma}_{/\mathcal{W}}$, we see that $\Lambda_n(s) \in \mathcal{W}^{\times}$; cf. (7.1.6). Thus $(\int_{\mathrm{Cl}_\infty} \varepsilon d\varphi_{k,\lambda})^{\sigma}$ and $\int_{\mathrm{Cl}_\infty} \varepsilon^{\sigma} d\varphi_{k,\lambda}$ differ only by a multiple of an element of $\mathcal{W}^{\times}$. □

7.2. Decomposition of Cl_∞.

So far we have already relied on ideas of Hida, in constructing the measures on Cl_∞ through the special values of the Eisenstein series, in previous sections. We follow his method more closely in the following.

Recall that $\mathrm{Cl}_\infty = \varprojlim_{n\geq 0} \mathrm{Cl}_n$ (6.3.1), and $\mathrm{Cl}_\infty = \Delta \times \mathit{\Gamma}$ (6.3.2). We set

$$\mathit{\Gamma}_n := (\text{the image of } \mathit{\Gamma} \text{ in } \mathrm{Cl}_n \text{ via } \mathrm{Cl}_\infty \to \mathrm{Cl}_n). \qquad (7.2.1)$$

It is easy to see that the composite of $\Delta \hookrightarrow \mathrm{Cl}_\infty \to \mathrm{Cl}_n$ is injective for n large, and

$$\mathrm{Cl}_n = \Delta \times \mathit{\Gamma}_n \text{ for } n \gg 0. \qquad (7.2.2)$$

Definition (7.2.3). For an idele $x \in K_{\mathbb{A}}^{\times}$ whose l-component x_l is one, the system $(x\mathfrak{o}_n)_{n\geq 0}$ of ideals determines an element of Cl_∞. This depends only on the ideal $\mathfrak{x} = x\mathfrak{o}$, and hereafter denoted by $\{\mathfrak{x}\}_\infty$. We denote by $\mathrm{Cl}^{\mathrm{alg}}$ the subgroup of Cl_∞ formed of such elements.

We set $\Delta^{\mathrm{alg}} := \Delta \cap \mathrm{Cl}^{\mathrm{alg}}$.

Thus if $\mathfrak{x}$ is an integral ideal of $\mathfrak{o}$ prime to l, $\{\mathfrak{x}\}_\infty = (\{\mathfrak{x}_n\}_n)_{n\geq 0}$ where $\mathfrak{x}_n = \mathfrak{x} \cap \mathfrak{o}_n$. We recall

Proposition (7.2.4) (Hida [**H3**, Lemma 8.23]). i) *Complex conjugation acts as the inverse on* Cl_∞.

ii) *Each element of* Δ^{alg} *is represented by a square free product of primes ramified in* $K/\mathbb{Q}$ *and prime to* l. Δ^{alg} *is an elementary abelian group of type* $(2, \ldots, 2)$.

iii) *Each element of* $\mathrm{Cl}_\infty/\Delta^{\mathrm{alg}}\mathit{\Gamma}$ *is represented by* (*the class in* $\mathrm{Cl}^{\mathrm{alg}}$ *of*) *a prime ideal split in* $K/\mathbb{Q}$ *and prime to* l.

iv) *When* $\mathfrak{x}$ *is a fractional* $\mathfrak{o}$-*ideal prime to* l, *we denote by* $\{\mathfrak{x}\}_{\mathit{\Gamma}}$ (*resp.* $\{\mathfrak{x}\}_\Delta$) *the projection of* $\{\mathfrak{x}\}_\infty$ *to* $\mathit{\Gamma}$ (*resp.* Δ).

When $\mathfrak{x}'$ *is also prime to* l, *if* $\{\mathfrak{x}\}_\Delta \notin \{\mathfrak{x}'\}_\Delta\Delta^{\mathrm{alg}}$, *then* $\{\mathfrak{x}\}_{\mathit{\Gamma}}\{\mathfrak{x}'\}_{\mathit{\Gamma}}^{-1} \notin \mathrm{Cl}^{\mathrm{alg}}$. □

We then take and fix a complete set of representatives $\mathcal{R}$ of Δ^{alg} as in (7.2.4), ii), and also a complete set of representatives $\mathcal{Q}$ of $\mathrm{Cl}_\infty/\Delta^{\mathrm{alg}}\mathit{\Gamma}$ as in (7.2.4), iii). We will always assume that each $\mathfrak{q} \in \mathcal{Q}$ is prime to plM, and $N(\mathfrak{q})$ ($\mathfrak{q} \in \mathcal{Q}$) are all different (which is of course possible).

We therefore have

$$\begin{cases} \mathrm{Cl}_\infty = \displaystyle\coprod_{\substack{\mathfrak{q}\in\mathcal{Q} \\ \mathfrak{r}\in\mathcal{R}}} \mathit{\Gamma}\{\mathfrak{q}\mathfrak{r}\}_\infty = \coprod_{\substack{\mathfrak{q}\in\mathcal{Q} \\ \mathfrak{r}\in\mathcal{R}}} \mathit{\Gamma}\{\mathfrak{q}\mathfrak{r}\}_\infty^{-1}, \text{ and} \\ \mathrm{Cl}_n = \displaystyle\coprod_{\substack{\mathfrak{q}\in\mathcal{Q} \\ \mathfrak{r}\in\mathcal{R}}} \mathit{\Gamma}_n\{\mathfrak{q}_n\mathfrak{r}_n\}_n = \coprod_{\substack{\mathfrak{q}\in\mathcal{Q} \\ \mathfrak{r}\in\mathcal{R}}} \mathit{\Gamma}_n\{\mathfrak{q}_n\mathfrak{r}_n\}_n^{-1} \text{ for } n \gg 0. \end{cases} \tag{7.2.5}$$

Definition (7.2.6). Fix a character $\nu : \Delta \to \overline{\mathbb{Q}}^\times$, and consider it also a character of Cl_∞ through the projection to Δ. For an $\mathfrak{o}$-ideal $\mathfrak{x}$ prime to lM, we set $c_{k,\lambda,\nu}(\mathfrak{x}) := \nu(\{\mathfrak{x}\}_\infty)N(\mathfrak{x})^k\lambda^{\mathrm{id}}(\mathfrak{x})\chi_{\mathfrak{f}}(N(\mathfrak{x}))$, and define

$$\mathbb{H}_{k,\lambda,\nu} := \sum_{\mathfrak{r}\in\mathcal{R}} c_{k,\lambda,\nu}(\mathfrak{r})\mathbb{G}_{k,\lambda} \mid [N(\mathfrak{r})].$$

$\mathbb{H}_{k,\lambda,\nu}$ is an element of $R^k(\mathcal{W}, \Gamma_{M,lR})$, where R is the product of norms of all primes in $\mathcal{R}$. Indeed, $c_{k,\lambda,\nu}(\mathfrak{r}) \in \mathcal{W}$ by the definition (6.2.2), and $\mathbb{G}_{k,\lambda} \mid [N(\mathfrak{r})] \in R^k(\mathcal{W}, \Gamma_{M,lN(\mathfrak{r})})$, cf. (3.2.1).

In the following argument, we take the set of ideals $\{\mathfrak{t}_1, \dots, \mathfrak{t}_t\}$ in (4.2.1) to be the set of all prime ideals dividing some element of $\mathcal{Q} \cup \mathcal{R}$. We will use it to define $\Gamma_{M,lT}$-test objects (6.1.6), and the special values $\mathbb{G}_{k,\lambda} \mid [S](\{\mathfrak{a}\}_n)$ (6.2.4), and also the values $(\mathbb{H}_{k,\lambda,\nu} \mid [N(\mathfrak{q})])(\{\mathfrak{g}\}_n)$ figuring below.

Lemma (7.2.7). *Let $\phi = \nu \times \phi_{\mathit{\Gamma}} : \Delta \times \mathit{\Gamma} \to \overline{\mathbb{Q}}$ be a function on Cl_∞ factoring through $\mathrm{Cl}_n = \Delta \times \mathit{\Gamma}_n$ for an n large. We have*

$$\int_{\mathrm{Cl}_\infty} \phi d\varphi_{k,\lambda} = \chi_{\mathfrak{f}}(l)^{-n} \sum_{\mathfrak{q}\in\mathcal{Q}} c_{k,\lambda,\nu}(\mathfrak{q}) \Biggl(\sum_{\{\mathfrak{g}\}_n \in \mathit{\Gamma}_n} \phi_{\mathit{\Gamma}}(\{\mathfrak{q}\}_{\mathit{\Gamma}_n}\{\mathfrak{g}\}_n^{-1})(\mathbb{H}_{k,\lambda,\nu} \mid [N(\mathfrak{q})])(\{\mathfrak{g}\}_n) \Biggr).$$

Here and below, $\{\mathfrak{q}\}_{\mathit{\Gamma}_n}$ is the projection of $\{\mathfrak{q}\}_\infty \in \mathrm{Cl}_\infty$ to $\mathit{\Gamma}_n$.

Proof. The left hand side is equal to

$$\chi_{\mathfrak{f}}(l)^{-n} \sum_{\mathfrak{r},\mathfrak{q},\{\mathfrak{g}_n\}} \nu(\{\mathfrak{r}\mathfrak{q}\}_\infty)\phi_{\mathit{\Gamma}}(\{\mathfrak{q}\}_{\mathit{\Gamma}_n}\{\mathfrak{g}\}_n^{-1})\mathbb{G}_{k,\lambda}(\{\mathfrak{r}_n\mathfrak{q}_n\}_n^{-1}\{\mathfrak{g}\}_n)$$

where the sum is over $\mathfrak{r} \in \mathcal{R}$, $\mathfrak{q} \in \mathcal{Q}$ and $\{\mathfrak{g}\}_n \in \mathit{\Gamma}_n$. But (5.3.6) and its proof show that, with the same notation as loc. cit.,

$$\mathbb{G}_{k,\lambda}(\{\mathfrak{s}_n^{-1}\mathfrak{a}\}_n) = \nu(\{\mathfrak{s}\}_\infty)^{-1}c_{k,\lambda,\nu}(\mathfrak{s})(\mathbb{G}_{k,\lambda} \mid [N(\mathfrak{s})])(\{\mathfrak{a}\}_n)$$

from which our claim follows. □

7.3. Main theorem of Part I.

Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{W}$. The following is the main result of Part I:

Theorem (7.3.1). *Assume* (5.2.3), (6.1.1) *and* (6.2.1). *Consider locally constant characters $\varepsilon : \mathrm{Cl}_\infty \to \mathcal{W}^\times$, i.e. characters that factor through some Cl_n with finite n. Then except for a finite number of exceptions, we have*

$$\int_{\mathrm{Cl}_\infty} \varepsilon d\varphi_{k,\lambda} \not\equiv 0 \mod \mathfrak{m}.$$

In view of (6.3.5), this theorem implies Theorem I in the Introduction to Part I under (5.2.3) and (6.2.1).

In this subsection, we give preliminary calculations toward this theorem. We write $\overline{\mathbb{F}}_p$ for the residue field $\mathcal{W}/\mathfrak{m}$, an algebraic closure of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. By reduction modulo $\mathfrak{m}$, we obtain from $\varphi_{k,\lambda}$ an $\overline{\mathbb{F}}_p$-valued measure on Cl_∞, which we denote by the same symbol, and we will work in characteristic p.

To prove the theorem, we may restrict ourselves only to characters $\varepsilon : \mathrm{Cl}_\infty \to \overline{\mathbb{F}}_p^\times$ of the form $\nu \times \varepsilon_\varGamma$, where a character ν of Δ is fixed and characters $\varepsilon_\varGamma$ of $\varGamma$ vary. *From now on, we assume that there is an infinite set $\mathcal{E}_\nu$ of locally constant characters $\varepsilon = \nu \times \varepsilon_\varGamma$ such that* $\int_{\mathrm{Cl}_\infty} \varepsilon d\varphi_{k,\lambda} = 0$ (until we arrive at a contradiction at the end of the next subsection). Let $\mathbb{F}$ be the field generated by the values of ν and all l-th roots of unity in $\overline{\mathbb{F}}_p$ over the residue field of F (7.1.9) at the prime defined by $F \subseteq \overline{\mathbb{Q}}_p$. When $l = 2$, we also add all fourth roots of unity to define $\mathbb{F}$. $\mathbb{F}$ contains the values $c_{k,\lambda,\nu}(\mathfrak{q})$ (reduced modulo $\mathfrak{m}$).

Now take $\varepsilon = \nu \times \varepsilon_\varGamma \in \mathcal{E}_\nu$ and let $\mathbb{F}(\varepsilon_\varGamma)$ be the field generated by the values of $\varepsilon_\varGamma$ over $\mathbb{F}$. If ε factors through $\mathrm{Cl}_n = \Delta \times \varGamma_n$, we have by (7.2.7),

$$\sum_{\mathfrak{q}\in\mathcal{Q}} c_{k,\lambda,\nu}(\mathfrak{q})\left(\sum_{\{\mathfrak{g}\}_n\in\varGamma_n} \varepsilon_\varGamma(\{\mathfrak{q}\}_{\varGamma_n}\{\mathfrak{g}\}_n^{-1})(\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})])(\{\mathfrak{g}\}_n\{\mathfrak{a}\}_n)\right) = 0$$

for any fixed $\{\mathfrak{a}\}_n \in \varGamma_n$, because $\varepsilon_\varGamma$ is a character. By (7.1.9), we may replace $\varepsilon_\varGamma$ above by $\varepsilon_\varGamma^\sigma$ for any $\mathrm{Gal}(\mathbb{F}(\varepsilon_\varGamma)/\mathbb{F})$, and consequently $\varepsilon_\varGamma$ by $\mathrm{Tr}_{\mathbb{F}(\varepsilon_\varGamma)/\mathbb{F}}(\varepsilon_\varGamma)$ which satisfies

$$\mathrm{Tr}_{\mathbb{F}(\varepsilon_\varGamma)/\mathbb{F}}(\varepsilon_\varGamma)(x) = \begin{cases} 0 & \text{if } \varepsilon_\varGamma(x) \notin \mathbb{F}, \\ [\mathbb{F}(\varepsilon_\varGamma) : \mathbb{F}]\varepsilon_\varGamma(x) & \text{if } \varepsilon_\varGamma(x) \in \mathbb{F}. \end{cases}$$

Here, $[\mathbb{F}(\varepsilon_\varGamma) : \mathbb{F}]$ is a power of l, and hence non-zero (in characteristic p).

Let l^r be the number of elements of l-power order in $\mathbb{F}^\times$, and denote by μ_{l^r} the subgroup of such elements; $\mu_{l^r} = \mathbb{F}^\times[l^\infty]$. We obtain

$$\sum_{\mathfrak{q}\in\mathcal{Q}} c_{k,\lambda,\nu}(\mathfrak{q})\left(\sum_{\substack{\{\mathfrak{g}\}_n\in\varGamma_n \\ \varepsilon_\varGamma(\{\mathfrak{g}\}_n)\in\mu_{l^r}}} \varepsilon_\varGamma(\{\mathfrak{g}\}_n)^{-1}(\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})])(\{\mathfrak{q}\}_{\varGamma_n}\{\mathfrak{g}\}_n\{\mathfrak{a}\}_n)\right) = 0.$$

If $\mathrm{Cl}_{n_0} = \Delta \times \varGamma_{n_0}$ with $\varGamma_{n_0} = \varGamma/\varGamma^{l^{s_0}}$ for one n_0, then $\mathrm{Cl}_{n_0+m} = \Delta \times \varGamma_{n_0+m}$ with $\varGamma_{n_0+m} = \varGamma/\varGamma^{l^{s_0+m}}$ for all $m \geq 0$. Therefore if $\mathrm{Ker}(\varepsilon_\varGamma) = \varGamma^{l^t}$ with $t > s_0 + r$, we have that

i) $\varepsilon_\varGamma$ induces an injection $\varGamma_{n(\varepsilon)} \hookrightarrow \overline{\mathbb{F}}_p^\times$ with $n(\varepsilon) = n_0 + t - s_0$; and moreover

ii) $\{\mathfrak{g}\}_{n(\varepsilon)} \in \varGamma_{n(\varepsilon)}$ satisfies $\varepsilon_\varGamma(\{\mathfrak{g}\}_{n(\varepsilon)}) \in \mu_{l^r}$ if and only if $\{\mathfrak{g}\}_{n(\varepsilon)} \in \mathrm{Ker}(\varGamma_{n(\varepsilon)} \to \varGamma_{n(\varepsilon)-r}) = \mathrm{Ker}(\mathrm{Cl}_{n(\varepsilon)} \to \mathrm{Cl}_{n(\varepsilon)-r}) =: G_{n(\varepsilon),r}$.

Thus replacing $\mathcal{E}_\nu$ by a smaller infinite subset if necessary, we henceforth assume that every $\varepsilon = \nu \times \varepsilon_\varGamma \in \mathcal{E}_\nu$ satisfies i), ii) and also

iii) $n(\varepsilon) \geq 2r$.

By this condition, the correspondence $i \mapsto \{e_{n(\varepsilon)-r,i}\mathfrak{o}_{n(\varepsilon)}\}_{n(\varepsilon)}$ gives an isomorphism of groups $\mathbb{Z}/l^r\mathbb{Z} \cong G_{n(\varepsilon),r}$, where $e_{n(\varepsilon)-r,i} = 1 + il^{n(\varepsilon)-r}Mw \in \mathfrak{o}^{\times}_{n(\varepsilon)-r,l}$, by (4.1.9). Thus replacing $\mathcal{E}_\nu$ again, we may also assume that

iv) the primitive l^r-th root of unity $\varepsilon_\Gamma(\{e_{n(\varepsilon)-r,1}\mathfrak{o}_{n(\varepsilon)}\}_{n(\varepsilon)})$ is independent of $\varepsilon \in \mathcal{E}_\nu$. Call this value ζ.

Thus, for any $\{\mathfrak{a}\}_{n(\varepsilon)} \in \Gamma_{n(\varepsilon)}$, we have

$$\sum_{\mathfrak{q}\in\mathcal{Q}} c_{k,\lambda,\nu}(\mathfrak{q}) \left(\sum_{i=0}^{l^r-1} \zeta^{-i} (\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})])(\{\mathfrak{q}\}_{\Gamma_{n(\varepsilon)}}\{e_{n(\varepsilon)-r,i}\mathfrak{a}\}_{n(\varepsilon)}) \right) = 0.$$

Next, for each $\mathfrak{q} \in \mathcal{Q}$, take and fix proper $\mathfrak{o}_n$-ideals $\mathfrak{d}(\mathfrak{q})_n$ such that $\{\mathfrak{q}\}_\Gamma = (\{\mathfrak{d}(\mathfrak{q})_n\}_n)_{n\geq 0}$. We further assume that each $\mathfrak{d}(\mathfrak{q})_n$ is prime to pMT, and that $\mathfrak{d}(\mathfrak{q})_{n+1}\mathfrak{o}_n = \mathfrak{d}(\mathfrak{q})_n$ for all $n \geq 0$. Such a choice of $\mathfrak{d}(\mathfrak{q})_n$ is of course possible.

Recall that in general,

$$(\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})])(\{\mathfrak{b}\}_n) = \lambda^{\mathrm{id}}(\mathfrak{b})^{-1}\chi_{\mathfrak{f}}(N(\mathfrak{b}))^{-1}(\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})])(X_{M,lT}(\mathfrak{b})_{/\overline{\mathbb{F}}_p})$$

for any proper $\mathfrak{o}_n$-ideal $\mathfrak{b}$ prime to pMT. In the above situation, we have

$$\begin{cases} \lambda^{\mathrm{id}}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}e_{n(\varepsilon)-r,i}\mathfrak{a}) = \lambda^{\mathrm{id}}(\mathfrak{d}(\mathfrak{q})_0)\lambda^{\mathrm{id}}(\mathfrak{a}), \\ \chi_{\mathfrak{f}}(N(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}e_{n(\varepsilon)-r,i}\mathfrak{a})) = \chi_{\mathfrak{f}}(N(\mathfrak{d}(\mathfrak{q})_0))\chi_{\mathfrak{f}}(N(\mathfrak{a})). \end{cases}$$

Setting

$$c'_{k,\lambda,\nu}(\mathfrak{d}(\mathfrak{q})_0) := \lambda^{\mathrm{id}}(\mathfrak{d}(\mathfrak{q})_0)^{-1}\chi_{\mathfrak{f}}(N(\mathfrak{d}(\mathfrak{q})_0))^{-1}c_{k,\lambda,\nu}(\mathfrak{q}) \tag{7.3.2}$$

we have

$$\sum_{i=0}^{l^r-1}\sum_{\mathfrak{q}\in\mathcal{Q}} c'_{k,\lambda,\nu}(\mathfrak{d}(\mathfrak{q})_0)\zeta^{-i}(\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})])(X_{M,lT}(e_{n(\varepsilon)-r,i}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a}))_{/\overline{\mathbb{F}}_p}) = 0$$

for any $\mathfrak{a}$ prime to pMT such that $\{\mathfrak{a}\}_{n(\varepsilon)} \in \Gamma_{n(\varepsilon)}$.

From now on, we set $n_1 := \min\{n(\varepsilon) - r \mid \varepsilon \in \mathcal{E}_\nu\}$, and consider only $\mathfrak{a}$ such that $\{\mathfrak{a}\}_{n(\varepsilon)} \in \mathrm{Ker}(\Gamma_{n(\varepsilon)} \to \Gamma_{n_1}) = \mathrm{Ker}(\mathrm{Cl}_{n(\varepsilon)} \to \mathrm{Cl}_{n_1})$. On the other hand, from the outset we could choose each $\mathfrak{q}$ in such a way that $\{\mathfrak{q}\}_\Gamma \in \mathrm{Ker}(\Gamma \to \Gamma_{n_1})$ so that $\{\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\}_{n(\varepsilon)} \in \mathrm{Ker}(\Gamma_{n(\varepsilon)} \to \Gamma_{n_1})$ also. In Section 4, we have defined for such $\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a}$ a collection of $\Gamma(l^\infty)^{\mathrm{arith}}$-structures $\beta_{l^\infty}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})_I$ on $E(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})$ for I in a congruence class $\overline{I} \in \mathbb{Z}/l^{n(\varepsilon)-n_1}\mathbb{Z}$. (The indices n, m and i in 4.3 are now replaced by n_1, $n(\varepsilon)-n_1$ and I, respectively.) These $\Gamma(l^\infty)^{\mathrm{arith}}$-structures extend to $\mathcal{W}$ (6.1.5), and we can consider the $\Gamma_{l^\infty M,T}$-test objects $X_{l^\infty M,T}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})_{I/\overline{\mathbb{F}}_p}$ in a similar manner as (4.3.5). The $\Gamma_{M,lT}$-test object associated to them (cf. 3.4) is $X_{M,lT}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})_{/\overline{\mathbb{F}}_p}$, which is independent of I.

Lemma (7.3.3). *With the same notation and assumptions as above, set*

$$\widetilde{\mathbb{H}}_{k,\lambda,\nu,\mathfrak{q}} := \sum_{i=0}^{l^r-1} \zeta^{-i}\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})]|B_{r,i} \in R^k(\overline{\mathbb{F}}_p, \Gamma_{l^{2r}M,T}).$$

Then we have

$$\sum_{\mathfrak{q}\in\mathcal{Q}} c'_{k,\lambda,\nu}(\mathfrak{d}(\mathfrak{q})_0)\widetilde{\mathbb{H}}_{k,\lambda,\nu,\mathfrak{q}}(X_{l^\infty M,T}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})_{I/\overline{\mathbb{F}}_p}) = 0 \tag{$***$}$$

for all $\varepsilon \in \mathcal{E}_\nu$. Here $\mathfrak{a}$ is any proper $\mathfrak{o}_{n(\varepsilon)}$-ideal prime to pMT such that $\{\mathfrak{a}\}_{n(\varepsilon)} \in$ $\mathrm{Ker}(\mathrm{Cl}_{n(\varepsilon)} \to \mathrm{Cl}_{n_1})$.

Proof. It is easy to see that $\widetilde{\mathbb{H}}_{k,\lambda,\nu,\mathfrak{q}}$ in fact belongs to $R^k(\overline{\mathbb{F}}_p, \Gamma_{l^{2r}M,T})$. From (4.3.6), we have

$$B_{r,i}X_{l^\infty M,T}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})_{I/\overline{\mathbb{F}}_p} = X_{l^\infty M,T}(e_{n(\varepsilon)-r,i}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a}))_{I'/\overline{\mathbb{F}}_p}$$

for $0 \le i \le l^{r-1}$ ($I' = I + il^{n(\varepsilon)-n_1-r}$). Since $\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})] \in R^k(\overline{\mathbb{F}}_p, \Gamma_{M,lT})$, the value $\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})](B_{r,i}X_{l^\infty M,T}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})_{I/\overline{\mathbb{F}}_p})$ is equal to $\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})](X_{M,lT}(e_{n(\varepsilon)-r,i}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a}))_{/\overline{\mathbb{F}}_p})$. □

7.4. Application of Hida's Zariski density theorem.

In general, let E be an ordinary elliptic curve over an $\mathbb{F}_p$-scheme S, equipped with an Igusa structure of level p

$$\gamma_p : \boldsymbol{\mu}_p \hookrightarrow E; \text{ a closed immersion of } S\text{-group schemes.} \tag{7.4.1}$$

Then there is the unique nowhere-vanishing invariant differential $\omega_{p\text{-can}}$ on E such that

$$\gamma_p^*\omega_{p\text{-can}} = dx/x \tag{7.4.2}$$

where x is the standard parameter on $\boldsymbol{\mu}_p$ or $\mathbb{G}_m$. For example, when $E = \mathrm{Tate}(q)$ over $\mathbb{F}_p((q))$ with the canonical Igusa structure of level p, $\omega_{p\text{-can}}$ is the reduction modulo p of ω_{can}.

Especially, if we set

$$a'(E, \beta_p) := (\omega_{p\text{-can}} \text{ on } E \text{ with respect to } \beta_p\,|_{\boldsymbol{\mu}_p}) \tag{7.4.3}$$

for each $\Gamma(p)^{\mathrm{arith}}$-curve (E, β_p) over an $\mathbb{F}_p$-scheme, the formation of this association is compatible with Cartesian squares, and hence gives a modular form of weight one belonging to $R^1(\mathbb{F}_p, \Gamma(p)^{\mathrm{arith}})$ in the sense recalled in the proof of (2.3.8). The corresponding element $a \in R^1(\mathbb{F}_p, \Gamma(p)^{\mathrm{arith}})$ in the sense of (2.1.2) is thus given by

$$a(E, \omega, \beta_p) = c^{-1} \text{ if } \omega = c\omega_{p\text{-can}} \tag{7.4.4}$$

for $\Gamma(p)^{\mathrm{arith}}$-test objects (E, ω, β_p) over $\mathbb{F}_p$-algebras. We set

$$M' = \begin{cases} M & \text{when } M \text{ is divisible by } p, \\ Mp & \text{when } M \text{ is not divisible by } p \end{cases} \tag{7.4.5}$$

and consider a also as an element of $R^1(\mathbb{F}_p, \Gamma(M')^{\mathrm{arith}})$ or $R^1(\mathbb{F}_p, \Gamma_{M',T})$.

In what follows, as in the previous subsection, we continue to work in characteristic p.

Lemma (7.4.6). *Choose $\omega(\mathfrak{o})$ on $E(\mathfrak{o})_{/\overline{\mathbb{F}}_p}(= E(\mathfrak{o})_{/\mathcal{W}_0} \otimes \overline{\mathbb{F}}_p)$ in such a way that $\omega(\mathfrak{o}) = \omega(\mathfrak{o})_{p\text{-can}}$. Then for a proper $\mathfrak{o}_n$-ideal $\mathfrak{a}$ prime to p, we have*

$$\omega(\mathfrak{a}) = l^n N(\mathfrak{a})\omega(\mathfrak{a})_{p\text{-can}} \ \text{ on } \ E(\mathfrak{a})_{/\overline{\mathbb{F}}_p}.$$

Proof. In (6.1.3), we have fixed our choice of $\omega(\mathfrak{o})$ over $\mathcal{W}_0$ which is unique only up to $\mathcal{W}_0^\times$-multiples. It is thus possible to choose it in such a way that $\omega(\mathfrak{o}) = \omega(\mathfrak{o})_{p\text{-can}}$ in characteristic p.

In general, let $\mathfrak{a}$ and $\mathfrak{a}'$ be proper $\mathfrak{o}_n$-ideals prime to p such that $\mathfrak{a} \subseteq \mathfrak{a}'$. We have, from (1.2.5), the commutative diagram:

$$\begin{tikzcd}
E(\mathfrak{a})_{/\overline{\mathbb{F}}_p} \arrow[r, "\pi"] & E(\mathfrak{a}')_{/\overline{\mathbb{F}}_p} \\
\boldsymbol{\mu}_p \arrow[u, "\gamma_p(\mathfrak{a})"] \arrow[r, "\deg(\pi)"'] & \boldsymbol{\mu}_p \arrow[u, "\gamma_p(\mathfrak{a}')"']
\end{tikzcd}$$

where π is the natural quotient morphism of degree $|\mathfrak{a}' : \mathfrak{a}|$, and $\gamma_p(\mathfrak{a})$ and $\gamma_p(\mathfrak{a}')$ are induced from $\beta_p(\mathfrak{a})$ and $\beta_p(\mathfrak{a}')$, respectively. (Indeed, (1.2.5) gives us a similar diagram over $\mathcal{K}_0$, which extends to $\mathcal{W}_0$.) It then follows that

$$\pi^*\omega(\mathfrak{a}')_{p\text{-can}} = \deg(\pi)\omega(\mathfrak{a})_{p\text{-can}}$$

(and similarly when $\mathfrak{a}$ and $\mathfrak{a}'$ are respectively replaced by $\mathfrak{o}_n$ and $\mathfrak{o}$). Our conclusion follows from the argument similar to that of (4.2.8). □

We now return to the equation $(***)$ in (7.3.3). Let us denote by $X_{l^sM',T}(\mathfrak{b})_{I/\overline{\mathbb{F}}_p}$ the $\Gamma_{l^sM',T}$-test object attached to $X_{l^\infty M',T}(\mathfrak{b})_{I/\overline{\mathbb{F}}_p}$ for $s < \infty$. We then denote by $X_{l^sM',T}(\mathfrak{b})^{p\text{-can}}_{I/\overline{\mathbb{F}}_p}$ the test object obtained from it by replacing $\omega(\mathfrak{b})$ by $\omega(\mathfrak{b})_{p\text{-can}}$. Also let $x_{l^sM',T}(\mathfrak{b})_{I/\overline{\mathbb{F}}_p}$ be the geometric point of the modular scheme $\mathfrak{M}(\Gamma_{l^sM',T})_{/\overline{\mathbb{F}}_p}$ (cf. 1.1; it exists because $M' \geq 3$) corresponding to $X_{l^sM',T}(\mathfrak{b})_{I/\overline{\mathbb{F}}_p}$ with the differential removed. Now if we set

$$c''_{k,\lambda,\nu}(\mathfrak{d}(\mathfrak{q})_0) := N(\mathfrak{d}(\mathfrak{q})_0)^{-k}c'_{k,\lambda,\nu}(\mathfrak{d}(\mathfrak{q})_0) \tag{7.4.7}$$

we obtain from $(***)$ that

$$\sum_{\mathfrak{q}\in\mathcal{Q}} c''_{k,\lambda,\nu}(\mathfrak{d}(\mathfrak{q})_0)\widetilde{\mathbb{H}}_{k,\lambda,\nu,\mathfrak{q}}(X_{l^{2r}M',T}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})^{p\text{-can}}_{I/\overline{\mathbb{F}}_p}) = 0.$$

Since

$$a(X_{l^{2r}M',T}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})^{p\text{-can}}_{I/\overline{\mathbb{F}}_p}) = 1$$

by (7,4,4), $(***)$ now becomes a *relation of modular functions* on $\mathfrak{M}(\Gamma_{l^{2r}M',T})_{/\overline{\mathbb{F}}_p}$

$$\sum_{\mathfrak{q}\in\mathcal{Q}} c''_{k,\lambda,\nu}(\mathfrak{d}(\mathfrak{q})_0)\frac{\widetilde{\mathbb{H}}_{k,\lambda,\nu,\mathfrak{q}}}{a^k}(x_{l^{2r}M',T}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})_{I/\overline{\mathbb{F}}_p}) = 0. \qquad (****)$$

Consider the set

$$\mathcal{X} := \{(x_{l^{2r}M',T}(\mathfrak{d}(\mathfrak{q})_{n(\varepsilon)}\mathfrak{a})_{I/\overline{\mathbb{F}}_p})_{\mathfrak{q}\in\mathcal{Q}} \mid \varepsilon \in \mathcal{E}_\nu, \{\mathfrak{a}\}_{n(\varepsilon)} \in \mathrm{Ker}(\mathrm{Cl}_{n(\varepsilon)} \to \mathrm{Cl}_{n_1})\}$$

(here, we consider only those $\mathfrak{a}$ prime to $M'T$) of geometric points on the product of $\#\mathcal{Q}$ copies of $\mathfrak{M}(\Gamma_{l^{2r}M',T})_{/\overline{\mathbb{F}}_p}$. It is a deep result of Hida that this subset is Zariski dense; [**H3**, Proposition 8.28] or [**H1**, Proposition 2.8]. Indeed, if we denote by V_0 the coarse moduli scheme classifying ordinary elliptic curves over $\overline{\mathbb{F}}_p$ (i.e. $V_0 =$ (affine j-line over $\overline{\mathbb{F}}_p$) $-$ (supersingular points)), there is a natural morphism $f : \mathfrak{M}(\Gamma_{l^{2r}M',T})_{/\overline{\mathbb{F}}_p} \to V_0$, "forgetting the level structure", and the resulting $f^{\#\mathcal{Q}} : \mathfrak{M}(\Gamma_{l^{2r}M',T})^{\#\mathcal{Q}}_{/\overline{\mathbb{F}}_p} \to V_0^{\#\mathcal{Q}}$ for the $\#\mathcal{Q}$-fold self-products. Since $\mathfrak{M}(\Gamma_{l^{2r}M',T})^{\#\mathcal{Q}}_{/\overline{\mathbb{F}}_p}$ is irreducible and $f^{\#\mathcal{Q}}$ is finite, our claim is equivalent to the Zariski density of $f^{\#\mathcal{Q}}(\mathcal{X})$ in $V_0^{\#\mathcal{Q}}$, which is certainly guaranteed by Hida's result mentioned above.

Since $c''_{k,\lambda,\nu}(\mathfrak{d}(\mathfrak{q})_0) \in \overline{\mathbb{F}}_p^\times$, it follows form this property that $(****)$ contradicts the following lemma, and hence completes the proof of Theorem (7.3.1).

Lemma (7.4.8). *For each $\mathfrak{q} \in \mathcal{Q}$, $\widetilde{\mathbb{H}}_{k,\lambda,\nu,\mathfrak{q}}/a^k$ is a non-constant function on $\mathfrak{M}(\Gamma_{l^{2r}M',T})_{/\overline{\mathbb{F}}_p}$.*

Proof. Since the q-expansion of a is one by (7.4.4) and the remark after (7.4.2), it is enough to show that the q-expansion of $\widetilde{\mathbb{H}}_{k,\lambda,\nu,\mathfrak{q}}$ is non-constant. For this, recall that $\widetilde{\mathbb{H}}_{k,\lambda,\nu,\mathfrak{q}}$ was defined by (7.3.3) using $\mathbb{H}_{k,\lambda,\nu}$, $\mathbb{H}_{k,\lambda,\nu}$ was defined by (7.2.6) using $\mathbb{G}_{k,\lambda}$, and the q-expansion of $\mathbb{G}_{k,\lambda}$ was given by (5.3.2).

Let

$$(\mathbb{H}_{k,\lambda,\nu})_q = \sum_n a_n q^{n/M}$$

be the q-expansion of $\mathbb{H}_{k,\lambda,\nu}$. We obtain from (3.2.2) and (3.3.8) that

$$(\mathbb{H}_{k,\lambda,\nu}|[N(\mathfrak{q})]|B_{r,i})_q = \sum_n a_n \zeta_{l^r}^{iN(\mathfrak{q})n} q^{N(\mathfrak{q})n/M}$$

with $\zeta_{l^r} = e^{2\pi i/l^r}$ (reduced modulo $\mathfrak{m}$). Thus if we write $\zeta = \zeta_{l^r}^u$ $((u,l) = 1)$, we have

$$(\widetilde{\mathbb{H}}_{k,\lambda,\nu,\mathfrak{q}})_q = \sum_n \left(\sum_{i=0}^{l^r-1} \zeta_{l^r}^{(N(\mathfrak{q})n-u)i}\right) a_n q^{N(\mathfrak{q})n/M}.$$

But by(7.2.6), $\mathbb{H}_{k,\lambda,\nu} = \sum_{\mathfrak{r}\in\mathcal{R}} c_{k,\lambda,\nu}(\mathfrak{r})\mathbb{G}_{k,\lambda}|[N(\mathfrak{r})]$ with $c_{k,\lambda,\nu}(\mathfrak{r}) \in \overline{\mathbb{F}}_p^\times$. Therefore if $N(\mathfrak{q})n \equiv u \bmod l^r$ and $n \not\equiv 0 \bmod N(\mathfrak{r})$ for $\mathfrak{r} \neq \mathfrak{o}$, the coefficient of $q^{N(\mathfrak{q})n/M}$ in $(\widetilde{\mathbb{H}}_{k,\lambda,\nu,\mathfrak{q}})_q$ is a non-zero multiple of $\sum_{n=dd'} \chi_{\mathfrak{f}}(d)\overline{\chi}_{\mathfrak{f}'}(d')d^{k-1} \in \overline{\mathbb{F}}_p$ by (5.3.2). Consequently, further assuming that n is a prime number congruent to one mod M', it is a non-zero multiple of $1+1$. Since p is odd, our claim follows. □

Part II. μ-type subgroups of $J_1(N)$.

1. Preliminaries on Iwasawa theory for imaginary quadratic fields.

1.1. p-adic L-functions.

We will use the same notation as in Part I, Section 0: We let K be an imaginary quadratic field with its ring of integers $\mathfrak{o}$. We fix an odd prime number p which splits as $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ in K. We fix an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$ such that the prime $\mathfrak{p}$ corresponds to this embedding.

We also use the following notation: If $\mathfrak{a}$ is an integral ideal of K, we set

$$K(\mathfrak{a}) := (\text{the ray class field modulo } \mathfrak{a} \text{ of } K). \tag{1.1.1}$$

We take and fix an integral ideal $\mathfrak{f}$ of K prime to $\mathfrak{p}$ and set

$$\begin{cases} \mathcal{F}_n := K(\mathfrak{f}\mathfrak{p}^n), \ \text{ for } \ n \geq 0, \\ \mathcal{F}_\infty := \bigcup_{n=0}^{\infty} \mathcal{F}_n, \\ \mathcal{G}(\mathfrak{f}) := \mathrm{Gal}(\mathcal{F}_\infty/K). \end{cases} \tag{1.1.2}$$

On the other hand, let

$$\begin{cases} K_\infty := (\text{the unique } \mathbb{Z}_p\text{-extension of } K \text{ unramified outside } \mathfrak{p}), \\ K_n := (\text{the subextension of } K_\infty/K \text{ of degree } p^n \text{ over } K), \\ \Gamma := \mathrm{Gal}(K_\infty/K), \\ \mathcal{H}(\mathfrak{f}) := \mathrm{Gal}(\mathcal{F}_\infty/K_\infty). \end{cases} \tag{1.1.3}$$

The extension $0 \to \mathcal{H}(\mathfrak{f}) \to \mathcal{G}(\mathfrak{f}) \to \Gamma \to 0$ splits, and we fix an identification isomorphism

$$\mathcal{G}(\mathfrak{f}) \cong \mathcal{H}(\mathfrak{f}) \times \Gamma. \tag{1.1.4}$$

$\mathcal{H}(\mathfrak{f})$ is isomorphic to $\mathrm{Gal}(\mathcal{F}_1/\mathcal{F}_1 \cap K_\infty)$, and we identify it with a quotient of $\mathrm{Gal}(\mathcal{F}_1/K)$ by this isomorphism.

In what follows, we will consider a grossencharacter η of (the infinity) type $(k, 0)$ $(k \in \mathbb{Z})$ of K in the terminology of de Shalit [**dS**, Chapter II, 1.1]. To be consistent with the notation of Part I, we mean by this that η is a continuous homomorphism $K_{\mathbb{A}}^\times/K^\times \to \mathbb{C}^\times$ such that $\eta(x) = x^{-k}$ for $x \in K_\infty^\times$, and denote by η^{id} the associated (quasi-)character of the group of fractional ideals of K prime to the conductor $\mathrm{cond}(\eta)$ of η. When $\mathrm{cond}(\eta)$ is a divisor of $\mathfrak{f}\mathfrak{p}^\infty$, we denote by $\eta^{\mathfrak{p}} : \mathcal{G}(\mathfrak{f}) \to \overline{\mathbb{Q}}_p^\times$ the associated p-adic Galois (quasi-)character satisfying $\eta^{\mathfrak{p}}(\mathrm{Frob}_{\mathfrak{q}}) = \eta^{\mathrm{id}}(\mathfrak{q})$ for a prime ideal $\mathfrak{q}$ of K prime to $\mathrm{cond}(\eta)\mathfrak{p}$ and a Frobenius element $\mathrm{Frob}_{\mathfrak{q}} \in \mathcal{G}(\mathfrak{f})$ at $\mathfrak{q}$.

We now quote the following theorem due to de Shalit. For references to works preceding it, see the introduction to [**dS**, Chapter II].

Theorem (1.1.5) ([**dS**, Chapter II, Theorem 4.12]). *Let $\Omega_\infty \in \mathbb{C}^\times$ be defined by Part* I, (6.1.3)*, and $\mathfrak{f}$ a non-trivial integral ideal of K prime to $\mathfrak{p}$. Then there is a p-adic unit $\Omega_p \in \mathbb{C}_p^\times$, and a p-adic integral measure $\mu(\mathfrak{f})$ on $\mathcal{G}(\mathfrak{f})$ having the following property*:

For any grossencharacter η of K of type $(k,0)$ with $k \in \mathbb{Z}$ and $k \geq 1$, and of conductor dividing $\mathfrak{f}\mathfrak{p}^\infty$, we have

$$\Omega_p^{-k} \int_{\mathcal{G}(\mathfrak{f})} \eta^{\mathfrak{p}}(\sigma) d\mu(\mathfrak{f};\sigma) = \Omega_\infty^{-k} G(\eta) \left(1 - \frac{\eta^{\mathrm{id}}(\mathfrak{p})}{p}\right) (k-1)! L^{(\mathfrak{f})}(0, \eta^{-1}). \qquad \square$$

In this theorem, $G(\eta)$ is the "like Gauss sum" defined in [**dS**, Chapter II, 4.11], and will be recalled in the next subsection. We have used the usual convention that $\eta^{\mathrm{id}}(\mathfrak{p}) = 0$ when the conductor of η is divisible by $\mathfrak{p}$, and $L^{(\mathfrak{f})}(s, \eta^{-1})$ is the Hecke L-function with the Euler factors at the primes dividing $\mathfrak{f}$ removed. The measure $\mu(\mathfrak{f})$ takes values in the ring of integers of $\mathbb{C}_p$, and the theorem especially claims that the right hand side of the above equation is algebraic and belongs to this ring. (See also the remark by Vatsal [**V**, Remark 3.8] for the right hand side.) We note that de Shalit's theorem also gives a pseudo-measure satisfying the same property as above when $\mathfrak{f} = \mathfrak{o}$. For our purpose, the case where $\mathfrak{f}$ is non-trivial suffices, and hence for simplicity, we do not touch the case $\mathfrak{f} = \mathfrak{o}$ here and below.

If we denote by R the ring generated by all $|\mathcal{H}(\mathfrak{f})|$-th roots of unity over the ring of integers of the completion of the maximal unramified extension of $\mathbb{Q}_p$, the measure $\mu(\mathfrak{f})$ actually takes values in R; $\mu(\mathfrak{f}) \in R[[\mathcal{G}(\mathfrak{f})]] = R[\mathcal{H}(\mathfrak{f})][[\Gamma]]$. Take an R-valued character χ of $\mathcal{H}(\mathfrak{f})$, which defines a ring homomorphism $R[[\mathcal{G}(\mathfrak{f})]] \twoheadrightarrow R[[\Gamma]]$. We fix a topological generator γ_0 of Γ, and by means of this, identify $R[[\Gamma]]$ with the formal power series ring $R[[T]]$ by $\gamma_0 \leftrightarrow 1 + T$. Let

$$f_{\mathfrak{f},\chi}(T) \in R[[T]] \tag{1.1.6}$$

be the power series corresponding to the image of $\mu(\mathfrak{f})$ to $R[[\Gamma]]$.

Corollary (1.1.7). *Let η be a grossencharacter of K as in* (1.1.5) *and assume that $\eta^{\mathfrak{p}}$ is of the form $\chi \times \eta^{\mathfrak{p}}_\Gamma$ according to the decomposition* (1.1.4). *Then we have*

$$f_{\mathfrak{f},\chi}(\eta^{\mathfrak{p}}_\Gamma(\gamma_0) - 1) = \Omega_p^k \cdot \Omega_\infty^{-k} G(\eta) \left(1 - \frac{\eta^{\mathrm{id}}(\mathfrak{p})}{p}\right) (k-1)! L^{(\mathfrak{f})}(0, \eta^{-1}). \qquad \square$$

The method of the construction of the measure $\mu(\mathfrak{f})$ given in [**dS**], originally due to Iwasawa, Coates and Wiles, has the following additional information on it: Let $U(\mathcal{F}_n)$ be the group of principal units of $\mathcal{F}_n \otimes_K K_{\mathfrak{p}}$, and let $U(\mathcal{F}_\infty) := \varprojlim_n U(\mathcal{F}_n)$. There is the subgroup of elliptic units $\mathcal{C}(\mathcal{F}_\infty)$ of $U(\mathcal{F}_\infty)$, [**dS**, Chapter III, 1.6].

Theorem (1.1.8) ([**dS**, Chapter III, Lemma 1.10]). *Let χ be a character of $\mathcal{H}(\mathfrak{f})$ such that* $\mathrm{cond}(\chi) = \mathfrak{g}$ *or* $\mathfrak{g}\mathfrak{p}$ *with $\mathfrak{g}$ prime to $\mathfrak{p}$ and non-trivial. Then the characteristic ideal of the* $R[[\Gamma]] \cong R[[T]]$*-module*

$$\begin{aligned}(U(\mathcal{F}_\infty)/\mathcal{C}(\mathcal{F}_\infty))_\chi &:= (U(\mathcal{F}_\infty)/\mathcal{C}(\mathcal{F}_\infty)\widehat{\otimes}_{\mathbb{Z}_p} R) \otimes_{R[[\mathcal{G}(\mathfrak{f})]],\chi} R[[\Gamma]] \\ &= (U(\mathcal{F}_\infty)/\mathcal{C}(\mathcal{F}_\infty)) \otimes_{\mathbb{Z}_p[[\mathcal{G}(\mathfrak{f})]],\chi} R[[\Gamma]]\end{aligned}$$

is generated by $f_{\mathfrak{g},\chi}$. □

Since the power series $f_{\mathfrak{g},\chi}$ depends only on χ, we will henceforth denote it by f_χ.

1.2. Comparison of special values and application.

In general, if a and b are elements of $\mathbb{C}_p^\times$, we write $a \sim b$ if a/b is a p-adic unit.

Lemma (1.2.1). *Let η be a grossencharacter of K of type $(k, 0)$ with an integer $k \geq 1$, and let e be the exact power of $\mathfrak{p}$ dividing* $\operatorname{cond}(\eta)$. *Let $\eta_\mathfrak{p}$ be the restriction of η to $\mathfrak{o}_\mathfrak{p}^\times$, and denote by the same symbol $\eta_\mathfrak{p}$ the induced Dirichlet character $(\mathbb{Z}/p^e\mathbb{Z})^\times = (\mathfrak{o}/\mathfrak{p}^e)^\times \to \overline{\mathbb{Q}}^\times$. Then we have*

$$G(\eta) \sim p^{e(k-1)} g(e^{2\pi i/p^e}, \eta_\mathfrak{p}^{-1})$$

where $g(e^{2\pi i/p^e}, \eta_\mathfrak{p}^{-1}) = \sum_{a \in (\mathbb{Z}/p^e\mathbb{Z})^\times} \eta_\mathfrak{p}^{-1}(a) e^{-2\pi i a/p^e}$ is the Gauss sum (Part I, (5.1.6)*).*

Proof. We first recall the definition of $G(\eta)$ [**dS**, Chapter II, 4.11]: We take an integral ideal $\mathfrak{f}$ of K prime to $\mathfrak{p}$ such that $\operatorname{cond}(\eta)$ is a divisor of $\mathfrak{f}\mathfrak{p}^\infty$, and $w_\mathfrak{f} :=$ (the number of units of K congruent to one modulo $\mathfrak{f}$) $= 1$. Take a grossencharacter φ of type $(1, 0)$ of conductor dividing $\mathfrak{f}$, and write $\eta = \varphi^k \xi$. ξ is thus of type $(0, 0)$ and may be considered as a Galois character. Then we have the expression $G(\eta) = (\varphi^{\mathrm{id}})^k(\mathfrak{p}^e)\xi(\mathfrak{q})\tau(\xi)$, where $\xi(\mathfrak{q})$ is a (harmless) root of unity, and

$$\tau(\xi) = \frac{1}{p^e} \sum_{\gamma \in \operatorname{Gal}(\mathcal{F}_e/\mathcal{F}_0)} \xi(\gamma) \zeta_{p^e}^{-\kappa(\gamma)}.$$

Here, $\mathcal{F}_n$ is defined by (1.1.2), ζ_{p^e} is a primitive p^e-th root of unity, and $\kappa : \operatorname{Gal}(\mathcal{F}_e/\mathcal{F}_0) \to (\mathbb{Z}/p^e\mathbb{Z})^\times$ is a Galois character giving the action on $\mathfrak{p}^e$-th division points of certain elliptic curve or a Lubin–Tate formal group. The extension $\mathcal{F}_e/\mathcal{F}_0$ is totally ramified at the primes dividing $\mathfrak{p}$, and via the Artin map $\mathfrak{o}_\mathfrak{p}^\times \twoheadrightarrow \operatorname{Gal}(\mathcal{F}_e/\mathcal{F}_0)$, κ is given by $\mathfrak{o}_\mathfrak{p}^\times \ni u \mapsto u^{-1} \bmod \mathfrak{p}^e$, cf. [**dS**, Chapter I, 1.8]. Since φ is unramified at $\mathfrak{p}$, this shows that $p^e\tau(\xi) \sim g(e^{2\pi i/p^e}, \eta_\mathfrak{p}^{-1})$, and it is clear that $(\varphi^{\mathrm{id}})^k(\mathfrak{p}^e)p^{-e} \sim p^{e(k-1)}$. □

In Part I, we considered the following situation: Let λ be a Hecke character of K such that $\lambda(x) = x^k$ for $x \in K_\infty^\times$ with an integer $k \geq 2$. Let e be the exponent of $\mathfrak{p}$ dividing the conductor $\mathfrak{c}$ of λ, and $\chi_\mathfrak{p} : (\mathbb{Z}/p^e\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$ the Dirichlet character obtained from the restriction of λ to $\mathfrak{o}_\mathfrak{p}^\times$. We then studied the following value for the twist $\lambda\varepsilon$ by a character ε of $\mathrm{Cl}_n = K_\mathbb{A}^\times / K_\infty^\times \widehat{\mathfrak{o}}_n^\times K^\times$ ($\mathfrak{o}_n = \mathbb{Z} + l^n\mathfrak{o}$) whose conductor divides a power of a prime number l prime to $p\mathfrak{c}$:

$$p^{e(k-1)}(k-1)!\, g(e^{2\pi i/p^e}, \chi_\mathfrak{p}) L^{(l)}(0, \lambda\varepsilon)/\Omega_\infty^k =: \mathcal{L}_1(\lambda\varepsilon). \tag{1.2.2}$$

Proposition (1.2.3). *Let the notation and the assumption be as above. Then the value $\mathcal{L}_1(\lambda\varepsilon)$ is algebraic and we have*

$$\mathcal{L}_1(\lambda\varepsilon) \sim \Omega_\infty^{-k} G(\eta) \left(1 - \frac{\eta^{\mathrm{id}}(\mathfrak{p})}{p}\right) (k-1)!\, L^{(\mathfrak{f})}(0, \eta^{-1}) =: \mathcal{L}_2(\lambda\varepsilon)$$

with $\eta = (\lambda\varepsilon)^{-1}$ and $\mathfrak{f} =$ (the non-$\mathfrak{p}$-part of $\mathfrak{c}$) $\times\, l^c$ with $c > 0$ such that $\operatorname{cond}(\lambda\varepsilon) \mid \mathfrak{f}\mathfrak{p}^\infty$.

Proof. We already know that $\mathcal{L}_2(\lambda\varepsilon)$ is algebraic.

It is clear that $L^{(l)}(0,\lambda\varepsilon)/\Omega_\infty^k = \Omega_\infty^{-k} L^{(\mathrm{f})}(0,\eta^{-1})$. Since we assumed that $k \geq 2$, it is also clear that $(1-\eta^{\mathrm{id}}(\mathfrak{p})/p) \sim 1$. Our claim therefore follows from (1.2.1). □

Especially, if we denote by $\mathfrak{P}$ the prime of $\overline{\mathbb{Q}}$ corresponding to $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, $\mathcal{L}_1(\lambda\varepsilon)$ and $\mathcal{L}_2(\lambda\varepsilon)$ are both $\mathfrak{P}$-integral elements of $\overline{\mathbb{Q}}$ and $\mathcal{L}_1(\lambda\varepsilon) \equiv 0 \mod \mathfrak{P}$ if and only if $\mathcal{L}_2(\lambda\varepsilon) \equiv 0 \mod \mathfrak{P}$.

We can now complete the proof of Theorem I in Part I, Section 0, which we proved under additional assumptions on λ:

(i) $e \geq \overline{e}$ (= the exponent of $\overline{\mathfrak{p}}$ dividing $\mathfrak{c}$),

(ii) $\mathfrak{c} \neq (1)$ when $k = 2$.

Now assume that λ as in that theorem is given. We can take a Hecke character μ of K of type $(0,0)$ and of conductor $\mathfrak{p}^C$, which, considered as a Galois character, factors through Γ, with C so large that $\lambda\mu$ satisfies (i) and (ii). Then for any ε as above, it follows from (1.1.7) that $\mathcal{L}_2(\lambda\varepsilon) \equiv \mathcal{L}_2(\lambda\mu\varepsilon) \mod \mathfrak{P}$. We conclude that Theorem I holds for λ if and only if it holds for $\lambda\mu$, which completes the proof.

1.3. The main conjecture proved by Rubin.

Let K and p be as in 1.1. We fix a finite abelian extension E of K, and assume:

$$\begin{cases} p \nmid |\,\mathfrak{o}^\times\,|, \\ p \nmid [E:K]. \end{cases} \tag{1.3.1}$$

Let K_∞ be the $\mathbb{Z}_p$-extension of K as in (1.1.3), and set

$$\begin{cases} E_n := EK_n \text{ for } 1 \leq n \leq \infty, \\ \Delta := \mathrm{Gal}(E/K), \\ \mathcal{G} := \mathrm{Gal}(E_\infty/K), \end{cases} \tag{1.3.2}$$

so that $\mathcal{G} \cong \Delta \times \Gamma$ with $\Gamma = \mathrm{Gal}(K_\infty/K)$. Let M_∞ be the maximal pro-p abelian extension of E_∞ unramified outside the primes above $\mathfrak{p}$, and set

$$\mathfrak{X} := \mathrm{Gal}(M_\infty/E_\infty). \tag{1.3.3}$$

It is a module over $\mathbb{Z}_p[[\mathcal{G}]] \cong \mathbb{Z}_p[\Delta][[\Gamma]]$. On the other hand, let $U(E_\infty) := \varprojlim_n U(E_n)$ be defined as in 1.1, and $\mathcal{C}(E_\infty)$ its subgroup of elliptic units as defined in Rubin [**Ru1**, Section 1, Section 4].

For a $\mathbb{Z}_p[\Delta]$-module Y and an irreducible $\mathbb{Z}_p$-representation χ_0 of Δ, we denote by Y^{χ_0} the χ_0-isotypic component of Y. Since $|\,\Delta\,|$ is prime to p, it is a direct summand of Y. The following is the "main conjecture" proved by Rubin in the case under our consideration:

Theorem (1.3.4) ([**Ru2**, Theorem 2, (i)]). *For any irreducible $\mathbb{Z}_p$-representation χ_0 of Δ, $\mathfrak{X}^{\chi_0}$ and $(U(E_\infty)/\mathcal{C}(E_\infty))^{\chi_0}$ are finitely generated torsion $\mathbb{Z}_p[\Delta]^{\chi_0}[[\Gamma]]$-modules, and they have the same characteristic ideal.* □

Let $\mathfrak{f}$ be the non-$\mathfrak{p}$-part of the conductor of the extension E/K. By our assumption (1.3.1), $E \subseteq \mathcal{F}_1 = K(\mathfrak{f}\mathfrak{p})$, $E_\infty \subseteq \mathcal{F}_\infty = K(\mathfrak{f}\mathfrak{p}^\infty)$, and Δ is a quotient of $\mathcal{H}(\mathfrak{f})$ in the notation of 1.1. Let χ be an R-valued character of Δ, R being as in 1.1. We can then consider $(U(\mathcal{F}_\infty)/\mathcal{C}(\mathcal{F}_\infty))_\chi$ and $(U(E_\infty)/\mathcal{C}(E_\infty))_\chi$ as in (1.1.8). It is straightforward to see that these $R[[\Gamma]]$-modules are pseudo-isomorphic, and we obtain from (1.3.4) and (1.1.8) the following:

Theorem (1.3.5). *Let the notation be as above and assume that the non-$\mathfrak{p}$-part of* $\mathrm{cond}(\chi)$ *is not $\mathfrak{o}$. Then the characteristic ideal of the* $R[[\Gamma]]$*-module $\mathfrak{X}_\chi$ is generated by f_χ.* □

2. An anticyclotomic analogue of a theorem of Washington.

2.1. Statement of the result.

As is well-known, Washington [**W**] proved the following theorem: Let k be an abelian number field, and K the cyclotomic $\mathbb{Z}_l$-extension of k. Let p be a prime number different from l. Then for any finite subextension k' of K/k, the order of the p-Sylow subgroup of the ideal class group of k' is bounded independently of k'. Washington deduced this theorem from a result on the non-vanishing modulo p of the Dirichlet L-values under twists by l-cyclotomic characters. Later, Sinnott [**Si**] gave a more transparent proof of this latter result, and it was a prototype of the far-reaching theorem of Hida which we have to some extent generalized in Part I. Although the original theorem of Washington is an easy consequence of the non-vanishing modulo p result by virtue of the analytic class number formula, its analogue for the anticyclotomic situation is not. It is an idea of Vatsal to use the main conjecture to deduce an analogue of Washington's theorem from the non-vanishing result, cf. [**V**, Section 3]. We thus follow his idea to prove Theorem (2.1.6) below; and further use it to obtain results on the μ-type subgroups of $J_1(N)$ in the subsequent sections always following Vatsal's method.

Throughout this section, we use the following notation: K is an imaginary quadratic field, and $\mathfrak{o}$ is its ring of integers. We assume that

$$\mathfrak{o}^\times = \{\pm 1\}. \tag{2.1.1}$$

We fix an odd prime number p which splits in K, and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ as in 1.1.

We also fix an odd prime number l different from p and unramified in K. We assume that

$$\begin{cases} (l-1,p) = 1 & \text{if } l \text{ splits in } K, \\ (l+1,p) = 1 & \text{if } l \text{ remains prime in } K. \end{cases} \tag{2.1.2}$$

We set

$$\begin{cases} H_n := (\text{the ring class field of } K \text{ of conductor } l^n),\ n \geq 0, \\ H_\infty := \displaystyle\bigcup_{n=0}^{\infty} H_n. \end{cases} \tag{2.1.3}$$

Especially H_0 is the Hilbert class field of K. The Galois group $\mathrm{Gal}(H_n/K)$ is canonically isomorphic to the group of proper $\mathfrak{o}_n$-ideal classes Cl_n, and the p-part of its order is independent of n, under (2.1.1) and (2.1.2); cf. Part I, (4.1.2).

Now take an extension $\widetilde{H}_0$ of H_0 satisfying

$$\begin{cases} \widetilde{H}_0 \text{ is finite and abelian over } K, \\ \widetilde{H}_0/K \text{ is unramified at the primes above } l, \\ \text{primes that ramify in } \widetilde{H}_0/K \text{ are split primes for } K/\mathbb{Q}, \\ [\widetilde{H}_0 : H_0] \text{ is prime to } p, \end{cases} \tag{2.1.4}$$

and set

$$\widetilde{H}_n := H_n\widetilde{H}_0 \text{ for } 0 \leq n \leq \infty. \tag{2.1.5}$$

The purpose of this section is to prove the following theorem. When $\widetilde{H}_0 = H_0$, it has been proved by Vatsal [**V**, Proposition 3.19]:

Theorem (2.1.6). *Let the notation and the assumption be as above. We especially assume* (2.1.4) *for* $\widetilde{H}_0$. *Let* $\widetilde{H}_n^{\mathrm{ur}}$ *be the maximal unramified abelian* (*pro-*)*p-extension of* $\widetilde{H}_n$ *for* $0 \leq n \leq \infty$. *Then there is a non-negative integer* n_0 *such that* $\widetilde{H}_n^{\mathrm{ur}} = \widetilde{H}_{n_0}^{\mathrm{ur}}\widetilde{H}_n$ *for all* $n \geq n_0$. *Especially* $\widetilde{H}_\infty^{\mathrm{ur}}$ *is a finite extension of* $\widetilde{H}_\infty$.

The following corollaries are consequences of this theorem:

Corollary (2.1.7). *Let* Σ *be a finite set of primes of* K *satisfying*:

$$\begin{cases} \textit{each prime in } \Sigma \textit{ is a split prime for } K/\mathbb{Q}, \\ \Sigma \textit{ does not contain primes above } p. \end{cases}$$

Let $\mathcal{M}_\infty^\Sigma$ *be the maximal abelian pro-p extension of* $\widetilde{H}_\infty$ *unramified outside* Σ. *Then* $\mathrm{Gal}(\mathcal{M}_\infty^\Sigma/\widetilde{H}_\infty)$ *is a finitely generated* $\mathbb{Z}_p$*-module.*

Proof. See [**V**, Theorem 3.20]. The points are:

(i) primes in Σ are finitely decomposed in H_∞ and hence in $\widetilde{H}_\infty$,

(ii) for each prime $\widetilde{\mathfrak{q}}$ of $\widetilde{H}_\infty$ lying over a prime in Σ, the inertia group of $\widetilde{\mathfrak{q}}$ in $\mathrm{Gal}(\mathcal{M}_\infty^\Sigma/\widetilde{H}_\infty)$ is pro-cyclic. □

Corollary (2.1.8). *Fix an integer* $r \geq 1$. *Let* $\widetilde{L}_n$ *be the composite of all abelian extensions of* $\widetilde{H}_n$ *which are unramified outside* Σ *and of degree dividing* p^r. *Then each* $\widetilde{L}_n$ *is finite over* $\widetilde{H}_n$, *and there is a non-negative integer* n_1 *such that* $\widetilde{L}_n = \widetilde{L}_{n_1}\widetilde{H}_n$ *for all* $n \geq n_1$. □

2.2. Reduction of the proof.

We follow the argument of [**V**, Section 3].

Lemma (2.2.1). *In general, let* K *be a finite extension of* $\mathbb{Q}$, *and let* F *and* F' *be* *finite abelian extensions of K such that $F' \supseteq F$. Let Δ (resp. Δ') be the Galois group of F/K (resp. F'/K). Let p be a prime number, and assume that $p \nmid [F' : K]$. Take an irreducible $\mathbb{Z}_p$-representation χ_0 of Δ, and consider it also as a representation of Δ'.*

(1) *Let A (resp. A') be the p-Sylow subgroup of the ideal class group of F (resp. F'). Then the norm map induces an isomorphism*

$$A'^{\chi_0} \xrightarrow{\sim} A^{\chi_0}.$$

(2) *Let K_∞ be a $\mathbb{Z}_p$-extension of K with $\Gamma = \mathrm{Gal}(K_\infty/K)$, and set $F_\infty := FK_\infty$ and $F'_\infty := F'K_\infty$. Fix a set P consisting of primes of K dividing p. Let $\mathcal{N}$ (resp. $\mathcal{N}'$) be the maximal abelian pro-p extension of F_∞ (resp. F'_∞) unramified outside the primes lying above P. Thus $\mathfrak{X} := \mathrm{Gal}(\mathcal{N}/F_\infty)$ (resp. $\mathfrak{X}' := \mathrm{Gal}(\mathcal{N}'/F'_\infty)$) is a module over $\mathbb{Z}_p[\Delta][[\Gamma]]$ (resp. $\mathbb{Z}_p[\Delta'][[\Gamma]]$). The restriction map induces an isomorphism*

$$\mathfrak{X}'^{\chi_0} \xrightarrow{\sim} \mathfrak{X}^{\chi_0}$$

of $\mathbb{Z}_p[\Delta]^{\chi_0}[[\Gamma]]$-modules.

Proof. This must be more or less well-known. We outline the proof of (1) for completeness.

Let L_0 be the maximal abelian subextension of L'/F. We first claim that $L_0 = LF'$. Let L'' be the maximal sub-p-extension of L_0/F. Then it is everywhere unramified since the ramification index of any prime in L'/F is prime to p. It follows that $L'' = L$ and $L_0 = LF'$.

We can identify $\mathrm{Gal}(L'/F')$ with A' as $\mathrm{Gal}(F'/F)$-modules by class field theory. The exact sequence

$$0 \to \mathrm{Gal}(L'/F') \to \mathrm{Gal}(L'/F) \to \mathrm{Gal}(F'/F) \to 0$$

splits, and hence we can identify the commutator subgroup of $\mathrm{Gal}(L'/F)$ with the submodule D of A' generated by all $(\delta - 1)x$ ($\delta \in \mathrm{Gal}(F'/F)$, $x \in A'$). Consequently, the first claim implies that $A'/D \xrightarrow{\sim} A$, from which our assertion follows. □

We now return to the situation considered in 2.1, and set

$$\begin{cases} \widetilde{G}_n := \mathrm{Gal}(\widetilde{H}_n/K), \\ G_n := \mathrm{Gal}(H_n/K), \end{cases} \tag{2.2.2}$$

for non-negative integers n. Since the extension H_∞/H_0 ramifies totally at the primes dividing l, it follows from the second condition in (2.1.4) that

$$H_\infty \cap \widetilde{H}_0 = H_0 \tag{2.2.3}$$

so that

$$|\,\widetilde{G}_n\,| = |\,G_n\,| \cdot [\widetilde{H}_0 : H_0] = |\,\mathrm{Cl}_n\,| \cdot [\widetilde{H}_0 : H_0]. \tag{2.2.4}$$

Therefore, under (2.1.4), the p-Sylow subgroups of $\widetilde{G}_n$ and G_n have the same order which is independent of n. The natural surjections $\widetilde{G}_m \twoheadrightarrow \widetilde{G}_n$, $G_m \twoheadrightarrow G_n$ and $\widetilde{G}_n \twoheadrightarrow G_n$ induce isomorphisms on their p-Sylow subgroups for all $m \geq n$. We identify these p-Sylow subgroups and denote it simply by $\mathfrak{d}$. Set

$$\begin{cases} F_n := \widetilde{H}_n^{\mathfrak{d}} : \text{the fixed field of } \mathfrak{d} < \widetilde{G}_n, \\ \mathfrak{g}_n := \mathrm{Gal}(F_n/K). \end{cases} \tag{2.2.5}$$

Thus the order of $\mathfrak{g}_n$ is prime to p, and we have the canonical isomorphism

$$\widetilde{G}_n \cong \mathfrak{d} \times \mathfrak{g}_n \tag{2.2.6}$$

through which we identify the both sides.

Let A_n (resp. B_n) be the p-Sylow subgroup of the ideal class group of F_n (resp. $\widetilde{H}_n$). It is a module over $\mathbb{Z}_p[\mathfrak{g}_n]$ (resp. $\mathbb{Z}_p[\widetilde{G}_n]$). When χ_0 is an irreducible $\mathbb{Z}_p$-representation of $\mathfrak{g}_n$, we may consider it also as representations of $\mathfrak{g}_m$ and $\widetilde{G}_m$ for all $m \geq n$.

Lemma (2.2.7). *Let χ_0 be an irreducible $\mathbb{Z}_p$-representation of $\mathfrak{g}_n$ as above. Then the norm maps induce the following isomorphisms*

$$\begin{cases} A_m^{\chi_0} \overset{\sim}{\to} A_n^{\chi_0}, \\ B_m^{\chi_0} \overset{\sim}{\to} B_n^{\chi_0} \end{cases}$$

for all $m \geq n$.

Proof. Apply (2.2.1) to the situations $F_m/F_n/K$ and $\widetilde{H}_m/\widetilde{H}_n/\widetilde{H}_n^{\mathfrak{g}_n}$. □

Proposition (2.2.8). *Let χ_0 be an irreducible $\mathbb{Z}_p$-representation of $\mathfrak{g}_n$. Then for any $m \geq n$, if $B_m^{\chi_0}$ is non-trivial, $A_m^{\chi_0}$ is also non-trivial.*

Proof. It is enough to treat the case $m = n$ by the previous lemma.

Assume that $B_n^{\chi_0} \neq \{0\}$. By class field theory, there corresponds an unramified extension H' of $\widetilde{H}_n$ such that $\mathrm{Gal}(H'/\widetilde{H}_n)$ is isomorphic to $B_n^{\chi_0}$ as a module over $\widetilde{G}_n = \mathfrak{d} \times \mathfrak{g}_n$. Since $\mathfrak{d}$ is a p-group, the maximal quotient of $\mathrm{Gal}(H'/\widetilde{H}_n)$ on which $\mathfrak{d}$ acts trivially is non-trivial. Let L' be the extension of $\widetilde{H}_n$ corresponding to this quotient.

Take a cyclic subgroup P of $\mathfrak{d}$, and let H_n' be its fixed subfield; $\widetilde{H}_n \supseteq H_n' \supseteq F_n$. Then since $\mathrm{Gal}(L'/\widetilde{H}_n)$ is central in $\mathrm{Gal}(L'/F_n)$, L'/H_n' is an abelian extension. On the other hand, we claim that $\widetilde{H}_n/F_n$ is unramified. Indeed, since $[H_n : H_0]$ is prime to p, the ramification index of any prime in the extension H_n/K is prime to p. Thus $H_n/H_n^{\mathfrak{d}}$, and hence $\widetilde{H}_n = F_n H_n/F_n$ also, is unramified. Consequently, L'/H_n' is also unramified. It follows that the χ_0-isotypic component of the p-Sylow subgroup of the ideal class group of H_n' is non-trivial.

Starting from this H_n' and repeating the above argument, we arrive at our conclusion. □

2.3. End of the proof of (2.1.6).

First set

$$\begin{cases} F_\infty := \bigcup_{n\geq 0} F_n, \ \mathfrak{g}_\infty := \mathrm{Gal}(F_\infty/K), \\ \widehat{\mathfrak{g}}_n := \mathrm{Hom}(\mathfrak{g}_n, \overline{\mathbb{Q}}_p^\times), \text{ the set of } \overline{\mathbb{Q}}_p^\times\text{-valued characters of } \mathfrak{g}_n, \\ \widehat{\mathfrak{g}}_\infty := \varinjlim_n \widehat{\mathfrak{g}}_n, \\ \widehat{\mathfrak{g}}_n^0 := (\text{the set of irreducible } \mathbb{Z}_p\text{-representations of } \mathfrak{g}_n), \\ \widehat{\mathfrak{g}}_\infty^0 := \varinjlim_n \widehat{\mathfrak{g}}_n^0. \end{cases} \tag{2.3.1}$$

Thus each element of $\widehat{\mathfrak{g}}_\infty^0$ may be identified with the $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbit of an element of $\widehat{\mathfrak{g}}_\infty$. For an element χ (resp. χ_0) of $\widehat{\mathfrak{g}}_\infty$ (resp. $\widehat{\mathfrak{g}}_\infty^0$), we write $n(\chi)$ (resp. $n(\chi_0)$) for the minimal integer n such that χ (resp. χ_0) belongs to $\widehat{\mathfrak{g}}_n$ (resp. $\widehat{\mathfrak{g}}_n^0$).

By virtue of (2.2.7) and (2.2.8), (2.1.6) is now a consequence of the following:

Theorem (2.3.2). *We have*

$$A_n^{\chi_0} = \{0\} \text{ for } n \geq n(\chi_0)$$

for all but finitely many $\chi_0 \in \widehat{\mathfrak{g}}_\infty^0$.

Now let K_∞/K be as in (1.1.3), and let

$$\begin{cases} F_{n,\infty} := F_n K_\infty, \\ M_{n,\infty} := (\text{the maximal abelian pro-}p\text{ extension of } F_{n,\infty}, \\ \qquad\qquad \text{unramified outside the primes above } \mathfrak{p}), \\ \mathfrak{X}_n := \mathrm{Gal}(M_{n,\infty}/F_{n,\infty}). \end{cases} \tag{2.3.3}$$

Thus $\mathfrak{X}_n$ is a module over $\mathbb{Z}_p[\mathfrak{g}_n][[\Gamma]]$.

Lemma (2.3.4). *Let* $\widehat{\mathfrak{g}}_\infty^0 \ni \chi_0$ *be non-trivial. For* $n \geq n(\chi_0)$*, if the characteristic ideal of the* $\mathbb{Z}_p[\mathfrak{g}_n]^{\chi_0}[[\Gamma]]$*-module* $\mathfrak{X}_n^{\chi_0}$ *is trivial, then* $A_n^{\chi_0}$ *vanishes.*

Proof. First note that $\mathfrak{X}_n^{\chi_0}$ is independent of $n \geq n(\chi_0)$ by (2.2.1), (2).

Since $\mathfrak{X}_n^{\chi_0}$ has no non-zero finite submodule by Greenberg [**Gre**, Section 4], the assumption implies that $\mathfrak{X}_n^{\chi_0} = \{0\}$. But if $A_n^{\chi_0} \neq \{0\}$, there is a non-trivial abelian unramified p-extension L_n of F_n such that $\mathfrak{g}_n$ acts via χ_0 on $\mathrm{Gal}(L_n/F_n)$. Since $F_{n,\infty}$ is abelian over K, the action of $\mathfrak{g}_n$ on $\mathrm{Gal}(F_{n,\infty}/F_n)$ is trivial. This implies that $L_nF_{n,\infty}/F_{n,\infty}$ is non-trivial and hence $\mathfrak{X}_n^{\chi_0} \neq \{0\}$. □

For each non-negative integer n, we can apply the consideration in 1.3 for F_n in place of E there. Take $\chi_0 \in \widehat{\mathfrak{g}}_n^0$ and let $\chi \in \widehat{\mathfrak{g}}_n$ be one of its absolutely irreducible component. Then the main conjecture proved by Rubin, in the form (1.3.5), asserts that the characteristic ideal of $\mathfrak{X}_{n,\chi}$, the base extension of $\mathfrak{X}_n^{\chi_0}$ by $\mathbb{Z}_p[\mathfrak{g}_n]^{\chi_0}[[\Gamma]] \xrightarrow{\chi} R[[\Gamma]]$, is generated by the power series f_χ giving the p-adic L-function whenever $\mathrm{cond}(\chi) \neq \mathfrak{o}, \mathfrak{p}$. Thus finally (2.3.2) follows from the following:

Theorem (2.3.5). *f_χ is a unit power series for all but finitely many $\chi \in \widehat{\mathfrak{g}}_\infty$ with* $\mathrm{cond}(\chi) \neq \mathfrak{o}$*,* $\mathfrak{p}$*.*

Proof. Recall that $\mathfrak{d}$ is the (common) p-Sylow subgroup of $\widetilde{G}_n$ and G_n, and $F_n \supseteq H_n^{\mathfrak{d}}$. The quotient homomorphism $\mathfrak{g}_n \to \mathfrak{g}_0$ induces an isomorphism $\mathrm{Gal}(F_n/H_n^{\mathfrak{d}}) \to \mathrm{Gal}(F_0/H_0^{\mathfrak{d}})$ for each $n \geq 0$. Indicating by "$\widehat{\ }$" the group of $\overline{\mathbb{Q}}_p^\times$-valued characters again, we have the commutative diagram:

$$\begin{tikzcd}
0 & \mathrm{Gal}(F_n/H_n^{\mathfrak{d}})^\frown \arrow[l] & \widehat{\mathfrak{g}}_n \arrow[l] & \mathrm{Gal}(H_n^{\mathfrak{d}}/K)^\frown \arrow[l] & 0 \arrow[l] \\
0 & \mathrm{Gal}(F_0/H_0^{\mathfrak{d}})^\frown \arrow[l] \arrow[u, "\wr"'] & \widehat{\mathfrak{g}}_0 \arrow[l] \arrow[u] & \mathrm{Gal}(H_0^{\mathfrak{d}}/K)^\frown \arrow[l] \arrow[u] & 0 \arrow[l]
\end{tikzcd}$$

with injective vertical maps. Let $\varphi_1, \ldots, \varphi_h \in \widehat{\mathfrak{g}}_0$ be the complete set of representatives of $\mathrm{Gal}(F_0/H_0^{\mathfrak{d}})^\frown$, and consider them also as elements of $\widehat{\mathfrak{g}}_n$. We have

$$\widehat{\mathfrak{g}}_n = \{\varphi_i \varepsilon \mid 1 \leq i \leq h,\ \varepsilon \in \mathrm{Gal}(H_n^{\mathfrak{d}}/K)^\frown\}.$$

Each element of $\widehat{\mathfrak{g}}_n$ takes values in $\overline{\mathbb{Q}}$ and hence may be considered as a Hecke character of K of finite order by class field theory. Note that, under (2.1.4), the conductor of each φ_i is prime to l, and the primes dividing it are split primes for $K/\mathbb{Q}$.

Under (2.1.1), there exists a grossencharacter of type $(2, 0)$ and of conductor $\mathfrak{o}$ of K. We take and fix its positive power ξ such that the associated Galois representation $\xi^{\mathfrak{p}}$ factors through $\Gamma = \mathrm{Gal}(K_\infty/K)$. Let $(k, 0)$ be its type.

Now fix φ_i and consider $\chi = \varphi_i \varepsilon \in \widehat{\mathfrak{g}}_\infty$. To prove the theorem, we may exclude finite number of ε of conductor $\mathfrak{o}$, and hence we assume that $\mathrm{cond}(\varepsilon) \neq \mathfrak{o}$. Then we have

$$f_\chi(\xi^{\mathfrak{p}}(\gamma_0) - 1) = \Omega_p^k \mathcal{L}_2(\lambda\varepsilon^{-1})$$

with $\lambda := (\xi\varphi_i)^{-1}$ by (1.1.7), where we used the notation as in (1.2.3). The same proposition (1.2.3) asserts that this value is a p-adic unit if and only if so is the value $\mathcal{L}_1(\lambda\varepsilon^{-1})$. But for the fixed λ, the main result Theorem I of Part I, Section 0 asserts that, when ε moves over the characters of $\mathrm{Gal}(H_n^{\mathfrak{d}}/K)$ ($\twoheadleftarrow \mathrm{Gal}(H_n/K)$) for all $n \geq 0$, this value is a p-adic unit except for a finite number of ε. This completes the proof. □

3. Supersingular reduction of CM points.

3.1. Review of the case of $X_0(M)$.

In the argument of Vatsal, one of the important points is the surjectivity of the supersingular reduction of certain CM points (or Heegner points) on $X_0(M)$, cf. [**V**, 4.6]. This is due to Vatsal and Cornut, and we first recall this result following Cornut [**C**].

For a positive integer M, we denote by $X_0(M)$ the usual modular curve over $\mathbb{Q}$ attached to $\Gamma_0(M)$. It has the natural model $X_0(M)_{/\mathbb{Z}[1/M]}$ proper and smooth over $\mathbb{Z}[1/M]$, and for any $\mathbb{Z}[1/M]$-algebra R, we denote by $X_0(M)_{/R}$ its base extension to R.

As in previous sections, we take and fix an imaginary quadratic field K with its ring of integers $\mathfrak{o}$. We again assume that

$$\mathfrak{o}^\times = \{\pm 1\}. \tag{3.1.1}$$

We fix a positive integer M whose prime factors are all split primes for $K/\mathbb{Q}$, and also an integral ideal $\mathfrak{m}$ of K satisfying

$$\mathfrak{o}/\mathfrak{m} \cong \mathbb{Z}/M\mathbb{Z}. \tag{3.1.2}$$

We start with a fixed elliptic curve E over $\mathbb{C}$ having complex multiplication by $\mathfrak{o}$; $\mathrm{End}(E) \cong \mathfrak{o}$, the isomorphism being normalized so that the associated representation of $\mathfrak{o}$ on $\mathrm{Lie}(E)$ gives the inclusion $\mathfrak{o} \hookrightarrow \mathbb{C}$. Let

$$C := E(\mathbb{C})[\mathfrak{m}] \tag{3.1.3}$$

be a cyclic subgroup of $E(\mathbb{C})$ of order M.

On the other hand, fix a prime number l prime to M. As in (2.1.3) we denote by H_n the ring class field of K of conductor l^n, and set $H_\infty := \bigcup_{n=0}^\infty H_n$. Let

$$\mathcal{L}_l := (\text{the set of cyclic subgroups of } E(\mathbb{C}) \text{ of order some power of } l) \tag{3.1.4}$$

and define

$$\mathcal{H} : \mathcal{L}_l \to X_0(M)(H_\infty) \text{ by } \mathcal{H}(X) := [E/X \to E/(X+C)]. \tag{3.1.5}$$

Here the brackets indicate the isomorphism class of the cyclic M-isogeny in it. It is well-known that this indeed defines a point of $X_0(M)$ with values in some H_n, a CM point (or a Heegner point), for which we use the same symbol $\mathcal{H}(X)$.

Take a prime number q which is prime to lM and remains prime in K, and a prime $\mathfrak{Q}$ of H_∞ above q. The residue field of $\mathfrak{Q}$ is $\mathbb{F}_{q^2}$, the finite field with q^2 elements. We have the "reduction modulo $\mathfrak{Q}$ map"

$$\mathrm{red}_q : X_0(M)(H_\infty) \to X_0(M)_{/\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}). \tag{3.1.6}$$

More generally, let V be a discrete valuation ring of mixed characteristic $(0,q)$ with the quotient field $\mathfrak{K}$ (resp. the residue field k). Then through the bijection $X_0(M)(\mathfrak{K}) \cong X_0(M)_{/\mathbb{Z}[1/M]}(V)$ (the valuative criterion of properness), we obtain the reduction map $X_0(M)(\mathfrak{K}) \to X_0(M)_{/\mathbb{Z}[1/M]}(k)$. If a cyclic M-isogeny $\mathcal{C}$ between elliptic curves over $\mathfrak{K}$ is given and if it extends to $\mathcal{C}_V$ over V, this reduction map sends the point of $X_0(M)(\mathfrak{K})$ corresponding to $\mathcal{C}$ to the point of $X_0(M)_{/\mathbb{Z}[1/M]}(k)$ corresponding to $\mathcal{C}_V \otimes_V k$. Thus, by our assumption on q, the image of $\mathcal{H}(X)$ under red_q is a point of the supersingular locus $X_0^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}$ of $X_0(N)_{/\mathbb{F}_{q^2}}$. The result of Vatsal and Cornut referred to above can now be stated as follows:

Theorem (3.1.7). *The composite map*

$$\mathrm{red}_q \circ \mathcal{H} : \mathcal{L}_l \to X_0^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}) = X_0^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}(\overline{\mathbb{F}}_q)$$

is surjective.

As is well-known, points of $X_0^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}$ are all rational over $\mathbb{F}_{q^2}$, and hence the last equality holds. Actually in [**C**], much more general results are proven, and the above statement is a very particular case of Theorem 3.1 or Corollary 3.2 in [**C**]. Although the proof of these results requires a theorem of Ratner in ergodic theory, only the commutativity of the diagram in [**C**, 3.4] (with $\mathcal{R} = \{1\}$ and $S = \{\text{one prime}\}$) suffices for (3.1.7).

3.2. The case of $X_1(M)$.

We keep the notation of 3.1.

We henceforth denote by $X_1(M)$ the modular curve over $\mathbb{Q}$ attached to $\Gamma_1(M)$, of which the cusp at infinity is rational over $\mathbb{Q}$. It is the generic fibre of the curve $X_1(M)_{/\mathbb{Z}[1/M]}$ proper and smooth over $\mathbb{Z}[1/M]$, which is the smooth compactification of the moduli scheme classifying pairs (E, α) consisting of an elliptic curve E and a closed immersion $\alpha : \boldsymbol{\mu}_M \hookrightarrow E[M]$ (rather than $\mathbb{Z}/M\mathbb{Z} \hookrightarrow E[M]$) of group schemes over $\mathbb{Z}[1/M]$-schemes. We use the notation $X_1(M)_{/R}$ in the same sense as $X_0(M)_{/R}$.

Let X be an element of $\mathcal{L}_l$, and consider the elliptic curve E/X. $\mathrm{End}(E/X)$ is isomorphic to the order $\mathfrak{o}_n = \mathbb{Z} + l^n\mathfrak{o}$ of conductor l^n for some n. $\mathfrak{m}' := \mathfrak{m} \cap \mathfrak{o}_n$ is then a proper $\mathfrak{o}_n$-ideal, and $(X + C)/X = (E/X)[\mathfrak{m}'](\mathbb{C})$ is cyclic of order M. Giving the data $E/X \to E/(X+C)$ considered in the previous subsection is equivalent to giving the pair $(E/X, (E/X)[\mathfrak{m}'])$.

Lemma (3.2.1). *Let the notation be as above. The residue field of the point $\mathcal{H}(X)$ of $X_0(M)$ generates H_n over K. Let $\mathcal{H}_1(X)$ be any one of the point of $X_1(M)$ lying over $\mathcal{H}(X)$. Then the residue field of $\mathcal{H}_1(N)$ generates over K the field $H_nK(\overline{\mathfrak{m}})$, $K(\overline{\mathfrak{m}})$ being the ray class field of K modulo $\overline{\mathfrak{m}}$*; (1.1.1).

Proof. We only prove the assertion for $\mathcal{H}_1(X)$, because that for $\mathcal{H}(X)$ is well-known and simpler. From the above remark, $\mathcal{H}_1(X)$ corresponds to a pair $(E/X, \alpha : \boldsymbol{\mu}_M \xrightarrow{\sim} (E/X)[\mathfrak{m}'])$, and the residue field of $\mathcal{H}_1(X)$ is the field of moduli of this pair. But it is also the field of moduli of $(E/X, \mathbb{Z}/M\mathbb{Z} \xrightarrow{\sim} (E/X)[\overline{\mathfrak{m}'}])$ obtained from it by the Cartier duality, and hence that of the pair $(E/X, P)$ where P is a generator of the cyclic group $(E/X)[\overline{\mathfrak{m}'}](\mathbb{C})$. As we assumed (3.1.1), it is given by $\mathbb{Q}(j_{(E/X)}, h^1_{(E/X)}(P))$ in the notation of [**Shi1**, 4.5], and our conclusion follows from [**Shi1**, Theorem 5.5]. (One can also deduce this directly from the main theorem of complex multiplication [**Shi1**, Theorem 5.4].) □

Now set

$$H_n' := H_nK(\overline{\mathfrak{m}}) \text{ for } 0 \leq n \leq \infty. \tag{3.2.2}$$

Let $X_0(M)(H_\infty)^{\mathrm{CM}}$ be the image of $\mathcal{L}_l$ under (3.1.5). Each point of $X_1(M)$ lying above a point in this set is rational over H_∞' by the previous lemma, and we set

$$X_1(M)(H_\infty')^{\mathrm{CM}} := (\text{the inverse image of } X_0(M)(H_\infty)^{\mathrm{CM}} \text{ in } X_1(M)). \tag{3.2.3}$$

Take a rational prime q not dividing lM which remains prime in K and splits completely in $K(\overline{\mathfrak{m}})/K$. (Let $K'/\mathbb{Q}$ be the Galois closure of $K(\overline{\mathfrak{m}})/\mathbb{Q}$. There are infinitely many prime numbers q unramified in $K'/\mathbb{Q}$ such that the Frobenius element of some extension of q for $K'/\mathbb{Q}$ is the complex conjugation, by Čebotarev density theorem. Any such $q \nmid lM$ works.) Thus q also splits completely in H'_∞/K. Let $\mathfrak{Q}'$ be a prime of H'_∞ above $\mathfrak{Q}$. We obtain the reduction modulo $\mathfrak{Q}'$ map

$$\mathrm{red}'_q : X_1(M)(H'_\infty) \to X_1(M)_{/\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}) \tag{3.2.4}$$

as in the previous subsection.

Proposition (3.2.5). *Take q as above. Then we have $X_1^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}) = X_1^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}(\overline{\mathbb{F}}_q)$, the superscript "ss" meaning the supersingular locus again. The reduction map* (3.2.4) *induces a surjection*

$$X_1(M)(H'_\infty)^{\mathrm{CM}} \twoheadrightarrow X_1^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}).$$

Proof. Take a point $x \in X_1^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}(\overline{\mathbb{F}}_q)$. By (3.1.7), its image to $X_0^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}(\overline{\mathbb{F}}_q) = X_0^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}(\mathbb{F}_{q^2})$ is of the form $\mathrm{red}_q(\mathcal{H}(X))$. There is a finite extension $\mathfrak{K}$ of K such that the M-isogeny giving $\mathcal{H}(X)$ is defined over $\mathfrak{K}$. Take a prime of $\mathfrak{K}H'_\infty$ above $\mathfrak{Q}'$, and let V be the valuation ring of its restriction to $\mathfrak{K}$. Taking $\mathfrak{K}$ large enough, we may assume that the above M-isogeny extends to $(E/X)_V \to (E/(X+C))_V$ over V, and further that $(E/X)_V[\overline{\mathfrak{m}'}]$ is a constant group scheme over V, since q is prime to M. Then it follows from the argument of the proof of (3.2.1) that the given point x lifts to $\mathcal{H}_1(X) \in X_1(M)(\mathfrak{K}) = X_1(M)_{/\mathbb{Z}[1/M]}(V)$ above $\mathcal{H}(X)$, which actually belongs to $X_1(M)(H'_\infty)$ by (3.2.1). We thus have $x = \mathrm{red}'_q(\mathcal{H}_1(X))$. □

Remark (3.2.6). We have seen that all supersingular points of $X_1(M)_{/\mathbb{F}_{q^2}}$ are rational over $\mathbb{F}_{q^2}$ under our choice of q. This is in fact an instance of the common feature of Ihara's model of modular curves over finite fields [**I**].

In general, let q be a prime number and n a positive integer not divisible by q. Let $X(n)_{/\mathbb{Z}[1/n]}$ be the compactification of the modular curve classifying pairs consisting of an elliptic curve E together with an isomorphism $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} E[n]$ (i.e. $\Gamma(n)^{\mathrm{naive}}$-curves in the terminology of Part I, (1.1.1)) over $\mathbb{Z}[1/n]$-schemes. There is a natural morphism $X(n)_{/\mathbb{Z}[1/n]} \to \boldsymbol{\mu}_n^{\mathrm{prim}}$ to the scheme of primitive n-th roots of unity. Consider the base extension from $\mathbb{Z}$ to $\mathbb{F}_q$:

$$X(n)_{/\mathbb{F}_q} \to \boldsymbol{\mu}_n^{\mathrm{prim}}{}_{/\mathbb{F}_q} \to \mathrm{Spec}(\mathbb{F}_q).$$

Fix a primitive n-th root of unity $\zeta_n \in \overline{\mathbb{F}}_q$. This defines a morphism $\mathrm{Spec}(\mathbb{F}_q(\zeta_n)) \to \boldsymbol{\mu}_n^{\mathrm{prim}}{}_{/\mathbb{F}_q}$, and we let $X(n)^{(\zeta_n)} \to \mathrm{Spec}(\mathbb{F}_q(\zeta_n))$ be the base change of the above situation by this morphism. Let f be the minimal positive integer such that $q^f \equiv 1 \bmod n$, so that $\mathbb{F}_q(\zeta_n) = \mathbb{F}_{q^f}$.

There is a natural action of $GL_2(\mathbb{Z}/n\mathbb{Z})/\{\pm 1\}$ on $X(n)_{/\mathbb{Z}[1/n]}$. Its subgroup $G := \{g \in GL_2(\mathbb{Z}/n\mathbb{Z})/\{\pm 1\} \mid \det(g) \text{ is a power of } q\}$ leaves $X(n)^{(\zeta_n)}$ stable. $A := \left(\pm\left(\begin{smallmatrix} q & 0 \\ 0 & q \end{smallmatrix}\right)\right) \otimes \sigma_{q^2}$, where $\pm\left(\begin{smallmatrix} q & 0 \\ 0 & q \end{smallmatrix}\right) \in G$ and σ_{q^2} is the q^2-th power automorphism of $\overline{\mathbb{F}}_q$, gives an automorphism of $X(n)^{(\zeta_n)} \otimes_{\mathbb{F}_{q^f}} \mathbb{F}_{q^{2f}}$ of order f. The quotient curve

$X(n)^{(\zeta_n)} \otimes_{\mathbb{F}_{q^f}} \mathbb{F}_{q^{2f}}/\langle A\rangle$ is Ihara's model $X(n)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}$ of $X(n)^{(\zeta_n)}$ over $\mathbb{F}_{q^2}$. An important property of this model is that its supersingular points are all rational over $\mathbb{F}_{q^2}$; cf. [**I**, Proposition 1.3.1].

Let us take and fix a primitive n-th root of unity ζ_n for each n prime to q compatibly (i.e. $\zeta_m^{m/n} = \zeta_n$ whenever n divides m). The above construction then gives us a projective system $\{X(n)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}\}_{q\nmid n}$ of proper, smooth and geometrically irreducible curves over $\mathbb{F}_{q^2}$. Set $X(\infty)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}} := \varprojlim_{q\nmid n} X(n)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}$.

In [**I**], the main theorem is stated in several equivalent ways. In the form [MT 3], it gives the following beautiful characterization of the tower $\{X(n)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}\}_{q\nmid n}$: For each integer $r > 1$ prime to q, a covering $Y \to X(r)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}$ over $\mathbb{F}_{q^2}$, with an irreducible curve Y proper and smooth over $\mathbb{F}_{q^2}$, factors through $X(\infty)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}} \to X(r)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}$ if and only if it enjoys the following properties: (1) the supersingular points of $X(r)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}$ all split completely in Y; (2) it is étale over the non-cuspidal points of $X(r)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}$; and (3) it is tamely ramified over the cusps of $X(r)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}$.

Now let us return to the situation considered before this remark. In our discussion, we assumed that q is inert in K and also that it splits completely in $K(\overline{\mathfrak{m}})/K$. Since we are assuming (3.1.1), this implies that $q \equiv \pm 1 \bmod M$. When this is the case, it is clear from the construction that $X(M)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}$ coincides with $X(M)^{(\zeta_M)}_{/\mathbb{F}_{q^2}}$. Therefore we have the canonical surjective morphism $X(M)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}} = X(M)^{(\zeta_M)}_{/\mathbb{F}_{q^2}} \to X_1(M)_{/\mathbb{F}_{q^2}}$. In this paper, we will ultimately reduce our main theorem (5.1.4) (i.e. the first theorem in the Introduction), or its equivalent form (5.1.7), to a variant of Ihara's theorem using this covering. See 5.3 below for this.

4. Étale coverings of curves and Jacobians.

4.1. Good reduction case.

We use the following notation in this subsection:

$$\begin{cases} L\text{: a finite extension of } \mathbb{Q}, \\ \mathfrak{o}_L\text{: the ring of integers of } L, \\ S = \mathrm{Spec}(\mathfrak{r})\text{: a non-empty open subscheme of } \mathrm{Spec}(\mathfrak{o}_L), \\ X\text{: a proper, smooth and geometrically irreducible curve over } L, \\ \mathcal{X}\text{: a proper and smooth curve over } S \text{ such that } \mathcal{X}\otimes_{\mathfrak{r}} L = X, \\ J\text{: the Jacobian variety of } X \text{ over } L, \\ \mathcal{J}\text{: the Néron model of } J \text{ over } S. \end{cases} \tag{4.1.1}$$

Note that, for any point s of S, the fibre of $\mathcal{X}$ at s is geometrically irreducible by Zariski connectedness theorem [**Groth1**, (4.3.12)]. $\mathcal{J}$ is an abelian scheme over S.

In the following, we assume that the genus of X is not zero, and that we are given a closed immersion of L-group schemes $\boldsymbol{\mu}_n \hookrightarrow J$ for a positive integer n. Set $J' := J/\boldsymbol{\mu}_n$. We have an exact sequence of group schemes over L

$$0 \to \boldsymbol{\mu}_n \to J \to J' \to 0 \text{ (exact)}. \tag{4.1.2}$$

Indicating by "$^\vee$" the dual abelian variety, we have

$$0 \leftarrow J^\vee \leftarrow J'^\vee \leftarrow \mathbb{Z}/n\mathbb{Z} \leftarrow 0 \text{ (exact)} \tag{4.1.3}$$

over L. Here, $J^\vee$ may be identified with J, and hence if we let $\mathcal{J}'$ be the Néron model of $J'^\vee$ over S, we have a complex of group schemes over S

$$0 \leftarrow \mathcal{J} \leftarrow \mathcal{J}' \leftarrow \mathbb{Z}/n\mathbb{Z} \leftarrow 0. \tag{4.1.4}$$

Lemma (4.1.5). *Assume either one of the following conditions*:

(i) *n is invertible in S*;

(ii) *n is a power of a prime number l, and the absolute ramification index of each prime ideal $\mathfrak{l}$ of $\mathfrak{r}$ above l is strictly less than $l-1$.*

Then the sequence (4.1.4) *is exact.*

Proof. More generally, suppose that abelian schemes $\mathcal{A}$ and $\mathcal{A}'$ and a complex

$$0 \to \mathbb{Z}/n\mathbb{Z} \to \mathcal{A}' \to \mathcal{A} \to 0$$

over S are given. Then if the generic fibre of this sequence is exact, it is also exact under (i) or (ii).

Indeed, $\mathcal{A}' \to \mathcal{A}$ is an isogeny of abelian schemes, and hence it is faithfully flat and its kernel $\mathcal{K}$ is a finite flat group scheme over S of rank n whose generic fibre is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

In the case (i), $\mathcal{K}$ is an étale group over S and hence $\mathcal{K} \cong \mathbb{Z}/n\mathbb{Z}$.

In the case (ii), we obtain the same conclusion by Raynaud [**Ra**, Théorème 3.3.3]. □

Now assume that $X(L)$ is non-empty. We take and fix $P \in X(L)$ and let $i : X \hookrightarrow J$ be the canonical closed immersion sending P to the origin.

Proposition (4.1.6). *Let the notation be as above. We continue to assume that there is a closed immersion $\boldsymbol{\mu}_n \hookrightarrow J$ over L, and assume either* (i) *or* (ii) *in* (4.1.5). *Then there is a $\mathbb{Z}/n\mathbb{Z}$-torsor*

$$\mathcal{Z} \to \mathcal{X} \text{ over } S$$

such that each fibre of $\mathcal{Z} \to S$ is geometrically irreducible (*whose construction we describe in the course of the proof*).

Proof. $i : X \to J$ extends uniquely to an S-morphism $\mathcal{X} \to \mathcal{J}$ by the Néron property. By the previous lemma, $\mathcal{J}' \to \mathcal{J}$ makes $\mathcal{J}'$ a $\mathbb{Z}/n\mathbb{Z}$-torsor over $\mathcal{J}$, and hence

$$\mathcal{Z} := \mathcal{X} \times_{\mathcal{J}} \mathcal{J}'$$

is a $\mathbb{Z}/n\mathbb{Z}$-torsor over $\mathcal{X}$. The geometric irreducibility of $\mathcal{Z} \otimes_{\mathfrak{r}} L$ is well-known; cf. Milne [**Mi**, Proposition 9.1]. It follows that all fibres of $\mathcal{Z}/S$ are geometrically irreducible as well. □

We let $Z := \mathcal{Z} \otimes_{\mathfrak{r}} L$ be the generic fibre of $\mathcal{Z}$, and $\operatorname{Spec}(\mathfrak{o}_L) - S := \{v_1, \ldots, v_t\}$ the set of finite primes of L outside S.

Corollary (4.1.7). *Let L' be a finite extension of L, and assume we are given a point $x \in X(L')$. Then the fibre product obtained by using this $x : \operatorname{Spec}(L') \to X$ and $Z \to X$ is of the form*

$$\operatorname{Spec}(L') \times_X Z = \coprod_{i=1}^{m} \operatorname{Spec}(L_i)$$

with fields L_i. Each L_i is an abelian extension of L' of degree dividing n, which is unramified outside the primes above v_j $(j = 1, \ldots, t)$.

Proof. Let w be a prime of L corresponding to a closed point of S. Take a prime w' of L' above w, and let $\mathfrak{r}'_{w'} \subset L'$ be its valuation ring. Since $\mathcal{X}$ is proper over S, the morphism $\operatorname{Spec}(L') \xrightarrow{x} X \to \mathcal{X}$ uniquely extends to an S-morphism $\operatorname{Spec}(\mathfrak{r}'_{w'}) \to \mathcal{X}$. The base extension $\operatorname{Spec}(\mathfrak{r}'_{w'}) \times_{\mathcal{X}} \mathcal{Z} \to \operatorname{Spec}(\mathfrak{r}'_{w'})$ of $\mathcal{Z} \to \mathcal{X}$ by this morphism is a $\mathbb{Z}/n\mathbb{Z}$-torsor by the previous proposition, of which $\operatorname{Spec}(L') \times_X Z \to \operatorname{Spec}(L')$ is the generic fibre. □

4.2. Semi-stable reduction case.

In this subsection, we let p be an odd prime, and F a finite extension of $\mathbb{Q}_p$ whose ring of integers we denote by $\mathfrak{r}_F$.

Proposition (4.2.1). *Let A and A' be abelian varieties over F. Let $\mathcal{A}$ and $\mathcal{A}'$ be their Néron models over $\mathfrak{r}_F$, respectively, and assume that they have semi-stable reduction.*

Assume that the ramification index of $F/\mathbb{Q}_p$ is strictly less than $p-1$. Let $f : A' \to A$ be an F-isogeny such that $\operatorname{Ker}(f) \cong \mathbb{Z}/p^r\mathbb{Z}$ for some $r \geq 0$.

Denote by the same letter f the associated homomorphism $\mathcal{A}' \to \mathcal{A}$. Then its kernel is isomorphic to $\mathbb{Z}/p^r\mathbb{Z}$ over $\mathfrak{r}_F$, and we have the exact sequence

$$0 \to \mathbb{Z}/p^r\mathbb{Z} \to \mathcal{A}' \xrightarrow{f} \mathcal{A} \to 0$$

of group schemes over $\mathfrak{r}_F$.

Proof. $f : \mathcal{A}' \to \mathcal{A}$ is an isogeny of Néron models having semi-stable reduction, and hence $\operatorname{Ker}(f)$ is a quasi-finite, separated and flat group scheme over $\mathfrak{r}_F$. Since $\mathfrak{r}_F$ is complete, we have the decomposition

$$\operatorname{Ker}(f) = X^{\mathrm{f}} \coprod X'$$

where X^{f} is finite and flat over $\mathfrak{r}_F$, and the closed fibre of X' is empty. Since we have the complex $\mathbb{Z}/p^r\mathbb{Z} \to \mathcal{A}' \to \mathcal{A}$, the first morphism factors through $\operatorname{Ker}(f)$, which in fact factors as $\mathbb{Z}/p^r\mathbb{Z} \to X^{\mathrm{f}} \hookrightarrow \operatorname{Ker}(f)$. Looking at the generic fibre, we conclude that $\mathbb{Z}/p^r\mathbb{Z} \xrightarrow{\sim} X^{\mathrm{f}} = \operatorname{Ker}(f)$ by [**Ra**, Théorème 3.3.3].

It remains to show the surjectivity of $f : \mathcal{A}' \to \mathcal{A}$. For this, we may replace $\mathfrak{r}_F$ by its strict localization $\mathfrak{r}_F^{\mathrm{str}}$. Let s be the closed point of $\operatorname{Spec}(\mathfrak{r}_F^{\mathrm{str}})$ and $\kappa(s)$ the residue field of s, so that $\kappa(s)$ is algebraically closed. We need to show that $f_s : \mathcal{A}'_s \to \mathcal{A}_s$, the fibre of f at s, is surjective. For this let $\mathcal{A}_s^0$ be the identity component of $\mathcal{A}_s$, and $\Phi(\mathcal{A}_s) := \mathcal{A}_s/\mathcal{A}_s^0$ the group of connected components of $\mathcal{A}_s$; and similarly for $\mathcal{A}'_s$. Since f_s induces surjective morphism on the identity components, our problem is reduced to showing that the homomorphism $\Phi(f_s) : \Phi(\mathcal{A}'_s) \to \Phi(\mathcal{A}_s)$ induced by f_s is surjective.

To see this, we recall Grothendieck's description of $\Phi(\mathcal{A}_s)$, [**Groth2**, (11.5.3)]; cf. also Ribet [**Ri2**, Section 3]. Let $X(A)$ be the character group of the maximal torus T of $\mathcal{A}_s$; $X(A) = \operatorname{Hom}_{\kappa(s)}(T, \mathbb{G}_m)$. Grothendieck's monodromy pairing induces a homomorphism $X(A^\vee) \to X(A)^* := \operatorname{Hom}(X(A), \mathbb{Z})$, and $\Phi(\mathcal{A}_s)$ is canonically isomorphic to its cokernel; and similarly for $\mathcal{A}'$. We have the commutative diagram, cf. [**Ri2**, loc. cit.]

$$\begin{tikzcd}
0 \arrow[r] & X(A'^\vee) \arrow[r] \arrow[d] & X(A')^* \arrow[r] \arrow[d] & \Phi(\mathcal{A}'_s) \arrow[r] \arrow[d, "\Phi(f_s)"] & 0 \\
0 \arrow[r] & X(A^\vee) \arrow[r] & X(A)^* \arrow[r] & \Phi(\mathcal{A}_s) \arrow[r] & 0.
\end{tikzcd}$$

Here, $f_s : \mathcal{A}'_s \to \mathcal{A}_s$ induces the homomorphism $T' \to T$ of their maximal tori, and the middle vertical homomorphism is obtained from this by functoriality. Therefore, it is enough to show that this $T' \to T$ is an isomorphism. By our assumption, there is an F-isogeny $g : A \to A'$ such that $g \circ f = p^r$. It follows that $\operatorname{Ker}(T' \to T)$ is a subscheme of $T'[p^r]$ so that $\operatorname{Ker}(T' \to T)(\kappa(s))$ consists of only one point. On the other hand, it follows from the first step of the proof that $\operatorname{Ker}(T' \to T)$ is a subscheme of the constant group scheme $\mathbb{Z}/p^r\mathbb{Z}$. We conclude that $\operatorname{Ker}(T' \to T)$ is trivial, and hence $T' \to T$ is an isomorphism, as desired. □

We keep the notation and the assumption of (4.2.1). Let X be a proper, smooth and geometrically irreducible curve over F, and suppose that a non-constant F-morphism $g : X \to A$ is given. The base change

$$f' : Z := X \times_A A' \to X \tag{4.2.2}$$

of $f : A' \to A$ by g is a $\mathbb{Z}/p^r\mathbb{Z}$-torsor.

COROLLARY (4.2.3). *Under the same assumption as above, let F' be a finite extension of F, and suppose that a point $x \in X(F')$ is given. Form the fibre product*

$$\operatorname{Spec}(F') \times_X Z = \coprod_{i=1}^{m} \operatorname{Spec}(F_i)$$

using x, with field extensions F_i of F'.

Assume that the composite of $\operatorname{Spec}(F') \xrightarrow{x} X \xrightarrow{g} A \to \mathcal{A}$ *extends to an $\mathfrak{r}_F$-morphism* $\operatorname{Spec}(\mathfrak{r}_{F'}) \to \mathcal{A}$ *for the ring of integers $\mathfrak{r}_{F'}$ of F'. Then each F_i is an unramified extension of F'.*

PROOF. This follows from the same reasoning as in the proof of (4.1.7) using (4.2.1). □

For example, when F' is an unramified extension of F, the Néron property of $\mathcal{A}$ assures us that the extension $\mathrm{Spec}(\mathfrak{r}_{F'}) \to \mathcal{A}$ always exists. In the general case, we have the following:

Corollary (4.2.4). *Let the situation be as in* (4.2.3), *and assume that a proper and flat curve* $\mathcal{X} \to \mathrm{Spec}(\mathfrak{r}_F)$ *whose generic fibre is* X *is given. Denote by* $\mathcal{X}^{\mathrm{smooth}}$ *the smooth locus of* $\mathcal{X}$ *over* $\mathrm{Spec}(\mathfrak{r}_F)$. *If* $x \in X(F')$ *extends to an* $\mathfrak{r}_F$*-morphism* $\mathrm{Spec}(\mathfrak{r}_{F'}) \to \mathcal{X}^{\mathrm{smooth}}$, *we have the same conclusion as* (4.2.3).

Proof. By the Néron property, $g : X \to A$ extends uniquely to an $\mathfrak{r}_F$-morphism $\mathcal{X}^{\mathrm{smooth}} \to \mathcal{A}$. Thus our claim follows from (4.2.3). □

5. μ-type subgroups of $J_1(Np)$.

5.1. Our main result.

As in 3.2, we denote by $X_1(M)_{/\mathbb{Z}[1/M]}$ the smooth compactification of the modular curve classifying pairs (E, α) consisting of an elliptic curve E and $\alpha : \boldsymbol{\mu}_M \hookrightarrow E[M]$ over $\mathbb{Z}[1/M]$-schemes. We write $X_1(M)$ for $X_1(M)_{/\mathbb{Q}}$ and let $J_1(M)$ be its Jacobian variety over $\mathbb{Q}$.

In what follows, we fix a positive integer N and an odd prime number p not dividing N. There is a natural (diamond) action of the group $(\mathbb{Z}/Np\mathbb{Z})^\times$ on $X_1(Np)_{/\mathbb{Z}[1/Np]}$ given by

$$\langle a \rangle (E, \alpha) = (E, a\alpha) \tag{5.1.1}$$

for $a \in (\mathbb{Z}/Np\mathbb{Z})^\times$ and pairs (E, α) as above. We may consider α as a pair (α_N, α_p) consisting of closed immersions $\alpha_N : \boldsymbol{\mu}_N \hookrightarrow E[N]$ and $\alpha_p : \boldsymbol{\mu}_p \hookrightarrow E[p]$. The diamond action $\langle\ \rangle$ of $(\mathbb{Z}/Np\mathbb{Z})^\times$ accordingly decomposes as actions $\langle\ \rangle_N$ of $(\mathbb{Z}/N\mathbb{Z})^\times$ and $\langle\ \rangle_p$ of $(\mathbb{Z}/p\mathbb{Z})^\times$:

$$(\langle b \rangle_N, \langle c \rangle_p)(E, \alpha_N, \alpha_p) = (E, b\alpha_N, c\alpha_p). \tag{5.1.2}$$

The automorphisms $\langle a \rangle$, $\langle b \rangle_N$ and $\langle c \rangle_p$ of $X_1(Np)$ induce automorphisms of $J_1(Np)$ (or its Néron model) covariantly (i.e. via Albanese functoriality), which we express by the same symbols.

Definition (5.1.3). In what follows, we fix a finite abelian extension k_0 of $\mathbb{Q}$ such that $[k_0 : \mathbb{Q}]$ is prime to p, and p is unramified in k_0. Let A be a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$. We denote by $\mathbb{Q}(\zeta_p)^A$ the fixed field under A of $\mathbb{Q}(\zeta_p)$, the field of p-th roots of unity, via the canonical isomorphism $(\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, and set

$$k_A := k_0\mathbb{Q}(\zeta_p)^A.$$

The following is the main result of this paper:

Theorem (5.1.4). *Let the notation and the assumption be as above. Assume that* p *does not divide* $\varphi(N)$, *where* φ *denotes the Euler function, and that* $A \supsetneqq \{1\}$. *Let* G

be a finite k_A-subgroup scheme of $J_1(Np)_{/k_A} = J_1(Np) \otimes_{\mathbb{Q}} k_A$ of μ-type whose order is a power of p. If $\langle a \rangle_p$ acts as the identity on G for all $a \in A$, then G is trivial.

We will complete the proof of this theorem in 5.3 below. Although the proof of the following corollary is similar and simpler, we derive it here directly from (5.1.4):

Corollary (5.1.5). *With the same assumption on N, p and A, let G' be a finite k_A-subgroup scheme of $J_1(N)_{/k_A}$ of μ-type and of order a power of p. Then G' is trivial.*

Proof. The degree of the covering $X_1(Np) \to X_1(N)$ is (either p^2-1 or $(p^2-1)/2$ and hence) prime to p. Thus the order of the kernel of the corresponding homomorphism $J_1(N) \to J_1(Np)$ is also prime to p. Since the image of G' to $J_1(Np)_{/k_A}$ is invariant under $\langle a \rangle_p$ for all $a \in A$, our claim follows from (5.1.4). □

Definition (5.1.6). We let $X_1(Np; A)$ be the quotient of $X_1(Np)$ by the action of A through $\langle\ \rangle_p$. We denote by $J_1(Np; A)$ its Jacobian variety over $\mathbb{Q}$.

Let us denote by $J_1(Np)^A$ the maximal abelian (especially connected) subvariety of $J_1(Np)$ invariant under A:

$$J_1(Np)^A := \mathrm{Ker}\biggl(\prod_{a\in A}(1-\langle a \rangle_p) : J_1(Np) \to \prod_{a \in A} J_1(Np)\biggr)^0.$$

The endomorphism $\sum_{a\in A}\langle a \rangle_p$ of $J_1(Np)$ gives a (surjective) homomorphism $J_1(Np) \to J_1(Np)^A$. Since $|\,A\,|$ is prime to p, it follows that the group G satisfying the condition in (5.1.4) must be contained in $J_1(Np)^A_{/k_A}$. On the other hand, it is easy to see that the quotient morphism $X_1(Np) \to X_1(Np; A)$ induces an isogeny $J_1(Np; A) \to J_1(Np)^A$ of degree prime to p. Therefore (5.1.4) is equivalent to the following:

Theorem (5.1.7). *Let N, p and A be as in* (5.1.4). *Then there is no non-trivial finite k_A-subgroup scheme of $J_1(Np; A)_{/k_A}$ of μ-type and of order a power of p.*

Let A and A' be subgroups of $(\mathbb{Z}/p\mathbb{Z})^\times$ such that $A' \supseteq A \supsetneq \{1\}$. Then $k_{A'} \subseteq k_A$ and the statement of (5.1.4) or (5.1.7) for A clearly implies that for A'. Thus only the case where $|\,A\,|$ is a prime number is essential for (5.1.4) or (5.1.7).

We will prove our main result in the form (5.1.7) below. To do this, we may make the simplifying assumption that $N \geq 5$ so that $X_1(N)_{/\mathbb{Z}[1/N]}$ is the fine moduli scheme (of generalized elliptic curves). Indeed, when $p = 3$ and $N \leq 4$, $\dim J_1(Np) = 0$, and hence there is nothing to prove. When $p \geq 5$, we can take a prime satisfying $l \not\equiv 0, \pm 1 \pmod{p}$ and $l \nmid N$ so that the degree of the covering $X_1(Nlp) \to X_1(Np)$ is prime to p. Hence we may replace N by Nl to prove (5.1.4) or (5.1.7).

We thus assume that $N \geq 5$ in the rest of this section.

5.2. A model of $X_1(Np; A)$ over $\mathbb{Z}[1/N, \zeta_p]^A$.

In this subsection, we describe a natural model of $X_1(Np; A)$ over the ring $\mathbb{Z}[1/N, \zeta_p]^A$ following Deligne and Rapoport [**DR**] and Gross [**Gro**].

Let $X(Np)_{/\mathbb{Z}[1/Np]}$ be the modular curve proper and smooth over $\mathbb{Z}[1/Np]$ corresponding to the $\Gamma(Np)^{\mathrm{naive}}$-moduli problem as in (3.2.6). We denote by $X(Np)_{/\mathbb{Z}[1/N]}$ the normalization of $X(1)_{/\mathbb{Z}[1/N]}$ (= the projective j-line over $\mathbb{Z}[1/N]$) in $X(Np)_{/\mathbb{Z}[1/Np]}$. This is a scheme over $\mathbb{Z}[1/N, \zeta_{Np}]$ in a natural manner, ζ_{Np} being a primitive Np-th root of unity. The group $GL_2(\mathbb{Z}/N\mathbb{Z}) \times GL_2(\mathbb{Z}/p\mathbb{Z})$ acts on this scheme, and this action is compatible with the action on $\mathbb{Z}[1/N, \zeta_{Np}]$ through the canonical homomorphism: $GL_2(\mathbb{Z}/N\mathbb{Z}) \times GL_2(\mathbb{Z}/p\mathbb{Z}) \overset{\det}{\to} (\mathbb{Z}/Np\mathbb{Z})^\times \overset{\sim}{\to} \mathrm{Gal}(\mathbb{Q}(\zeta_{Np})/\mathbb{Q})$.

Consider the following subgroups of $GL_2(\mathbb{Z}/N\mathbb{Z})$ and $GL_2(\mathbb{Z}/p\mathbb{Z})$:

$$\begin{cases} H_N := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z}) \right\}, \\ H_p := \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/p\mathbb{Z}) \right\}, \\ H'_p := \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Z}/p\mathbb{Z}) \right\}, \\ H_p(A) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{Z}/p\mathbb{Z}) \mid d \in A \right\}, \\ H'_p(A) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in GL_2(\mathbb{Z}/p\mathbb{Z}) \mid a, d \in A \right\}. \end{cases} \tag{5.2.1}$$

The group H'_p (resp. $H'_p(A)$) is the image in $GL_2(\mathbb{Z}/p\mathbb{Z})$ of $\Gamma'_{\mathrm{oo}}(p)$ (resp. $\Gamma'_{\mathrm{oo}}(A)$) in the notation of [**DR**, IV, 4.1] (resp. [**DR**, V, 2.14].) The quotient scheme $X(Np)_{/\mathbb{Z}[1/Np]}/(H_N \times H_p)$ is the model $X_1(Np)_{/\mathbb{Z}[1/Np]}$ we have been considering (cf. [**Gro**, Proposition 2.1]), and $X(Np)_{/\mathbb{Z}[1/N]}/(H_N \times H'_p)$ is the model of $X_1(Np)$ over $\mathbb{Z}[1/N, \zeta_p]$ considered in [**Gro**, Proposition 7.1]. Thus

$$X_1(Np; A)_{/\mathbb{Z}[1/Np]} := X(Np)_{/\mathbb{Z}[1/Np]}/(H_N \times H_p(A)) \tag{5.2.2}$$

is a proper and smooth model of $X_1(Np; A)$ over $\mathbb{Z}[1/Np]$. We are interested in

$$X_1(Np; A)_{/\mathbb{Z}[1/N, \zeta_p]^A} := X(Np)_{/\mathbb{Z}[1/N]}/(H_N \times H'_p(A)) \tag{5.2.3}$$

which is a model of $X_1(Np; A) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_p)^A$ over $\mathbb{Z}[1/N, \zeta_p]^A$.

Theorem (5.2.4). (1) *$X_1(Np; A)_{/\mathbb{Z}[1/N, \zeta_p]^A}$ is a regular two-dimensional scheme proper and flat over $\mathbb{Z}[1/N, \zeta_p]^A$.*

(2) *$X_1(Np; A)_{/\mathbb{Z}[1/N, \zeta_p]^A} \to \mathrm{Spec}(\mathbb{Z}[1/N, \zeta_p]^A)$ is smooth over $\mathrm{Spec}(\mathbb{Z}[1/Np, \zeta_p]^A)$.*

(3) *Its characteristic p fibre $X_1(Np; A)_{/\mathbb{F}_p}$ has two irreducible components smooth over $\mathbb{F}_p$. $X_1(Np; A)_{/\mathbb{F}_p}$ is smooth over $\mathbb{F}_p$ except for a finite number of ordinary double points where two irreducible components intersect at supersingular points* (*i.e. the points above the supersingular locus of $X_1(N)_{/\mathbb{F}_p}$*).

Proof. Deligne and Rapoport proved similar result for groups of type "$\Gamma(n) \cap \Gamma'_{\mathrm{oo}}(H)$" for $p \nmid n \geq 3$ in [**DR**, V, 2.19]. Since we are assuming that $N \geq 5$, the same result holds with $\Gamma(n)$ replaced by the inverse image of H_N in $GL_2(\widehat{\mathbb{Z}})$. □

The curve $X_1(Np;A)_{/\mathbb{Z}[1/N,\zeta_p]^A}$ thus has semi-stable reduction at the unique prime of $\mathbb{Z}[1/N,\zeta_p]^A$ above p. We obtain from this the following result (cf. [**DR**, V, Proposition 3.3]):

Corollary (5.2.5). *$J_1(Np;A)\otimes_{\mathbb{Q}}\mathbb{Q}(\zeta_p)^A$ has semi-stable reduction at the unique prime of $\mathbb{Q}(\zeta_p)^A$ above p.* □

5.3. Proof of (5.1.7).

We let $N(\geq 5)$, p and A be as in (5.1.4) and (5.1.7). We now assume that there is a non-trivial finite k_A-subgroup scheme G of $J_1(Np;A)_{/k_A}$ of μ-type and of order a power of p for k_A defined in (5.1.3). $G[p]$ is isomorphic to a product of several copies of $\boldsymbol{\mu}_p$. We thus assume that there is a closed immersion $\boldsymbol{\mu}_p\hookrightarrow J_1(Np;A)_{/k_A}$ of k_A-group schemes until we arrive at a contradiction at the end of this section. We have an exact sequence of k_A-group schemes

$$0\to\boldsymbol{\mu}_p\to J_1(Np;A)_{/k_A}\to J'\to 0 \tag{5.3.1}$$

with $J':=J_1(Np;A)_{/k_A}/\boldsymbol{\mu}_p$.

Let $\mathfrak{o}_{k_A}$ be the ring of integers of k_A, and set $S:=\operatorname{Spec}(\mathfrak{o}_{k_A}[1/Np])$. Denote by $\mathcal{J}_1(Np;A)$ (resp. $\mathcal{J}'$) the Néron model of $J_1(Np;A)_{/k_A}$ (resp. $J'^{\vee}$) over S. By (4.1.5), we have an exact sequence over S

$$0\to\mathbb{Z}/p\mathbb{Z}\to\mathcal{J}'\to\mathcal{J}_1(Np;A)\to 0. \tag{5.3.2}$$

On the other hand, the cusp at infinity is a $\mathbb{Q}$-rational point of $X_1(Np;A)$, and hence there is the canonical closed immersion $i: X_1(Np;A)\hookrightarrow J_1(Np;A)$ over $\mathbb{Q}$ sending that cusp to the origin. Since $X_1(Np;A)_{/S}$:=(the base extension of $X_1(Np;A)_{/\mathbb{Z}[1/Np]}$ to S) is smooth over S, this uniquely extends to an S-morphism $X_1(Np;A)_{/S}\to\mathcal{J}_1(Np;A)$. From this and (5.3.2), we obtain a $\mathbb{Z}/p\mathbb{Z}$-torsor

$$\mathcal{Z}:=X_1(Np;A)_{/S}\times_{\mathcal{J}_1(Np;A)}\mathcal{J}' \tag{5.3.3}$$

over $X_1(Np;A)_{/S}$. We already know that all fibres of $\mathcal{Z}/S$ are geometrically irreducible by (4.1.6). We are going to show that a suitably chosen fibre of $\mathcal{Z}/X_1(Np;A)_{/S}$ over S contradicts a theorem of Ihara [**I**].

To do this, we first take and fix an imaginary quadratic field K satisfying

$$\begin{cases}\text{primes dividing } Np \text{ all split in } K/\mathbb{Q},\\ \text{primes that ramify in } k_A/\mathbb{Q} \text{ also all split in } K/\mathbb{Q},\\ \pm 1 \text{ are the only units of } K.\end{cases} \tag{5.3.4}$$

We next take and fix a prime number l satisfying

$$\begin{cases} l \text{ does not divide } 2Np,\\ l \text{ is unramified in } k_A/\mathbb{Q},\\ l \text{ is unramified in } K/\mathbb{Q} \text{ and satisfies (2.1.2).}\end{cases} \tag{5.3.5}$$

The choice of such K and l is of course possible.

Now set

$$M := Np. \tag{5.3.6}$$

Under (5.3.4), there is an integral ideal $\mathfrak{m}$ of K such that $\mathfrak{o}/\mathfrak{m} \cong \mathbb{Z}/M\mathbb{Z}$ for the ring $\mathfrak{o}$ of integers of K. Using this $\mathfrak{m}$, we can consider the set of CM points

$$X_0(M)(H_\infty)^{\mathrm{CM}} = (\text{the image of } \mathcal{L}_l \text{ under (3.1.5)})$$

as in 3.1 and 3.2, where H_∞ is defined by (2.1.3). We set

$$\widetilde{H}_0 := k_A K(\overline{\mathfrak{m}}) \tag{5.3.7}$$

$K(\overline{\mathfrak{m}})$ being, as before, the ray class field modulo $\overline{\mathfrak{m}}$ of K, and define $\widetilde{H}_n = H_n\widetilde{H}_0$ as in (2.1.5). By our choice of K and l, *this* $\widetilde{H}_0$ *satisfies* (2.1.4). Indeed, $[K(\overline{\mathfrak{m}}) : H_0] = \varphi(Np)/2$ is prime to p since p does not divide $\varphi(N)$, and $[k_A : \mathbb{Q}]$ is prime to p by the definition (5.1.3). Consequently, $[\widetilde{H}_0 : H_0]$ is also prime to p, and other conditions in (2.1.4) are clear.

Since $\widetilde{H}_0$ contains $K(\overline{\mathfrak{m}})$, all points of $X_1(M)$ or $X_1(M;A)$ lying above points in $X_0(M)(H_\infty)^{\mathrm{CM}}$ are rational over $\widetilde{H}_\infty$ by (3.2.1). We let

$$X_1(M)(\widetilde{H}_\infty)^{\mathrm{CM}} \text{ and } X_1(M;A)(\widetilde{H}_\infty)^{\mathrm{CM}}$$

be the inverse images of $X_0(M)(H_\infty)^{\mathrm{CM}}$ in $X_1(M)$ and $X_1(M;A)$, respectively.

Lemma (5.3.8). *Let $\widetilde{L}_n$ be the composite of all abelian extensions of $\widetilde{H}_n$ of degree one or p and unramified outside the primes dividing N, for $0 \le n \le \infty$ (cf. (2.1.8)). For any $x \in X_1(M;A)(\widetilde{H}_\infty)^{\mathrm{CM}}$, all points of $\mathcal{Z} \otimes_{\mathfrak{o}_{k_A}[1/Np]} k_A =: Z$ above x are rational over $\widetilde{L}_\infty$.*

Proof. The given point x is rational over $\widetilde{H}_n$ for some $n < \infty$. Let $\mathrm{Spec}(\widetilde{H}_n) \to X_1(M;A)_{/k_A}$ correspond to x, and form the fibre product $\mathrm{Spec}(\widetilde{H}_n) \times_{X_1(M;A)_{/k_A}} Z$. It is of the form $\coprod \mathrm{Spec}(k_i)$ with abelian extensions k_i of $\widetilde{H}_n$ of degree one or p. By (4.1.7), each extension $k_i/\widetilde{H}_n$ is unramified outside the primes dividing Np. It thus remains to show that each such extension is unramified at the primes above p.

Take a prime $\mathfrak{p}$ (resp. $\mathfrak{p}'$) of k_A (resp. $\widetilde{H}_n$) above p (resp. above $\mathfrak{p}$). Let F (resp. F') be the completion of k_A (resp. $\widetilde{H}_n$) at $\mathfrak{p}$ (resp. at $\mathfrak{p}'$), with its ring of integers $\mathfrak{r}_F$ (resp. $\mathfrak{r}_{F'}$). We know by (5.2.5) that $J_1(M;A)_{/F}$ has semi-stable reduction. Let $X_1(M;A)_{/\mathfrak{r}_F}$ be the base change to $\mathfrak{r}_F$ of the model $X_1(M;A)_{/\mathbb{Z}[1/N,\zeta_p]^A}$ considered in (5.2.4). The F-morphism $\mathrm{Spec}(F') \to X_1(M;A)_{/F}$ corresponding to x uniquely extends to an $\mathfrak{r}_F$-morphism $\widetilde{x} : \mathrm{Spec}(\mathfrak{r}_{F'}) \to X_1(M;A)_{/\mathfrak{r}_F}$. Composing this with the canonical $\mathfrak{r}_F$-morphism $X_1(M;A)_{/\mathfrak{r}_F} \to X_1(N)_{/\mathfrak{r}_F}$, we obtain an $\mathfrak{r}_{F'}$-valued point of $X_1(N)_{/\mathfrak{r}_F}$. But on the generic fibre, this point corresponds to a pair (E', α) over F' with an elliptic curve E' having complex multiplication by an order of K of l-power conductor. Since p splits in K, this elliptic curve over F' has ordinary reduction. The description of

$X_1(M;A)_{/\mathfrak{r}_F}$ given in (5.2.4), (3) then implies that $\widetilde{x}$ must be an $\mathfrak{r}_{F'}$-valued point of the smooth locus of $X_1(M;A)_{/\mathfrak{r}_F}$ over $\mathfrak{r}_F$. Therefore, since $A \supsetneqq \{1\}$, (4.2.4) assures us that the extensions $k_i/\widetilde{H}_n$ are unramified at $\mathfrak{p}'$. □

Let $\widetilde{L}_n$ be the extension of $\widetilde{H}_n$ as in the previous lemma. Then we know by (2.1.8) that there is an integer $n_1 \geq 0$ such that $\widetilde{L}_n = \widetilde{L}_{n_1}\widetilde{H}_n$ for all $n \geq n_1$, including $n = \infty$.

We now take a prime number q satisfying

$$\begin{cases} q \text{ is prime to } Npl, \\ q \text{ is inert in } K, \\ q \text{ splits completely in } \widetilde{L}_{n_1}/K. \end{cases} \tag{5.3.9}$$

For the same reason as in 3.2, Čebotarev density theorem guarantees the existence of such q. Since q splits completely in H_∞/K, it also splits completely in $\widetilde{L}_\infty/K$. Take and fix a prime $\widetilde{\mathfrak{Q}}$ of $\widetilde{H}_\infty$ above q. As in 3.2, this allows us to consider the reduction modulo $\widetilde{\mathfrak{Q}}$ map

$$X_1(M)(\widetilde{H}_\infty)^{\mathrm{CM}} \to X_1^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}) = X_1^{\mathrm{ss}}(M)_{/\mathbb{F}_{q^2}}(\overline{\mathbb{F}}_q)$$

which is surjective, by (3.2.5). We therefore obtain the surjective reduction modulo $\widetilde{\mathfrak{Q}}$ map

$$X_1(M;A)(\widetilde{H}_\infty)^{\mathrm{CM}} \to X_1^{\mathrm{ss}}(M;A)_{/\mathbb{F}_{q^2}}(\mathbb{F}_{q^2}) = X_1^{\mathrm{ss}}(M;A)_{/\mathbb{F}_{q^2}}(\overline{\mathbb{F}}_q)$$

for the supersingular locus $X_1^{\mathrm{ss}}(M;A)_{/\mathbb{F}_{q^2}}$ of $X_1(M;A)_{/\mathbb{F}_{q^2}}$.

Now let $\mathcal{Z}_q \xrightarrow{f} X_1(M;A)_{/\mathbb{F}_{q^2}}$ be the base change of $\mathcal{Z} \to X_1(M;A)_{/S}$ from S to the residue field $\mathbb{F}_{q^2}$ of $\widetilde{\mathfrak{Q}}$. It is a $\mathbb{Z}/p\mathbb{Z}$-torsor with $\mathcal{Z}_q$ geometrically irreducible over $\mathbb{F}_{q^2}$. We moreover have that all supersingular points of $X_1(M;A)_{/\mathbb{F}_{q^2}}$ split completely in $\mathcal{Z}_q$. Indeed, take an $x \in X_1^{\mathrm{ss}}(M;A)_{/\mathbb{F}_{q^2}}(\mathbb{F}_{q^2})$. We can lift it to a CM point $\widetilde{x} \in X_1(M;A)(\widetilde{H}_\infty)^{\mathrm{CM}}$. There is an integer n such that this point is the generic fibre of an $\mathfrak{r}_n$-valued point of $X_1(M;A)_{/S}$, where $\mathfrak{r}_n$ is the valuation ring of the restriction of $\widetilde{\mathfrak{Q}}$ to $\widetilde{H}_n$. The fibre product $\mathrm{Spec}(\mathfrak{r}_n) \times_{X_1(M;A)_{/S}} \mathcal{Z}$ obtained from this is a $\mathbb{Z}/p\mathbb{Z}$-torsor over $\mathrm{Spec}(\mathfrak{r}_n)$ so that it is of the form $\mathrm{Spec}(R_n)$ with R_n finite and étale over $\mathfrak{r}_n$. It follows from (5.3.8) and our choice of q that $\mathrm{Spec}(R_n \otimes_{\mathfrak{r}_n} \mathbb{F}_{q^2}) = f^{-1}(x)$ is a sum of several copies of $\mathrm{Spec}(\mathbb{F}_{q^2})$.

Under (5.3.9), q splits completely in $K(\overline{\mathfrak{m}})$, and in this case we have a canonical morphism $X(M)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}} \xrightarrow{g} X_1(M)_{/\mathbb{F}_{q^2}}$ from Ihara's model, cf. (3.2.6). In general, for any positive integer n prime to q, the main result of [**I**], in the form $[\mathrm{MT}\ 2]_n$, asserts that there is no non-trivial étale covering $Y \to X(n)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}$ with Y a geometrically irreducible curve over $\mathbb{F}_{q^2}$ in which all supersingular points split completely. Since the morphism g ramifies totally at the cusp infinity (cf. e.g. [**I**, 1.2] or [**DR**, VII, 2.4]), and the degree of the morphism $X_1(M)_{/\mathbb{F}_{q^2}} \to X_1(M;A)_{/\mathbb{F}_{q^2}}$ is prime to p, the base change of f by $X(M)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}} \to X_1(M;A)_{/\mathbb{F}_{q^2}}$ gives such a forbidden covering of $X(M)^{\mathrm{Ihara}}_{/\mathbb{F}_{q^2}}$. This completes the proof of (5.1.7).

6. Application to the theory of cyclotomic fields.

6.1. Review of known results.

Throughout this final section, we let p be a prime number such that $p \geq 5$, and N a positive integer prime to p.

We first recall the connection between the modular Galois representation and the theory of cyclotomic fields. Such connection was first studied by Ribet [**Ri1**], and then by Mazur and Wiles [**MW**], who proved the Iwasawa main conjecture for $\mathbb{Q}$, and subsequently by Harder and Pink [**HP**], Kurihara [**Ku**] and the author, among others.

We use the same terminology as in [**O4**, 1.2]. Let $\mathfrak{r}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. We consider

$$\begin{cases} ES_p(N)_{\mathfrak{r}} := (\varprojlim_{r\geq 1} H^1(X_1(Np^r) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Z}_p)) \otimes_{\mathbb{Z}_p} \mathfrak{r}, \\ GES_p(N)_{\mathfrak{r}} := (\varprojlim_{r\geq 1} H^1(Y_1(Np^r) \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Z}_p)) \otimes_{\mathbb{Z}_p} \mathfrak{r}, \end{cases} \tag{6.1.1}$$

where we take the projective limits of the étale cohomology groups of the modular curves $X_1(Np^r)$ (cf. 3.2) and their open subschemes $Y_1(Np^r) := X_1(Np^r) - (\text{cusps})$ relative to the trace maps. The covariant action of the usual Hecke correspondences on these curves defines the Hecke operators $T^*(n)$ for positive integers n and $T^*(q,q)$ for positive integers q prime to Np, on the spaces $ES_p(N)_{\mathfrak{r}}$ and $GES_p(N)_{\mathfrak{r}}$. We can especially consider Hida's idempotent

$$e^* := \lim_{n\to\infty} T^*(p)^{n!} \tag{6.1.2}$$

and the resulting ordinary parts $e^*ES_p(N)_{\mathfrak{r}}$ and $e^*GES_p(N)_{\mathfrak{r}}$. We consider

$$\begin{cases} \mathfrak{r}[[\varprojlim_{r\geq 1} (\mathbb{Z}/Np^r\mathbb{Z})^\times]] = \mathfrak{r}[(\mathbb{Z}/Np\mathbb{Z})^\times][[1+p\mathbb{Z}_p]] \text{ and its subring} \\ \Lambda_{\mathfrak{r}} := \mathfrak{r}[[1+p\mathbb{Z}_p]]. \end{cases} \tag{6.1.3}$$

We let

$$\iota : \varprojlim_{r\geq 1} (\mathbb{Z}/Np^r\mathbb{Z})^\times \hookrightarrow \mathfrak{r}[[\varprojlim_{r\geq 1} (\mathbb{Z}/Np^r\mathbb{Z})^\times]]^\times \tag{6.1.4}$$

be the natural inclusion. We can then let the algebras in (6.1.3) act on $ES_p(N)_{\mathfrak{r}}$ and $GES_p(N)_{\mathfrak{r}}$ in such a way that $\iota(q)$ for a positive integer q prime to Np acts as $T^*(q,q)$. Hida's universal ordinary p-adic Hecke algebras

$$\begin{cases} e^*h^*(N;\mathfrak{r}) \subset \mathrm{End}(e^*ES_p(N)_{\mathfrak{r}}), \\ e^*\mathcal{H}^*(N;\mathfrak{r}) \subset \mathrm{End}(e^*GES_p(N)_{\mathfrak{r}}) \end{cases} \tag{6.1.5}$$

are defined as the subalgebras generated by all $T^*(n)$ and $T^*(q,q)$ over $\Lambda_{\mathfrak{r}}$. It is a fundamental fact proved by Hida that these algebras are finite and flat over $\Lambda_{\mathfrak{r}}$. There is a natural surjection

$$e^*\mathcal{H}^*(N;\mathfrak{r}) \twoheadrightarrow e^*h^*(N;\mathfrak{r}) \tag{6.1.6}$$

sending $T^*(n)$ and $T^*(q,q)$ to $T^*(n)$ and $T^*(q,q)$, respectively.

We next consider the Eisenstein components of the above objects, cf. [**O4**, 1.4, 1.5]. For this, we take and fix an *even* Dirichlet character θ of conductor N or Np. It can thus be expressed as

$$\theta = \chi\omega^i \tag{6.1.7}$$

with χ a primitive Dirichlet character modulo N, and $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times \hookrightarrow \overline{\mathbb{Q}}_p^\times$ the Teichmüller character. We henceforth assume that:

$$\begin{cases} p \nmid \varphi(N), \\ \chi(p) \neq 1 \text{ when } i \equiv -1 \bmod p-1, \\ \theta \neq \omega^{-2}. \end{cases} \tag{6.1.8}$$

We set

$$\mathfrak{r} :=(\text{the ring generated by the values of } \theta \text{ over } \mathbb{Z}_p) \tag{6.1.9}$$

which is an étale $\mathbb{Z}_p$-algebra by our assumption. We define the Eisenstein ideal $\mathcal{I}^* = \mathcal{I}^*(\theta)$ of $e^*\mathcal{H}^*(N;\mathfrak{r})$ as the ideal generated by all $T^*(n) - \sum_{0<t|n, p\nmid t} \theta(t)t\iota(\langle t\rangle)$, where $\langle t\rangle := t\omega(t)^{-1}$ denotes the principal part of $t \in \mathbb{Z}_p^\times$. It is also the ideal generated by $T^*(l) - (1+\theta(l)l\iota(\langle l\rangle))$ for all prime numbers $l \neq p$, $T^*(p)-1$ and $T^*(q,q) - \theta(q)\iota(\langle q\rangle)$ with q prime to Np. We define the Eisenstein ideal $I^* = I^*(\theta)$ of $e^*h^*(N;\mathfrak{r})$ as the ideal generated by the elements of the same name as above; i.e. as the image of $\mathcal{I}^*$ by the surjection (6.1.6).

As usual, we fix a topological generator u_0 of $1+p\mathbb{Z}_p$, and use it to identify $\Lambda_\mathfrak{r}$ with the formal power series ring $\mathfrak{r}[[T]]$ by letting $\iota(u_0)$ correspond to $1+T$. We set

$$\begin{cases} \mathfrak{m}^* = \mathfrak{m}^*(\theta) := (I^*, p, T) \subseteq e^*h^*(N;\mathfrak{r}), \\ \mathfrak{M}^* = \mathfrak{M}^*(\theta) := (\mathcal{I}^*, p, T) \subseteq e^*\mathcal{H}^*(N;\mathfrak{r}). \end{cases} \tag{6.1.10}$$

$\mathfrak{M}^*$ is always a proper, and hence a maximal ideal of $e^*\mathcal{H}^*(N;\mathfrak{r})$, whereas it can happen that $\mathfrak{m}^* = e^*h^*(N;\mathfrak{r})$. We set

$$\begin{cases} X := e^*ES_p(N)_{\mathfrak{r},\mathfrak{M}^*}, \\ \mathfrak{h}^* := e^*h(N;\mathfrak{r})_{\mathfrak{M}^*}, \\ \mathfrak{I}^* := I^*_{\mathfrak{M}^*}, \end{cases} \tag{6.1.11}$$

the localizations at the maximal ideal $\mathfrak{M}^*$ via (6.1.6). On the other hand, let $G(T, \theta\omega^2) \in \Lambda_\mathfrak{r}$ be the Iwasawa power series satisfying

$$G(u_0^s - 1, \theta\omega^2) = L_p(-1-s, \theta\omega^2), \tag{6.1.12}$$

the right hand side being the Kubota–Leopoldt p-adic L-function. We then know, by [**O4**, Case (II) of (1.5.5), 3.2] that

$$\mathfrak{h}^*/\mathfrak{I}^* \cong \Lambda_{\mathfrak{r}}/(G(T,\theta\omega^2)). \tag{6.1.13}$$

Thus $\mathfrak{m}^*$ is a maximal ideal if and only if $G(T,\theta\omega^2)$ is not a unit power series, in which case the modules in (6.1.11) are the same if we consider the localizations at $\mathfrak{m}^*$ instead of $\mathfrak{M}^*$. Otherwise, X and $\mathfrak{h}^*$, as well as the Iwasawa module $\mathrm{Gal}(L_\infty/F_\infty)_{(\theta\omega)^{-1}}$ vanish, and the assertions (6.2.1) and (6.2.2) below will be trivial. *We thus assume that $G(T,\theta\omega^2)$ is not a unit power series, in the rest of this subsection.*

The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on X $\mathfrak{h}^*$-linearly, and we are going to review the nature of this Galois representation in connection with the Iwasawa theory, cf. [**O4**, 3.4, Appendix]. This method is originally due to [**HP**] and [**Ku**].

Let I_p be the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at the prime corresponding to our fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, and set

$$X_+ := X^{I_p}. \tag{6.1.14}$$

We know that it is a free $\mathfrak{h}^*$-module of rank one, and also that $X/X_+ \otimes_{\Lambda_{\mathfrak{r}}} \mathrm{Q}(\Lambda_{\mathfrak{r}})$ is a free $\mathfrak{h}^* \otimes_{\Lambda_{\mathfrak{r}}} \mathrm{Q}(\Lambda_{\mathfrak{r}})$-module of rank one where $\mathrm{Q}(\Lambda_{\mathfrak{r}})$ is the quotient field of $\Lambda_{\mathfrak{r}}$. Further, there is a natural way to choose a splitting image X_- of $X \twoheadrightarrow X/X_+$ as in [**O4**, 3.4]; it is so chosen to satisfy (6.1.19) below. We fix a $\mathfrak{h}^* \otimes_{\Lambda_{\mathfrak{r}}} \mathrm{Q}(\Lambda_{\mathfrak{r}})$-basis e_- of $X_- \otimes_{\Lambda_{\mathfrak{r}}} \mathrm{Q}(\Lambda_{\mathfrak{r}})$ and an $\mathfrak{h}^*$-basis e_+ of X_+ to define the representation

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathfrak{h}^* \otimes_{\Lambda_{\mathfrak{r}}} \mathrm{Q}(\Lambda_{\mathfrak{r}}));\ \sigma \mapsto \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \tag{6.1.15}$$

by the rule

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ni \sigma : \begin{cases} e_- \mapsto a(\sigma)e_- + c(\sigma)e_+, \\ e_+ \mapsto b(\sigma)e_- + d(\sigma)e_+. \end{cases} \tag{6.1.16}$$

Elements $a(\sigma)$, $d(\sigma)$ and $b(\sigma)c(\tau)$ do not depend on the particular choice of bases of X_+ and $X_- \otimes_{\Lambda_{\mathfrak{r}}} \mathrm{Q}(\Lambda_{\mathfrak{r}})$.

Let

$$\kappa : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_p^\times \tag{6.1.17}$$

be the p-cyclotomic character. We know that

$$\det\rho(\sigma) = (\theta\omega)^{-1}(\sigma)\langle\kappa(\sigma)\rangle^{-1}\iota(\langle\kappa(\sigma)\rangle^{-1}) \in \Lambda_{\mathfrak{r}}^\times \text{ for all } \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}). \tag{6.1.18}$$

We recall that, there is an element $\sigma_0 \in I_p$ such that $\langle\kappa(\sigma_0)\rangle = 1$ and $\omega^{-i-1}(\sigma_0) \neq 1$ when $i \not\equiv -1 \bmod p-1$, and a geometric Frobenius $\varPhi_p \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $\kappa(\varPhi_p) = 1$, and the splitting image X_- was so chosen that

$$\begin{cases} \rho(\sigma_0) = \begin{pmatrix} \omega^{-i-1}(\sigma_0) & 0 \\ 0 & 1 \end{pmatrix} \text{ when } i \not\equiv -1 \bmod p-1, \\ \rho(\varPhi_p) = \begin{pmatrix} \chi(p)T^*(p)^{-1} & 0 \\ 0 & T^*(p) \end{pmatrix} \text{ when } i \equiv -1 \bmod p-1. \end{cases} \tag{6.1.19}$$

Using this and [**O5**, (4.1.12)], we have the following lemma; cf. [**O5**, 4.2]:

Lemma (6.1.20). *Elements $a(\sigma)$, $d(\sigma)$ and $b(\sigma)c(\tau)$ belong to $\mathfrak{h}^*$, and each of the following sets generates the Eisenstein ideal $\mathfrak{I}^*$:*

$$\begin{cases} \{a(\sigma) - \det\rho(\sigma) \mid \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\}, \\ \{d(\sigma) - 1 \mid \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\}, \\ \{b(\sigma)c(\tau) \mid \sigma, \tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\}. \end{cases}$$ □

Now let F be the extension of $\mathbb{Q}$ corresponding to $\theta\omega$. $F/\mathbb{Q}$ is an imaginary abelian extension of degree prime to p. We let F_∞ be the cyclotomic $\mathbb{Z}_p$-extension of F, set

$$\begin{cases} \Delta := \mathrm{Gal}(F/\mathbb{Q}), \\ \Gamma := \mathrm{Gal}(F_\infty/F), \end{cases} \tag{6.1.21}$$

and identify $\mathrm{Gal}(F_\infty/\mathbb{Q})$ with $\Delta \times \Gamma$. Set

$$B := (\text{the } \mathfrak{h}^*\text{-submodule of } \mathfrak{h}^* \otimes_{\Lambda_\mathfrak{r}} \mathrm{Q}(\Lambda_\mathfrak{r}) \text{ generated by all } b(\sigma),\ \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})). \tag{6.1.22}$$

It follows from (6.1.20) that we have a representation

$$\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \left\{ \begin{pmatrix} (\mathfrak{h}^*/\mathfrak{I}^*)^\times & B/\mathfrak{I}^*B \\ 0 & 1 \end{pmatrix} \right\} \text{ by } \varphi(\sigma) := \begin{pmatrix} \overline{\det\rho(\sigma)} & \overline{b(\sigma)} \\ 0 & 1 \end{pmatrix} \tag{6.1.23}$$

the bar indicating reduction modulo $\mathfrak{I}^*$. The field corresponding to $\mathrm{Ker}(\overline{\det\rho})$ is F_∞, cf. [**O3**, (3.3.8)], and if we denote by L the field corresponding to $\mathrm{Ker}(\varphi)$, the correspondence $\sigma \mapsto \overline{b(\sigma)}$ gives an isomorphism

$$\mathrm{Gal}(L/F_\infty) \xrightarrow{\sim} B/\mathfrak{I}^*B, \tag{6.1.24}$$

cf. [**O4**, (A.1.11)].

Let L_∞ be the maximal unramified abelian pro-p-extension of F_∞, and consider the "$(\theta\omega)^{-1}$-part" of the associated Galois group

$$\mathrm{Gal}(L_\infty/F_\infty)_{(\theta\omega)^{-1}} := \mathrm{Gal}(L_\infty/F_\infty) \otimes_{\mathbb{Z}_p[\Delta]} \mathfrak{r}, \tag{6.1.25}$$

the tensor product being induced by $(\theta\omega)^{-1} : \mathbb{Z}_p[\Delta] \to \mathfrak{r}$. The p-cyclotomic character κ gives an isomorphism $\Gamma \xrightarrow{\sim} 1 + p\mathbb{Z}_p$, and hence $\mathfrak{r}[[\Gamma]] \xrightarrow{\sim} \Lambda_\mathfrak{r}$. We consider $\mathrm{Gal}(L_\infty/F_\infty)_{(\theta\omega)^{-1}}$ as a $\Lambda_\mathfrak{r}$-module through this isomorphism. On the other hand, for a $\Lambda_\mathfrak{r}$-module M, we denote by $M^\dagger$ the same group M on which the action of $\iota(u_0) \in \Lambda_\mathfrak{r}$ is newly defined by that of $u_0^{-1}\iota(u_0^{-1})$. The Galois group $\mathrm{Gal}(L/F_\infty)$ coincides with the group (6.1.25), cf. [**O2**, (5.3.20)], and we obtain:

Proposition (6.1.26). *Under the above notation and the assumptions, the correspondence $\sigma \mapsto \overline{b(\sigma)}$ gives an isomorphism of $\Lambda_\mathfrak{r}$-modules*

$$\mathrm{Gal}(L_\infty/F_\infty)_{(\theta\omega)^{-1}} \xrightarrow{\sim} (B/\mathfrak{I}^*B)^\dagger.$$ □

6.2. Application to a conjecture of Sharifi.

We have thus described the Iwasawa module $\mathrm{Gal}(L_\infty/F_\infty)_{(\theta\omega)^{-1}}$ in terms of the module $B \cong Be_- \subseteq X_-$. In [**Sha**], Sharifi made the conjecture below about the nature of this module. It is in fact a consequence of his much more precise conjectures (cf. Conjectures 4.12, 5.2 and 5.4, and the remark at the end of Section 5 in [**Sha**]). See the work of Fukaya and Kato [**FK**] for results in this direction. Our application is concerned with the conjecture of the following form:

Conjecture of Sharifi (6.2.1). *Be_- coincides with X_-. In other words, via the map $\sigma \mapsto \sigma e_+ - e_+$ mod $\mathfrak{I}^* X$, one has an isomorphism of $\Lambda_{\mathfrak{r}}$-modules*

$$\mathrm{Gal}(L_\infty/F_\infty)_{(\theta\omega)^{-1}} \xrightarrow{\sim} (X_-/\mathfrak{I}^* X_-)^\dagger.$$

Sharifi proved this conjecture under the assumption that $e^*\mathcal{H}^*(N;\mathfrak{r})_{\mathfrak{M}^*}$ is a Gorenstein ring, cf. [**Sha**, Proposition 4.10].

Since X_- is known to be isomorphic to $\mathrm{Hom}_{\Lambda_\mathfrak{r}}(\mathfrak{h}^*, \Lambda_\mathfrak{r})$, [**O3**, (2.3.6)], or a local component of the space of ordinary $\Lambda_\mathfrak{r}$-adic cusp forms of level N, [**O1**, (2.5.3)], this conjecture describes $\mathrm{Gal}(L_\infty/F_\infty)_{(\theta\omega)^{-1}}$ concretely in terms of such objects. As application of our study of μ-type subgroups of $J_1(M)$, we have

Theorem (6.2.2). *In addition to the assumptions in the previous subsection, assume that $(i, p-1) > 1$, i.e. the kernel of ω^i is non-trivial, in the expression* (6.1.7) *of θ. Then Sharifi's conjecture* (6.2.1) *is valid for the character θ.*

As noted in the previous subsection, we may and do assume that $G(T, \theta\omega^2)$ is not a unit in $\Lambda_\mathfrak{r}$ in proving this theorem. We first note

Lemma (6.2.3). *Let $\mathcal{M}$ be the minimal submodule of X containing X_+ and stable under the action of $\mathfrak{h}^*$ and* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. *Then we have*

(1) *$\mathcal{M} = X_+ \oplus Be_-$.*

(2) *$X/\mathcal{M}$ is annihilated by $\mathfrak{I}^*$, and* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \ni \sigma$ *acts as multiplication by* $\det\rho(\sigma)$ *on this module.*

Proof. (1) By the definition (6.1.22) of B, $X_+ \oplus Be_-$ is an $\mathfrak{h}^*$-submodule of X. It follows from the definitions (6.1.15) and (6.1.16) that $\mathcal{M} \supseteq X_+ \oplus Be_-$, and also that the right hand side is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable.

(2) Again by (6.1.16), $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts as $a(\sigma)$ on $X/\mathcal{M}$. Since $a(\sigma\tau) = a(\sigma)a(\tau) + b(\sigma)c(\tau)$, (6.1.20) shows that this module is annihilated by $\mathfrak{I}^*$, and hence the action of σ on it is given by $a(\sigma) \equiv \det\rho(\sigma)$ mod $\mathfrak{I}^*$. □

The projection gives an isomorphism

$$e^*ES_p(N)_\mathfrak{r}/T \xrightarrow{\sim} e^*H^1(X_1(Np) \otimes_\mathbb{Q} \overline{\mathbb{Q}}, \mathfrak{r}) \tag{6.2.4}$$

by [**O1**, (1.4.3)] (with $T = \omega_{1,0} \in \Lambda_\mathfrak{r}$ in the notation loc. cit.), which commutes with the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the Hecke operators $T^*(n)$ and $T^*(q,q)$. Let $h_2^*(\Gamma_1(Np);\mathfrak{r})$ be the $\mathfrak{r}$-subalgebra of $\mathrm{End}(H^1(X_1(Np) \otimes_\mathbb{Q} \overline{\mathbb{Q}}, \mathfrak{r}))$ generated by all $T^*(n)$ and $T^*(q,q)$, and let $e^*h_2^*(\Gamma_1(Np);\mathfrak{r}) \subseteq \mathrm{End}(e^*H^1(X_1(Np)\otimes_{\mathbb{Q}}\overline{\mathbb{Q}},\mathfrak{r}))$ be its ordinary part. Let $\mathfrak{m}_0^*$ be the image of $\mathfrak{m}^*$ by the canonical surjection $e^*h^*(N;\mathfrak{r}) \twoheadrightarrow e^*h_2^*(\Gamma_1(Np);\mathfrak{r})$. It is a maximal ideal, and we have an isomorphism

$$X/(p,T) \xrightarrow{\sim} e^*H^1(X_1(Np)\otimes_{\mathbb{Q}}\overline{\mathbb{Q}},\mathfrak{r})_{\mathfrak{m}_0^*}/p. \tag{6.2.5}$$

On the other hand, we have a canonical isomorphism

$$H^1(X_1(Np)\otimes_{\mathbb{Q}}\overline{\mathbb{Q}},\mathfrak{r}) \cong \mathrm{Hom}(T_p(J_1(Np)),\mathfrak{r}) \tag{6.2.6}$$

which is an isomorphism of $h_2^*(\Gamma_1(Np);\mathfrak{r})$-modules if we let $T^*(n)$ and $T^*(q,q)$ act on the right hand side via the contravariant action of Hecke correspondences of the same kind on $J_1(Np)$. In the following, we denote by the same symbol $\mathfrak{m}_0^*$ the maximal ideal of $h_2^*(\Gamma_1(Np);\mathfrak{r})$ corresponding to the above $\mathfrak{m}_0^*$ in its direct factor $e^*h_2^*(\Gamma_1(Np);\mathfrak{r})$.

Lemma (6.2.7). *Assume that $\mathcal{M} \neq X$. Then there is a non-trivial submodule of $(J_1(Np)[p](\overline{\mathbb{Q}})\otimes_{\mathbb{F}_p}\mathfrak{k})[\mathfrak{m}_0^*]$ on which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts via $\theta\omega$. Here $\mathfrak{k}$ denotes the residue field of $\mathfrak{r}$.*

Proof. Since $\det\rho(\sigma) \equiv (\theta\omega)^{-1}(\sigma) \bmod (p,T)$ by (6.1.18), Nakayama's lemma and (6.2.3) imply that each module in (6.2.5) admits a non-trivial quotient as an $e^*h_2^*(\Gamma_1(Np);\mathfrak{r})$-module on which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts via the character $(\theta\omega)^{-1}$.

On the other hand, we obtain from (6.2.6) that

$$H^1(X_1(Np)\otimes_{\mathbb{Q}}\overline{\mathbb{Q}},\mathfrak{r})/\mathfrak{m}_0^* \cong \mathrm{Hom}_{\mathfrak{k}}((J_1(Np)[p](\overline{\mathbb{Q}})\otimes_{\mathbb{F}_p}\mathfrak{k})[\mathfrak{m}_0^*],\mathfrak{k}).$$

Therefore, again by Nakayama's lemma, the right hand side admits a non-trivial quotient as a $\mathfrak{k}$-vector space on which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts via $(\theta\omega)^{-1}$. □

We can now complete the proof of (6.2.2): Set $A := \mathrm{Ker}(\omega^i)$. Assume that $Be_- \subsetneq X_-$, equivalently that $\mathcal{M} \subsetneq X$. We first note that the ("dual") diamond action $\langle a\rangle^* = \langle a\rangle^{-1}$ of $a \in (\mathbb{Z}/Np\mathbb{Z})^\times$, which is $T^*(q,q)$ for $a = q \bmod Np$, is given by $\theta(a)$ on $(J_1(Np)[p](\overline{\mathbb{Q}})\otimes_{\mathbb{F}_p}\mathfrak{k})[\mathfrak{m}_0^*]$. Hence $\langle a\rangle_p = 1$ for all $a \in A$ on this group.

Let $(\theta\omega)_0$ denote the irreducible $\mathbb{Z}_p$-representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ containing $\theta\omega$. It then follows from (6.2.7) and the above remark that the $(\theta\omega)_0$-isotypic component $((\sum_{a\in A}\langle a\rangle_p)J_1(Np)[p](\overline{\mathbb{Q}}))^{(\theta\omega)_0}$ is non-trivial. Let H be the finite subgroup scheme of $J_1(Np)$ corresponding to this $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module. Then, if we let k_A be the field $\mathbb{Q}(\zeta_N)\mathbb{Q}(\zeta_p)^A$, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/k_A)$ on $H(\overline{\mathbb{Q}})$ is given by ω, that is, $H\otimes_{\mathbb{Q}}k_A$ is a subgroup scheme of μ-type of $J_1(Np)_{/k_A}[p]$ on which we have $\langle a\rangle_p = 1$ for all $a \in A$. This contradicts our main theorem (5.1.4), and finishes the proof.

In (6.2.2) and the main result (5.1.4) on which it depends, we needed the assumption "$A \supsetneq \{1\}$". It was essential in order to apply Raynaud's result in Section 4 (cf. (4.2.1) and its corollaries), which enabled us to show the unramifiedness of the primes above p in (5.3.8). We thus do not know at present whether or not it is possible to modify this assumption in our argument.

Finally, as an example, consider the case where χ in (6.1.7) is even. Then, since we are assuming that θ is even, the kernel of ω^i must be non-trivial. When $N = 1$, this is automatically the case. In the excluded case where $\theta = \omega^{-2}$, both $\Lambda_{\mathfrak{r}}$-modules figuring in (6.2.1) vanish, and therefore Sharifi's conjecture (6.2.1) is valid when $N = 1$.

References

[C] C. Cornut, Mazur's conjecture on higher Heegner points, Invent. Math., **148** (2002), 495–523.

[D] P. Deligne, Formes modulaires et représentations l-adiques, In: Séminaire Bourbaki, Lecture Notes in Math., **179**, Springer, Berlin, 1971, exp. 355, 139–172.

[DR] P. Deligne and M. Rapoport, Les schémas de modules de courbes elliptiques, In: Modular Functions of One Variable II, Lecture Notes in Math., **349**, Springer, Berlin, 1973, 143–316.

[FK] T. Fukaya and K. Kato, On conjectures of Sharifi, preprint.

[Gre] R. Greenberg, On the structure of certain Galois groups, Invent. Math., **47** (1978), 85–99.

[Gro] B. Gross, A tameness criterion for Galois representations associated to modular forms (mod p), Duke Math. J., **61** (1990), 445–517.

[Groth1] A. Grothendieck, Éléments de géométrie algébrique, III, Rédigés avec la collaboration de J. Dieudonné, Publ. Math. Inst. Hautes Études Sci., **11** (1961).

[Groth2] A. Grothendieck, Modèles de Néron et monodromie, In: Groupes de Monodromie en Géométrie Algébrique. Séminaire de Géométrie Algébrique 7, I, Lecture Notes in Math., **288**, Springer, Berlin, 1972, exp. IX, 313–523.

[HP] G. Harder and R. Pink, Modular konstruierte unverzweigte abelsche p-Erweiterungen von $\mathbb{Q}(\zeta_p)$ und die Struktur ihrer Galoisgruppen, Math. Nachr., **159** (1992), 83–99.

[H1] H. Hida, Non-vanishing modulo p of Hecke L-values, In: Geometric Aspects of Dwork Theory, (eds. A. Adolphson, F. Baldassarri, P. Berthelot, N. Katz and F. Loeser), Walter de Gruyter, 2004, 735–784.

[H2] H. Hida, Non-vanishing modulo p of Hecke L-values and application, In: L-Functions and Galois Representations, London Math. Soc. Lecture Note Ser., **320**, Cambridge Univ. Press, 2007, 207–269.

[H3] H. Hida, Elliptic Curves and Arithmetic Invariants, Springer Monogr. Math., Springer, 2013.

[I] Y. Ihara, On modular curves over finite fields, In: Discrete Subgroups of Lie Groups and Applications to Moduli, Oxford Univ. Press, 1975, 161–202.

[Ka1] N. Katz, p-adic properties of modular schemes and modular forms, In: Modular Functions of One Variable III, Lecture Notes in Math., **350**, Springer, Berlin, 1973, 69–190.

[Ka2] N. Katz, p-adic interpolation of real analytic Eisenstein series, Ann. Math. (2), **104** (1976), 459–571.

[Ka3] N. Katz, p-adic L-functions for CM fields, Invent. Math., **49** (1978), 199–297.

[KM] N. Katz and B. Mazur, Arithmetic Moduli of Elliptic Curves, Ann. of Math. Stud., **108**, Princeton Univ. Press, 1985.

[Ku] M. Kurihara, Ideal class groups of cyclotomic fields and modular forms of level 1, J. Number Theory, **45** (1993), 281–294.

[Ma] B. Mazur, Modular curves and the Eisenstein ideal, Publ. Math. Inst. Hautes Études Sci., **47** (1977), 33–186.

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of **Q**, Invent. Math., **76** (1984), 179–330.

[Mi] J. S. Milne, Jacobian varieties, In: Arithmetic Geometry, (eds. G. Cornell and J. Silverman), Springer-Verlag, 1986, 167–212.

[O1] M. Ohta, On the p-adic Eichler–Shimura isomorphism for Λ-adic cusp forms, J. Reine Angew. Math., **463** (1995), 49–98.

[O2] M. Ohta, Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves, Comp. Math., **115** (1999), 241–301.

[O3] M. Ohta, Ordinary p-adic étale cohomology groups attached to towers of elliptic modular curves. II, Math. Ann., **318** (2000), 557–583.

[O4] M. Ohta, Congruence modules related to Eisenstein series, Ann. Sci. École Norm. Sup. (4), **36** (2003), 225–269.

[O5] M. Ohta, Companion forms and the structure of p-adic Hecke algebras II, J. Math. Soc. Japan, **59** (2007), 913–951.

[O6] M. Ohta, Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties, J. Math. Soc. Japan, **65** (2013), 733–772.

[O7] M. Ohta, Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II, Tokyo J. Math., **37** (2014), 273–318.

[Ra] M. Raynaud, Schémas en groupes de type $(p, \dots, p)$, Bull. Soc. Math. France, **102** (1974), 241–280.

[Ri1] K. Ribet, A modular construction of unramified p-extensions of $\boldsymbol{Q}(\mu_p)$, Invent. Math., **34** (1976), 151–162.

[Ri2] K. Ribet, On the component groups and the Shimura subgroups of $J_0(N)$, In: Séminaire de Théorie des Nombres de Bordeaux, 1987–1988, Univ. Bordeaux, exp. 6.

[Ru1] K. Rubin, The "main conjectures" of Iwasawa theory for imaginary quadratic fields, Invent. Math., **103** (1991), 25–68.

[Ru2] K. Rubin, More "main conjectures" for imaginary quadratic fields, In: Elliptic Curves and Related Topics, (eds. H. Kisilevsky and M. Murty), CRM Proc. Leture Notes, **4**, Amer. Math. Soc., 1994, 23–28.

[ST] J.-P. Serre and J. Tate, Good reduction of abelian varieties, Ann. Math. (2), **88** (1968), 492–517.

[dS] E. de Shalit, Iwasawa Theory of Elliptic Curves with Complex Multiplication, Perspect. Math., **3**, Academic Press, 1987.

[Sha] R. Sharifi, A reciprocity map and the two-variable p-adic L-function, Ann. Math. (2), **173** (2011), 251–300.

[Shi1] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan, **11**, Iwanami Shoten and Princeton Univ. Press, 1971.

[Shi2] G. Shimura, On some arithmetic properties of modular forms of one and several variables, Ann. Math. (2), **102** (1975), 491–515 (Collected Papers II, [75c]).

[Si] W. Sinnott, On a theorem of L. Washington, Astérisque, **147–148** (1987), 209–224.

[V] V. Vatsal, Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves, J. Inst. Math. Jussieu, **4** (2005), 281–316.

[W] L. Washington, The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension, Invent. Math., **49** (1978), 87–97.

[Y] H. Yoshida, Absolute CM-Periods, Math. Surveys Monogr., **106**, Amer. Math. Soc., 2003.

Masami Ohta
Professor Emeritus
Tokai University
Hiratsuka
Kanagawa 259-1292, Japan
E-mail: ohta@tokai-u.jp