

The Eisenstein Quotient of the Jacobian Variety of a Drinfeld Modular Curve

By

Akio TAMAGAWA *

§ 0. Introduction

Let $K = \mathbb{F}_q(T)$, the rational function field over the finite field \mathbb{F}_q (T : indeterminate), and $A = \mathbb{F}_q[T]$. For a non-zero ideal \mathfrak{n} of A , we can define a smooth proper geometrically connected curve $X_0(\mathfrak{n})$ over K , called the Drinfeld modular curve of Hecke type with conductor \mathfrak{n} . In this article, we define the “Eisenstein quotient” \tilde{J} of the Jacobian variety J of $X_0(\mathfrak{n})$ for \mathfrak{n} maximal and investigate its arithmetic properties. One of the main results is as follows :

Theorem (5.7).

- (i) $\tilde{J}^-(K)$ is finite.
- (ii) $\text{III}(\tilde{J}^-/K) \otimes_{\mathbb{Z}} \mathbb{Z}[q^{-1}]$ is finite.

Here \tilde{J}^- is a certain quotient of \tilde{J} (the “minus part” of \tilde{J}) and III means the Shafarevich-Tate group.

In [19], Mazur established a very elaborate theory of Eisenstein ideals for modular curves over the rational number field \mathbb{Q} and his theory has various applications to number theory. (For example, the theorem corresponding to (5.7) (i) above has been a main tool of almost all the researches on rational points on modular curves.) The problem to develop the theory of Eisenstein ideals for Drinfeld modular curves was suggested by Mazur, already in the introduction of [19]. We consider that the present paper is its first step and hope for further development.

In § 1, we define an (l -primary) admissible group over an irreducible locally noetherian normal scheme S of dimension 1, following Mazur [19], and give an

Received April 7, 1994.

1991 Math. Subject Classifications : 11G09, 11G40, 14K15.

* Research Institute for Mathematical Sciences, Kyoto University, Kyoto 606-01, Japan

estimate (1.11) of its étale cohomology in case $S = \mathbb{P}_{\mathbb{F}_q}^1$. In § 2, we recall the definition of the “ L -series with coefficients in F ” of an abelian variety over a global field of positive characteristic on which an order of an algebraic number field F acts, and we prove two propositions (2.4), (2.7) on the order of the L -series at $s=1$. This section depends entirely on the theory of étale cohomology. In § 3, we recall Drinfeld’s theory concerning Langlands correspondence and give the functional equation (3.14) of the L -series attached to some l -adic representation (or, equivalently, to some automorphic form). As in [19], Eichler-Shimura type congruence relation (3.9) will play a crucial role in investigating the Eisenstein quotient later. The formula for the ε -factor and its corollary (3.17) will be also used to prove main results. After these preliminaries, we investigate the Eisenstein ideal of the Hecke algebra in § 4, and give the proof of main results (5.1), (5.7) in § 5. In Appendix, we prove that $\text{End}_{\bar{k}}(J) \otimes_{\mathbb{Z}} \mathbb{Q}$ is generated by Hecke operators as a \mathbb{Q} -algebra. This is an analogue of a result of Ribet [24].

Usual notations are employed freely :

$$\mathbb{F}_q, \mathbb{Z}, \mathbb{Q}, \mathbb{Q}_l, \mathbb{C}; \text{Hom}, \text{End}, \text{Aut}, \text{Gal}; \text{etc.}$$

We shall fix some other notations here.

For a finite set \mathcal{S} ,

$$\#\mathcal{S} = \text{the cardinal number of } \mathcal{S}.$$

For a module M and $f \in \text{End}(M)$,

$$M[f] = \{x \in M \mid fx = 0\},$$

$$M[f^\infty] = \bigcup_{n \geq 0} M[f^n].$$

For an integer $l \in \mathbb{Z}$, we write $M[l]$ and $M[l^\infty]$ instead of $M[l \cdot \text{id}_M]$ and $M[(l \cdot \text{id}_M)^\infty]$ respectively. Moreover, when l is a prime number,

$$T_l(M) = \varprojlim M[l^n],$$

$$V_l(M) = T_l(M) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

Similar notations are employed for commutative group schemes, abelian sheaves, etc.

For a group G and a G -module M ,

$$M^G = \{x \in M \mid \sigma x = x \text{ for any } \sigma \in G\}.$$

For a field k ,

\bar{k} = an algebraic closure of k ,

k^{sep} = a separable closure of k .

Acknowledgement

This paper is essentially the author’s master’s thesis at the University of Tokyo. He would like to express his sincere gratitude to his advisor Kazuya Kato, under whose direction this work was completed. He is also very grateful to Takayuki Oda and Fumiyuki Momose for their helpful advice and warm encouragement and to Yuichiro Taguchi and Takuya Konno for their useful advice.

§ 1. l -Primary Admissible Groups

Let S be an irreducible locally noetherian normal scheme of dimension 1 and S' a non-empty open subscheme of S . We denote by K the function field of S .

Example (1.1).

$$\begin{aligned}
 S &= \mathbf{P}_{\mathbb{F}_q}^1, \\
 S' &= \mathbf{P}_{\mathbb{F}_q}^1 - \{\infty, \mathfrak{n}\} = \text{Spec}\mathbb{F}_q[T] - \{\mathfrak{n}\}, \\
 K &= \mathbb{F}_q(T),
 \end{aligned}$$

where T is an indeterminate and \mathfrak{n} is a maximal ideal of $\mathbb{F}_q[T]$.

In this section, we define admissible groups over S (with respect to S'), and give an estimate of their étale cohomology groups in the case of (1.1).

Fix a prime number l which is invertible in $\Gamma(S, \mathcal{O}_S)$. We shall define two categories \mathcal{C}, \mathcal{D} which turn out to be equivalent to each other.

The category \mathcal{C} is a full subcategory of (group schemes / S). A group scheme G over S is an object of \mathcal{C} if and only if

- (i) G is commutative ; G is flat, separated, and of finite type over S ,
- (ii) $G \times_S S'$ is finite over S' , and
- (iii) $l^N \cdot id_G = 0$ in $\text{End}(G/S)$ for some $N \geq 0$.

Remark (1.2). An object G/S of \mathcal{C} is automatically étale. In fact, the condition (iii) implies that $l^N \text{Lie}(G/S) = 0$, so $\text{Lie}(G/S) = 0$, which assures that G is étale over S .

Example (1.3). Let B be an abelian variety which has good reduction at each closed point of S' . Then $\mathcal{B}[I^r]$ ($r \geq 0$), $\mathcal{B}^0[I^r]$ ($r \geq 0$) are objects of \mathcal{C} , where \mathcal{B} is the Néron model over S of B and \mathcal{B}^0 is the “connected component” of \mathcal{B} .

Next we shall define the category \mathcal{D} . We fix a separable closure K^{sep} of K and for each $x \in S - S'$ we fix the following commutative diagram :

$$(1.4) \quad \begin{array}{ccccc} K^{\text{sep}} & \leftarrow & \mathcal{O}_{S,x}^{\text{sh}} & \longrightarrow & \kappa(x)^{\text{sep}} \\ \uparrow & \circlearrowleft & \uparrow & \circlearrowleft & \uparrow \\ K & \leftarrow & \mathcal{O}_{S,x} & \longrightarrow & \kappa(x) \end{array} ,$$

where $\kappa(x)^{\text{sep}}$ is a separable closure of the residue field $\kappa(x)$ of $\mathcal{O}_{S,x}$ and $\mathcal{O}_{S,x}^{\text{sh}}$ is a strict henselization of $\mathcal{O}_{S,x}$. Then we get the decomposition group D_x and the inertia group I_x :

$$(1.5) \quad \text{Gal}(K^{\text{sep}}/K) \supset D_x \supset I_x.$$

An object of \mathcal{D} is a family $(M, (M_x)_{x \in S - S'})$, where M is an l -primary finite discrete $\text{Gal}(K^{\text{sep}}/K)$ -module which is unramified everywhere on S' and, for each $x \in S - S'$, M_x is a D_x -submodule of M on which I_x acts trivially. A morphism $(M, (M_x)_{x \in S - S'}) \rightarrow (N, (N_x)_{x \in S - S'})$ is a $\text{Gal}(K^{\text{sep}}/K)$ -homomorphism $M \rightarrow N$ which sends M_x into N_x for all $x \in S - S'$.

We denote by Φ the functor $\mathcal{C} \rightarrow \mathcal{D}$ which sends an object G/S of \mathcal{C} to $(G(K^{\text{sep}}), (\text{Image}(G(\mathcal{O}_{S,x}^{\text{sh}}) \rightarrow G(K^{\text{sep}})))_{x \in S - S'})$ and a morphism $f : G \xrightarrow{S} H$ of \mathcal{C} to the $\text{Gal}(K^{\text{sep}}/K)$ -homomorphism $G(K^{\text{sep}}) \rightarrow H(K^{\text{sep}})$ induced by f .

Proposition (1.6). $\Phi : \mathcal{C} \xrightarrow{\sim} \mathcal{D}$ (category equivalence).

Proof. Using elementary étale sheaf theory, we can easily prove that Φ is full and faithful (cf. [21, II, 3.10, 3.12, 3.16]). Note that the separatedness of G/S implies the injectivity of the map $G(\mathcal{O}_{S,x}^{\text{sh}}) \rightarrow G(K^{\text{sep}})$.

We shall prove that Φ is essentially surjective. Let $(M, (M_x)_{x \in S - S'})$ be an object of the category \mathcal{D} . By Galois theory, there exists a finite étale scheme G_K over K with an isomorphism of $\text{Gal}(K^{\text{sep}}/K)$ -sets $G_K(K^{\text{sep}}) \simeq M$ and this isomorphism induces on G_K a structure of commutative group scheme over K . Let G_0 be the normalization of S in G_K and G_1 be the maximal open subscheme of G_0 that is étale over S (i.e. G_1 is the complement of the support of $\Omega_{G_0/S}^1$). By definition, we can easily show that G_1 is isomorphic to $(i_K)_* G_K$ as a (sets)-valued sheaf on the étale site on S , where i_K is the natural morphism $\text{Spec } K \rightarrow S$. This isomorphism induces on G_1 a structure of commutative étale group scheme over S .

For each $x \in S - S'$, $G_1 \times_S \kappa(x)$ is a finite étale scheme over $\kappa(x)$ and we have

$$\begin{array}{ccccc}
 (G_1 \times_S \kappa(x))(\kappa(x)^{\text{sep}}) \leftarrow G_1(\mathcal{O}_{S,x}^{\text{sh}}) \xrightarrow{\sim} & G_K(K^{\text{sep}})^{I_x} & \subset & G_K(K^{\text{sep}}) & \\
 & \wr & & \wr & \\
 & M^{I_x} & \subset & M & \\
 & \cup & & & \\
 & M_x & & & .
 \end{array}$$

Since M_x is a $D_x/I_x (= \text{Gal}(\kappa(x)^{\text{sep}}/\kappa(x)))$ -submodule of M^{I_x} , there exists a (unique) open and closed subscheme H_x of $G_1 \times_S \kappa(x)$ such that $H_x(\kappa(x)^{\text{sep}}) \simeq M_x$ via the isomorphism above.

Define G to be the open subscheme $G_1 - \bigcup_{x \in S-S'} (G_1 \times_S \kappa(x) - H_x)$ of G_1 . Then a structure of commutative group scheme over S is induced on G from that of G_1 . By construction, G is an object of \mathcal{C} and $\Phi(G) \simeq (M, (M_x)_{x \in S-S'})$. This completes the proof. ■

Lemma (1.7). *Let*

$$G_1 \rightarrow G_2 \rightarrow G_3$$

be a sequence in \mathcal{C} and we set $\Phi(G_i) = (M_i, (M_{i,x})_{x \in S-S'})$ ($i = 1, 2, 3$). Then the following two conditions are equivalent :

- (i) *the sequence above is exact as a sequence of sheaves on the étale site on S ;*
- (ii) *the sequence*

$$\Phi(G_1) \rightarrow \Phi(G_2) \rightarrow \Phi(G_3)$$

in \mathcal{D} obtained by applying Φ to the sequence above is exact in the sense that

$$M_1 \rightarrow M_2 \rightarrow M_3$$

is exact and

$$M_{1,x} \rightarrow M_{2,x} \rightarrow M_{3,x}$$

is exact for all $x \in S-S'$.

Proof. Rephrasing the condition (i) in terms of stalks, we obtain the condition (ii). ■

Lemma (1.8). *Let G be an object of \mathcal{C} and set $\Phi(G) = (M, (M_x)_{x \in S-S'})$. For any given exact sequence*

$$0 \rightarrow L \rightarrow M \rightarrow N \rightarrow 0$$

of $\text{Gal}(K^{\text{sep}}/K)$ -modules, there exists a sequence

$$(*) \quad 0 \rightarrow F \rightarrow G \rightarrow H \rightarrow 0$$

in \mathcal{C} which is exact as a sequence of sheaves on the étale site on S , such that there exists the following commutative diagram of $\text{Gal}(K^{\text{sep}}/K)$ -modules

$$\begin{array}{ccccccccc} 0 & \rightarrow & F(K^{\text{sep}}) & \rightarrow & G(K^{\text{sep}}) & \rightarrow & H(K^{\text{sep}}) & \rightarrow & 0 \\ & & \wr & & \wr & & \wr & & \\ 0 & \rightarrow & L & \rightarrow & M & \rightarrow & N & \rightarrow & 0. \end{array}$$

The sequence $(*)$ is determined uniquely (up to isomorphism) by the condition above.

Proof. For each $x \in S - S'$, let L_x be the inverse image of M_x in L and N_x the image of M_x in N . Take a sequence

$$0 \rightarrow F \rightarrow G \rightarrow H \rightarrow 0$$

in \mathcal{C} which corresponds to the sequence

$$0 \rightarrow (L, (L_x)_{x \in S - S'}) \rightarrow (M, (M_x)_{x \in S - S'}) \rightarrow (N, (N_x)_{x \in S - S'}) \rightarrow 0$$

via Φ . By (1.7), this satisfies the condition. The uniqueness can be easily seen. ■

Definition. Let G be an object of \mathcal{C} and set $\Phi(G) = (M, (M_x)_{x \in S - S'})$. We define the following invariants :

$$\begin{aligned} \rho(G) &= \text{length}_{\mathbf{Z}\text{-mod}} M = \log_l \# M, \\ \delta_x(G) &= \rho(G) - \text{length}_{\mathbf{Z}\text{-mod}} M_x = \log_l (M : M_x) \quad (x \in S - S'), \\ h^i(G) &= \text{length}_{\mathbf{Z}\text{-mod}} H_{\text{ét}}^i(S, G) = \log_l \# H_{\text{ét}}^i(S, G). \end{aligned}$$

If $H_{\text{ét}}^i(S, G)$ is not a finite module, then we set $h^i(G) = \infty$.

Remark (1.9).

(i) Since $G(S) \hookrightarrow G(K) \hookrightarrow G(K^{\text{sep}}) = M$,

$$h^0(G) \leq \rho(G) < \infty.$$

(ii) Let

$$0 \rightarrow G_1 \rightarrow G_2 \rightarrow G_3 \rightarrow 0$$

be a sequence in \mathcal{C} which is exact as a sequence of sheaves on the étale site on S . Then

$$f(G_2) = f(G_1) + f(G_3)$$

for $f = \rho, \delta_x$ and

$$g(G_2) \leq g(G_1) + g(G_3)$$

for $g = h^i, h^1 - h^0$ (or, more generally, $\sum_{i=0}^{2k+1} (-1)^{i+1} h^i$, if $h^i(G_j) < \infty$ for $0 \leq i \leq 2k, j = 1, 2, 3$).

Definition.

- (i) We say that an l -primary finite discrete $\text{Gal}(K^{\text{sep}}/K)$ -module M is *admissible* if the composition factors of the $\text{Gal}(K^{\text{sep}}/K)$ -module M are isomorphic either to $\mathbb{Z}/l\mathbb{Z}$ or to $\mu_l(K^{\text{sep}})$.
- (ii) We say that an object G of \mathcal{C} is *admissible* if the $\text{Gal}(K^{\text{sep}}/K)$ -module $G(K^{\text{sep}})$ is admissible in the sense of (i).

Lemma (1.10). *Let G be an object of \mathcal{C} and we set $m = \rho(G)$. If G is admissible, then there exist $2m + 1$ objects $G_i (i = 0, \dots, m), H_i (i = 1, \dots, m)$ of \mathcal{C} which satisfy the following conditions :*

- (i) $G_0 = G, G_m = 0$;
- (ii) for each $i = 1, \dots, m$, there exists a sequence

$$0 \rightarrow G_i \rightarrow G_{i-1} \rightarrow H_i \rightarrow 0$$

in \mathcal{C} which is exact as a sequence of sheaves on the étale site on S ;

- (iii) for all $i = 1, \dots, m$, the $\text{Gal}(K^{\text{sep}}/K)$ -module $H_i(K^{\text{sep}})$ is isomorphic either to $\mathbb{Z}/l\mathbb{Z}$ or to $\mu_l(K^{\text{sep}})$.

Proof. Using (1.7), (1.8), (1.9), we can prove the lemma by induction on $m = \rho(G)$. ■

We shall turn to the special case (1.1).

Proposition (1.11). *In the case of (1.1), we have the following inequality :*

$$h^1(G) - h^0(G) \leq \delta_n(G) (< \infty),$$

where G is an admissible object of \mathcal{C} .

Proof. By (1.9)(ii) ($f = \delta_n, g = h^1 - h^0$) and (1.10), the problem is reduced to checking the inequality in the case where the $\text{Gal}(K^{\text{sep}}/K)$ -module $G(K^{\text{sep}})$ is isomorphic either to $\mathbb{Z}/l\mathbb{Z}$ or to $\mu_l(K^{\text{sep}})$. In each case, there are (up to isomorphism) four cases. (Use (1.6).) By some elementary computation in étale cohomology (cf. [19], where *fppf* cohomology is involved), we establish the following table :

$G(K^{\text{sep}})$	$\delta_\infty(G)$	$\delta_n(G)$	$h^0(G)$	$h^1(G)$	$h^1(G) - h^0(G)$
$\mathbb{Z}/l\mathbb{Z}$	0	0	1	1	0
"	1	0	0	0	0
"	0	1	0	$\begin{cases} 0 & l \nmid d \\ 1 & l \mid d \end{cases}$	$\begin{cases} 0 & l \nmid d \\ 1 & l \mid d \end{cases}$
"	1	1	0	1	1
$\mu_l(K^{\text{sep}})$	0	0	$\begin{cases} 0 & l \nmid q-1 \\ 1 & l \mid q-1 \end{cases}$	$\begin{cases} 0 & l \nmid q-1 \\ 1 & l \mid q-1 \end{cases}$	0
"	1	0	0	0	0
"	0	1	0	$\begin{cases} 0 & l \nmid \frac{q^d-1}{q-1} \\ 1 & l \mid \frac{q^d-1}{q-1} \end{cases}$	$\begin{cases} 0 & l \nmid \frac{q^d-1}{q-1} \\ 1 & l \mid \frac{q^d-1}{q-1} \end{cases}$
"	1	1	0	$\begin{cases} 0 & l \nmid q^d-1 \\ 1 & l \mid q^d-1 \end{cases}$	$\begin{cases} 0 & l \nmid q^d-1 \\ 1 & l \mid q^d-1 \end{cases}$

where $d = \deg n = [\kappa(n) : \mathbb{F}_q]$. In all the cases, the inequality holds. ▣

§ 2. *L*-series of Abelian Varieties

Let F be an algebraic number field and R an order of F . We shall recall the definition of the “*L*-series with coefficients in F ” of an abelian variety over a global field of positive characteristic on which R acts.

We need some lemmas to define the local factors of the *L*-series. (Note that we have only to refer to [29] and [23] for good primes. For bad primes, there seem to be no suitable references.)

Lemma (2.1). *Let k be a field and G a commutative algebraic group over k equipped with a ring homomorphism $R \rightarrow \text{End}_k(G)$. (By an algebraic group we mean a group scheme smooth of finite type over a field.) Let l be any prime number distinct from the characteristic of k . Then :*

- (i) $V_l(G(\bar{k}))$ is a free $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -module of finite rank which is independent of the choice of l .

(ii) Assume that k is a finite field. Let φ_k be the $(\#k)$ -th power Frobenius element in $\text{Gal}(\bar{k}/k)$. (Note that φ_k acts on $G(\bar{k})$ and that its action commutes with that of R .) Then the characteristic polynomial of φ_k in the free $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -module $V_l(G(\bar{k}))$ has coefficients in F , when we regard F as a subring of $R \otimes_{\mathbb{Z}} \mathbb{Q}_l = F \otimes_{\mathbb{Q}} \mathbb{Q}_l$, and is independent of the choice of l .

Proof. (i) Using the structure theorem for commutative algebraic groups ([1], [8], [26]), we can easily reduce the problem to the case where G is either an abelian variety or a torus. Since $V_l(G(\bar{k}))$ is a \mathbb{Q}_l -vector space of finite dimension which is independent of l , we have only to show that $V_l(G(\bar{k}))$ is a free $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -module.

For each $f \in \text{End}_{\bar{k}}(G)$, the characteristic polynomial of f in the \mathbb{Q}_l -vector space $V_l(G(\bar{k}))$ has coefficients in \mathbb{Q} . In fact, when G is an abelian variety, this is well-known ([22, IV, 19, Theorem 4]) and when G is a torus, it is easily seen. (We may assume $G = (\mathbf{G}_m)^n$ and then the following diagram is commutative :

$$\begin{array}{ccc} \text{End}_{\bar{k}}(G) & \simeq & M_n(\mathbb{Z}) \\ \downarrow & & \downarrow \\ \text{End}_{\mathbb{Q}_l}(V_l(G(\bar{k}))) & \simeq & M_n(\mathbb{Q}_l). \end{array}$$

In particular, the characteristic polynomial of $f \in R$ in the \mathbb{Q}_l -vector space $V_l(G(\bar{k}))$ has coefficients in \mathbb{Q} and then the same statement holds for $f \in F = R \otimes_{\mathbb{Z}} \mathbb{Q}$. This implies that $V_l(G(\bar{k}))$ is free as an $R \otimes_{\mathbb{Z}} \mathbb{Q}_l (= F \otimes_{\mathbb{Q}} \mathbb{Q}_l)$ -module ([30, II, Lemma 1]).

(ii) Again by using the structure theorem, we can reduce the problem to the case where G is either an abelian variety or a torus. Then $\text{End}_k(G)$ is a free \mathbb{Z} -module of finite rank and the given homomorphism $R \rightarrow \text{End}_k(G)$ is injective unless $G = 0$.

Let $f_k \in \text{End}_k(G)$ be the Frobenius endomorphism attached to the finite field k . The action of f_k on $G(\bar{k})$ coincides with that of φ_k . We denote by $R[f_k]$ (resp. $\mathbb{Z}[f_k]$) the subring of $\text{End}_k(G)$ generated by f_k over the image of R (resp. \mathbb{Z}). Then the commutative \mathbb{Q} -subalgebra $R[f_k] \otimes_{\mathbb{Z}} \mathbb{Q}$ of $\text{End}_k(G) \otimes_{\mathbb{Z}} \mathbb{Q}$ is semi-simple. In fact, $\mathbb{Z}[f_k] \otimes_{\mathbb{Z}} \mathbb{Q}$, which is included in the center of the semi-simple \mathbb{Q} -algebra $\text{End}_k(G) \otimes_{\mathbb{Z}} \mathbb{Q}$, has no non-trivial nilpotent elements, hence it is semi-simple, and so is $F \otimes_{\mathbb{Q}} (\mathbb{Z}[f_k] \otimes_{\mathbb{Z}} \mathbb{Q})$. Being a quotient of the semi-simple \mathbb{Q} -algebra $F \otimes_{\mathbb{Q}} (\mathbb{Z}[f_k] \otimes_{\mathbb{Z}} \mathbb{Q})$, $R[f_k] \otimes_{\mathbb{Z}} \mathbb{Q}$ is also semi-simple.

Let

$$R[f_k] \otimes_{\mathbb{Z}} \mathbb{Q} \simeq F_1 \times \cdots \times F_t$$

be a decomposition into a direct product of fields, where F_i is a finite extension of \mathbb{Q} for each $i = 1, \dots, t$. We define the ideal I_i of $R[f_k]$ to be the kernel of

$$R[f_k] \rightarrow R[f_k] \otimes_{\mathbb{Z}} \mathbb{Q} \simeq F_1 \times \cdots \times F_t \xrightarrow{\text{proj.}} F_i,$$

and set $G_i = G/I_i G$. We can easily check that the morphism $G \rightarrow G_1 \times \cdots \times G_t$ induces a canonical isomorphism

$$V_l(G(\bar{k})) \xrightarrow{\sim} V_l(G_1(\bar{k})) \times \cdots \times V_l(G_t(\bar{k})),$$

which is identified with the decomposition associated with the ring decomposition $R[f_k] \otimes_{\mathbb{Z}} \mathbb{Q}_l \simeq (F_1 \otimes_{\mathbb{Q}} \mathbb{Q}_l) \times \cdots \times (F_t \otimes_{\mathbb{Q}} \mathbb{Q}_l)$. It suffices to verify the statement of (ii) for each $G_i (i=1, \dots, t)$, so we may assume that $R[f_k] \otimes_{\mathbb{Z}} \mathbb{Q}$ is a field (which is necessarily an algebraic number field) and that $R[f_k]$ is an order of the algebraic number field.

Then we can apply (i) to the ring homomorphism $R[f_k] \rightarrow \text{End}_k(G)$. The $R[f_k] \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -module $V_l(G(\bar{k}))$ is free of finite rank m which is independent of l . The polynomial in question is equal to the m -th power of the characteristic polynomial of f_k in the field extension $R[f_k] \otimes_{\mathbb{Z}} \mathbb{Q}/F$, so it has coefficients in F and is independent of the choice of l . ■

Let K be a discrete valuation field with finite residue field k . Fix an extension to \bar{K} of the given valuation on K , so that we get the decomposition group D , the inertia group I , and the isomorphism $D/I \xrightarrow{\sim} \text{Gal}(\bar{k}/k)$. Let φ_k be the $(\#k)$ -th power Frobenius element in $\text{Gal}(\bar{k}/k)$.

Let B be an abelian variety over K equipped with a ring homomorphism $R \rightarrow \text{End}_k(B)$. For a prime number $l \neq \text{char.}(k)$, $\text{Gal}(K^{\text{sep}}/K)$ acts on the Tate module $V = V_l(B(\bar{k}))$, and its action commutes with that of R . Moreover, R and $\text{Gal}(K^{\text{sep}}/K)$ act on $V^* = \text{Hom}_{\mathbb{Q}_l}(V, \mathbb{Q}_l)$, as follows :

$$\begin{aligned} (ah)(x) &= h(ax) \quad (h \in V^*, a \in R, x \in V), \\ (oh)(x) &= \sigma(h(\sigma^{-1}x)) = h(\sigma^{-1}x) \quad (h \in V^*, \sigma \in \text{Gal}(K^{\text{sep}}/K), x \in V). \end{aligned}$$

Lemma (2.2). *Notations and assumptions as above. Let W be either V^l or $(V^*)^l$.*

- (i) *W is a free $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -module of finite rank which is independent of the choice of l .*
- (ii) *The characteristic polynomial of φ_k in the free $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -module W has coefficients in F , and is independent of the choice of l .*

Proof. Let O_K be the valuation ring of K and \mathcal{B} the Néron model over O_K of B . Then R acts on the commutative algebraic group $\mathcal{B} \otimes_{O_K} k$ over k , as follows :

$$R \rightarrow \text{End}_K(B) \xleftarrow{\sim} \text{End}_{O_K}(\mathcal{B}) \rightarrow \text{End}_k(\mathcal{B} \otimes_{O_K} k).$$

Since the isomorphism

$$(V_l(B(\bar{K})))^l \xleftarrow{\sim} V_l(\mathcal{B}(\mathcal{O}_{\bar{K}})) \xrightarrow{\sim} V_l((\mathcal{B} \otimes_x k)(\bar{k}))$$

is compatible with the actions of R and $\text{Gal}(\bar{k}/k)$, (i) and (ii) for $W = V^l$ follow from (i) and (ii) of (2.1) respectively.

Let B' be the dual abelian variety of B . Then R acts on B' via the anti-isomorphism $\text{End}_K(B) \xrightarrow{\sim} \text{End}_K(B')$. The isomorphism

$$\begin{aligned} \text{Hom}_{\mathbb{Q}_l}(V_l(B(\bar{K})), \mathbb{Q}_l) &\simeq \text{Hom}_{\mathbb{Q}_l}(V_l(B(\bar{K})), \mathbb{Q}_l(1)) \otimes_{\mathbb{Q}_l} \mathbb{Q}_l(-1) \\ &\simeq V_l(B'(\bar{K})) \otimes_{\mathbb{Q}_l} \mathbb{Q}_l(-1) \end{aligned}$$

is compatible with the actions of R and $\text{Gal}(K^{\text{sep}}/K)$, so the isomorphism

$$(V^*)^l \simeq (V_l(B'(\bar{K})))^l \otimes_{\mathbb{Q}_l} \mathbb{Q}_l(-1)$$

is compatible with the actions of R and $\text{Gal}(\bar{k}/k)$. Thus, (i) and (ii) for $(V^*)^l$ follow immediately from (i) and (ii) for $(V_l(B'(\bar{K})))^l$ respectively. ■

Let S be a smooth proper geometrically connected curve over the finite field \mathbb{F}_q and denote by K the function field of S . For each closed point x of S , we fix a commutative diagram (1.4) (hence (1.5)). Let φ_x be the $(\#\kappa(x))$ -th power Frobenius element in $\text{Gal}(\bar{\kappa}(x)/\kappa(x)) \simeq D_x/I_x$. We shall define the “ L -series with coefficients in F ” for an abelian variety B over K equipped with a ring homomorphism $R \rightarrow \text{End}_K(B)$.

We choose a prime number l which does not divide q . For each closed point x of S , we set

$$\begin{aligned} P_x(u; F) &:= \det(id - \varphi_x^{-1} u^{\text{deg } x} \mid (V_l(B(\bar{K})))^*{}^{l_x}; R \otimes_{\mathbb{Z}} \mathbb{Q}_l), \\ Q_x(t; F) &:= \det(t \cdot id - \varphi_x \mid (V_l(B(\bar{K})))^*{}^{l_x}; R \otimes_{\mathbb{Z}} \mathbb{Q}_l), \end{aligned}$$

where $V; R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ means that V is considered as an $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -module when we take the determinant. From (2.2), $Q_x(t; F)$ is in $F[t]$ and is independent of l . Since

$$P_x(u; F) = Q_x(0; F)^{-1} Q_x(u^{\text{deg } x}; F),$$

we see that $P_x(u; F)$ is in $F[u^{\text{deg } x}] \subset F[u]$ and is independent of l .

Definition.

$$Z_B(u; F) := \prod_{\substack{x: \text{closed} \\ \text{point of } S}} P_x(u; F)^{-1} \in F[[u]].$$

(Note that there are finitely many x with $\deg x \leq N$ for each $N \in \mathbb{N}$ and that, for each x , $P_x(0; F) = 1$.)

Let B' be the dual abelian variety of B and let \mathcal{B} (resp. \mathcal{B}') be the Néron model over S of B (resp. of B'). As we have seen in the proof of (2.2), the isomorphism

$$(V_l(B(\bar{K}))^*)^{I_x} \simeq (V_l(B'(\bar{K})))^{I_x} \otimes_{\mathbb{Q}_l} \mathbb{Q}_l(-1)$$

exists, hence

$$\begin{aligned} P_x(q^{-1}u; F) &= \det(id - \varphi_x^{-1}u^{\deg x} \mid (V_l(B'(\bar{K})))^{I_x}; R \otimes_{\mathbb{Z}} \mathbb{Q}_l) \\ &= \det(id - \varphi_x^{-1}u^{\deg x} \mid V_l(\mathcal{B}')_{\bar{x}}; R \otimes_{\mathbb{Z}} \mathbb{Q}_l), \end{aligned}$$

where $V_l(\mathcal{B}')_{\bar{x}}$ is the stalk at \bar{x} of the étale \mathbb{Q}_l -sheaf $V_l(\mathcal{B}')$. Then by the theory of étale cohomology, we conclude that

$$Z_B(q^{-1}u; F) = \prod_{i=0}^2 \det(id - \varphi^{-1}u \mid H_{\text{ét}}^i(\bar{S}, V_l(\mathcal{B}'))); R \otimes_{\mathbb{Z}} \mathbb{Q}_l)^{(-1)^{i+1}},$$

where $\bar{S} = S \otimes_{\mathbb{F}_q} \bar{\mathbb{F}}_q$ and φ is the q -th power Frobenius element in $\text{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$. (Note that “det” makes sense since $H_{\text{ét}}^i(\bar{S}, V_l(\mathcal{B}'))$ is at least a finitely generated locally free $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -module.) Since $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ is a direct product of fields and, for an extension E/F of fields, $F((u)) \cap E(u) = F(u)$ (cf. [2, Part III, Chapter I, Lemma 1]), it follows that $Z_B(q^{-1}u; F) \in F(u)$, hence $Z_B(u; F) \in F(u)$. Moreover, the weight theory ([6, 3.2.3]) implies that, for each $i = 0, 1, 2$,

$$\det(id - \varphi^{-1}u \mid H_{\text{ét}}^i(\bar{S}, V_l(\mathcal{B}'))); R \otimes_{\mathbb{Z}} \mathbb{Q}_l$$

is in $F[[u]]$ (thereby $H_{\text{ét}}^i(\bar{S}, V_l(\mathcal{B}'))$ turns out to be a free $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -module) and it is independent of l . (Observe that, if we choose a non-empty open subscheme U of S over which $\mathcal{B}' \times_S U$ is proper, $V_l(\mathcal{B}')$ is isomorphic to $j_* (V_l(\mathcal{B}' \times_S U))$, where $j: U \rightarrow S$.)

Definition.

$$\rho_F := (\text{the order at } u = q^{-1} \text{ of } Z_B(u; F) \in F(u)),$$

$$r_F := \dim_F(B(K) \otimes_{\mathbb{Z}} \mathbb{Q}),$$

and for a prime number $l \neq \text{char.}(\mathbb{F}_q)$ and a field E which appears as a component in the direct product decomposition of $R \otimes_{\mathbb{Z}} \mathbb{Q}_l = F \otimes_{\mathbb{Z}} \mathbb{Q}_l$,

$$\sigma_{F, l, E} := \dim_E e' H_{\text{ét}}^1(S, V_l(\mathcal{B}')),$$

where e is the idempotent of $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ which corresponds to E (i.e. $E = R \otimes_{\mathbb{Z}} \mathbb{Q}_l / (1 - e)$) and $'$ means the action on B', \mathcal{B}' , etc. (See the proof of (2.2) .)

Remark (2.3). Let ρ, r, σ_l denote $\rho_{\mathbb{Q}}, r_{\mathbb{Q}}, \sigma_{\mathbb{Q}, l, \mathbb{Q}_l}$ respectively. Then we can easily check the following equalities :

$$\begin{aligned} \rho &= [F : \mathbb{Q}] \rho_F, \\ r &= [F : \mathbb{Q}] r_F, \\ \sigma_l &= \sum_E [E : \mathbb{Q}_l] \sigma_{F, l, E}. \end{aligned}$$

From now on, we fix a pair (l, E) .

Proposition (2.4). (cf. [27].)

- (i) $\rho_F \geq \sigma_{F, l, E} \geq r_F \geq 0$.
- (ii) If $\sigma_{F, l, E} = 0$, then $\rho_F = \sigma_{F, l, E} = r_F = 0$.

Proof. First we note that $V_l(\mathcal{B}') = V_l(\mathcal{B}'^0)$, where \mathcal{B}'^0 is the “connected component” of \mathcal{B}' . From the Kummer sequence for \mathcal{B}'^0 , we have the following exact sequence of $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -modules :

$$0 \rightarrow \mathcal{B}'^0(S) \otimes_{\mathbb{Z}} \mathbb{Q}_l \rightarrow H^1(S, V_l(\mathcal{B}'^0)) \rightarrow V_l(H^1(S, \mathcal{B}'^0)) \rightarrow 0.$$

(Note that $\mathcal{B}'^0(S)$ is a finitely generated \mathbb{Z} -module.) Considering the E -part of this exact sequence, we obtain $r_F \leq \sigma_{F, l, E}$.

On the other hand, since $\text{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q) \simeq \hat{\mathbb{Z}}$ has cohomological dimension 1, the Hochschild-Serre spectral sequence gives the following exact sequence of $R \otimes_{\mathbb{Z}} \mathbb{Q}_l$ -modules :

$$0 \rightarrow H^1(\mathbb{F}_q, H^0(\overline{S}, V_l(\mathcal{B}'))) \rightarrow H^1(S, V_l(\mathcal{B}')) \rightarrow H^0(\mathbb{F}_q, H^1(\overline{S}, V_l(\mathcal{B}'))) \rightarrow 0,$$

where $H^i(\mathbb{F}_q, H^j(\overline{S}, V_l(\mathcal{B}'))) := (\varprojlim H^i(\mathbb{F}_q, H^j(\overline{S}, \mathcal{B}'[l^r]))) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Now since

$$\#H^1(\mathbb{F}_q, H^0(\overline{S}, \mathcal{B}'[l^r])) = \#H^0(\mathbb{F}_q, H^0(\overline{S}, \mathcal{B}'[l^r]))$$

$$\begin{aligned}
 &= \# \mathcal{B}' [l'] (S) \\
 &\leq \# \mathcal{B}' (K) [l^\infty] \quad (\text{bounded}),
 \end{aligned}$$

we see that $H^1(\mathbb{F}_q, H^0(\bar{S}, V_i(\mathcal{B}')))=0$, hence

$$H^1(S, V_i(\mathcal{B}')) \simeq H^0(\mathbb{F}_q, H^1(\bar{S}, V_i(\mathcal{B}'))).$$

Considering the E -part, we deduce :

$$\begin{aligned}
 \sigma_{F, l, E} &= (\text{the dimension over } E \text{ of the eigenspace of } \varphi \text{ with eigenvalue} \\
 &\quad \text{1 in the } E\text{-vector space } e' H^1(\bar{S}, V_i(\mathcal{B}')) \\
 &\quad (\text{i.e. } \dim_E e' H^1(\bar{S}, V_i(\mathcal{B}')) [\varphi - 1]) \\
 &\leq (\text{the dimension over } E \text{ of the generalized eigenspace of } \varphi \\
 &\quad \text{with eigenvalue 1 in the } E\text{-vector space } e' H^1(\bar{S}, V_i(\mathcal{B}')) \\
 &\quad (\text{i.e. } \dim_E e' H^1(\bar{S}, V_i(\mathcal{B}')) [(\varphi - 1)^\infty]) \\
 &= \rho_F ([6, 3.2.3]).
 \end{aligned}$$

If the eigenspace is $\{0\}$, then the generalized eigenspace is also $\{0\}$. Hence (ii) follows. ■

Remark (2.5). If we assume that $\# \text{III} (B/K) < \infty$ (or, more weakly, $\# \text{III} (B/K) [l'^\infty] < \infty$ for some number $l' \neq \text{char.}(\mathbb{F}_q)$), then we obtain $\rho = r$ ([27]), hence $\rho_F = \sigma_{F, l, E} = r_F$.

Next we fix a polarization $\lambda : B \rightarrow B'$ over K and consider the following condition :

(2.6) the image of $(R \rightarrow \text{End}_K(B))$ is invariant under the Rosati involution \dagger .

This condition requires that two homomorphisms

$$\begin{array}{ccc}
 R \rightarrow \text{End}_K(B) \otimes_{\mathbb{Z}} \mathbb{Q} & \xrightarrow{\text{anti-isom}} & \text{End}_K(B') \otimes_{\mathbb{Z}} \mathbb{Q} \\
 \cup & & \cup \\
 f & \longmapsto & f'
 \end{array}$$

and

$$\begin{array}{ccc}
 R \rightarrow \text{End}_K(B) \otimes_{\mathbb{Z}} \mathbb{Q} & \xrightarrow{\text{isom}} & \text{End}_K(B') \otimes_{\mathbb{Z}} \mathbb{Q} \\
 \cup & & \cup \\
 f & \longmapsto & \lambda f \lambda^{-1}
 \end{array}$$

are the same. If (2.6) holds, then the isomorphism (induced by λ)

$$H^1_{\text{ét}}(\bar{S}, V_l(\mathcal{B})) \xrightarrow{\sim} H^1_{\text{ét}}(\bar{S}, V_l(\mathcal{B}'))$$

induces an isomorphism

$$eH^1_{\text{ét}}(\bar{S}, V_l(\mathcal{B})) \xrightarrow{\sim} \lambda e \lambda^{-1} H^1_{\text{ét}}(\bar{S}, V_l(\mathcal{B}')) \stackrel{(2.6)}{=} e' H^1_{\text{ét}}(\bar{S}, V_l(\mathcal{B}')) .$$

Note that (2.6) is satisfied automatically when $(F, R) = (\mathbf{Q}, \mathbf{Z})$.

Proposition (2.7). *Under the assumption (2.6),*

$$\rho_F \equiv \sigma_{F, l, E} \pmod{2} .$$

Proof. The pairing

$$\begin{aligned} (\quad | \quad) : H^1(\bar{S}, V_l(\mathcal{B})) \times H^1(\bar{S}, V_l(\mathcal{B})) \\ \xrightarrow{id \times \lambda} H^1(\bar{S}, V_l(\mathcal{B})) \times H^1(\bar{S}, V_l(\mathcal{B}')) \\ \xrightarrow{\substack{\text{Weil pairing} \\ \text{cup product}}} H^2(\bar{S}, \mathbf{Q}_l(1)) = \mathbf{Q}_l \end{aligned}$$

is a non-degenerate bilinear form on the finite-dimensional \mathbf{Q}_l -vector space $H^1(\bar{S}, V_l(\mathcal{B}))$ ([21, v, 2.2c]). It is symmetric, since the Weil pairing is alternating.

For $\alpha \in R$,

$$(\alpha v | w) = (v | \alpha^\dagger w) \stackrel{(2.6)}{=} (v | \alpha w),$$

hence the same equality holds for $\alpha \in R \otimes_{\mathbf{Z}} \mathbf{Q}_l$. This implies that the decomposition of the $R \otimes_{\mathbf{Z}} \mathbf{Q}_l$ -module $H^1(\bar{S}, V_l(\mathcal{B}))$ associated with the direct product decomposition of $R \otimes_{\mathbf{Z}} \mathbf{Q}_l$ is an orthogonal sum decomposition with respect to the symmetric form $(\quad | \quad)$. Thus the restriction of the pairing to $eH^1(\bar{S}, V_l(\mathcal{B})) \times eH^1(\bar{S}, V_l(\mathcal{B}))$ is again non-degenerate and symmetric. Then (2.7) follows from the next lemma (2.8). ■

Lemma (2.8). *Let k be a field of characteristic $\neq 2$. Let V be a k -vector space of finite dimension equipped with a non-degenerate symmetric bilinear form $(\quad | \quad) : V \times V \rightarrow k$. If $f \in \text{End}_k(V)$ satisfies $(fv | fw) = (v | w)$ for all $v, w \in V$, then (the dimension over k of the generalized eigenspace of f with eigenvalue 1 in V) \equiv (the dimension over k of the eigenspace of f with eigenvalue 1 in V) (mod. 2).*

Proof. Considering $V \otimes_{\mathbf{k}} \bar{k}$ if necessary, we may assume $k = \bar{k}$.

First, the non-degeneracy of the pairing implies that f is injective, and then $f \in \text{Aut}_k(V)$ since V is of finite dimension. Thus the decomposition

$$V = \bigoplus_{\alpha \in k^*} V(\alpha)$$

exists, where $V(\alpha)$ is the generalized eigenspace of f with eigenvalue α in V (i.e. $V(\alpha) = V[(f-\alpha)^\infty]$).

We can easily show that $(V(\alpha) | V(\beta)) = 0$ unless $\alpha\beta = 1$. Then the restriction of the pairing to $V(1) \times V(1)$ is still non-degenerate, so we may assume that $V = V(1)$.

Put $V' = \{v \in V | (v | w) = 0 \text{ for all } w \in V[f-1]\}$. Then

$$V' = (f^{-1} - 1)V = (f-1)(-f^{-1})V = (f-1)V.$$

Since

$$\dim_k V' = \dim_k V - \dim_k V[f-1],$$

the problem is reduced to checking that $\dim_k V'$ is even.

As $(V[f-1] | V') = (V' | V[f-1]) = 0$, we can define a new pairing on $V' \times V'$ as follows:

$$\langle \quad | \quad \rangle : V' \times V' \longrightarrow k$$

$$\langle (f-1)v | (f-1)w \rangle = (v | (f-1)w) - ((f-1)v | w) \quad (v, w \in V).$$

This pairing becomes an alternating bilinear form on V' . If $v' = (f-1)v \in V'$ ($v \in V$) satisfies that $\langle v' | w' \rangle = 0$ for all $w' \in V'$, then for all $w \in V$,

$$\begin{aligned} 0 &= \langle v' | (f-1)w \rangle \\ &= \langle (f-1)v | (f-1)w \rangle \\ &= (v | (f-1)w) - ((f-1)v | w) \\ &= (v | (f^{-1}-1)(-f)w) - ((f-1)v | w) \\ &= ((f-1)v | -fw) - ((f-1)v | w) \\ &= (v' | -(f+1)w). \end{aligned}$$

Now $V = V(1)$ implies $(f+1)V = V$. (Note that $\text{char.}(k) \neq 2$.) Then it follows from the non-degeneracy of the pairing $(\quad | \quad)$ that $v' = 0$. Thus the pairing $\langle \quad | \quad \rangle$ is non-degenerate, and the k -vector space V' , having a non-degenerate alternating bilinear form, is even-dimensional. \blacksquare

§ 3. Drinfeld Modular Curves and Automorphic Forms

Notation.

$$S = \mathbf{P}_{\mathbf{F}_q}^1 = \mathbf{A}_{\mathbf{F}_q}^1 \cup \{\infty\} \quad (\infty = (1 : 0)),$$

$$A = \Gamma(S - \{\infty\}, \mathcal{O}_S) = \mathbf{F}_q[T] \quad (T : \text{indeterminate}),$$

$$K = \text{the function field of } S = \mathbf{F}_q(T),$$

$$\begin{aligned} \Sigma &= \{\text{the prime divisors of } K\} = \{\text{the closed points of } S\} \\ &= \{\text{the maximal ideals of } A\} \cup \{\infty\}, \end{aligned}$$

$$K_\nu : \text{the } \nu\text{-adic completion of } K (\nu \in \Sigma),$$

$$O_\nu : \text{the integer ring of the local field } K_\nu,$$

$$\mathbf{A}_K = \text{the adèle ring of } K = \prod'_{\nu \in \Sigma} K_\nu,$$

$$\mathbf{A}_K^\times = \text{the idele group of } K = \prod'_{\nu \in \Sigma} K_\nu^\times,$$

$$\hat{A} = \varprojlim_{\substack{I : \text{non-zero} \\ \text{ideal of } A}} A/I = \prod_{\nu \in \Sigma - \{\infty\}} O_\nu,$$

$$\mathbf{A}_K^f = \prod'_{\nu \in \Sigma - \{\infty\}} K_\nu,$$

$$\mathbf{A}_K^{f \times} = \prod'_{\nu \in \Sigma - \{\infty\}} K_\nu^\times,$$

$$C_\infty = \text{the } (\infty\text{-adic}) \text{ completion of an algebraic closure } \bar{K}_\infty \text{ of } K_\infty,$$

$$\Omega = \mathbf{A}^1(C_\infty) - \mathbf{A}^1(K_\infty) = \mathbf{P}^1(C_\infty) - \mathbf{P}^1(K_\infty).$$

In this section, we shall recall the relation between Drinfeld modular curves and automorphic forms. We refer the reader to [7], [9], [14] for Drinfeld modules and their moduli schemes, and to [15], [17], [25] for automorphic forms on GL_2 . See also [12].

⟨Generalities⟩

For an open subgroup H of $GL_2(\hat{A})$, M_H denotes the corresponding (coarse) moduli scheme of Drinfeld A -modules of rank 2, and Y_H denotes $M_H \otimes_A K$. The scheme Y_H is a smooth affine (not necessarily geometrically connected) curve over K . Define X_H to be the (unique) smooth compactification of Y_H over K .

From now on, fix a prime number l not dividing q . We denote by \mathcal{H} the

module $\varinjlim_{\substack{H : \text{open subgroup} \\ \text{of } GL_2(\bar{A})}} H^1_{\text{ét}}(X_H \otimes_{\bar{K}} K^{\text{sep}}, \bar{\mathbf{Q}}_l)$, on which $GL_2(\mathbf{A}_K^f) \times \text{Gal}(K^{\text{sep}}/K)$ acts.

Fixing an embedding $K^{\text{sep}} \hookrightarrow K_{\infty}^{\text{sep}}$, we have the following isomorphism of $GL_2(\mathbf{A}_K^f) \times \text{Gal}(K_{\infty}^{\text{sep}}/K_{\infty})$ -modules :

$$(3.1) \quad \mathcal{H} \simeq \text{Hom}_{GL_2(K_{\infty})}(V_{\text{sp}}, \mathcal{A}_0) \otimes W_{\infty},$$

where

$$\begin{aligned} \mathcal{A}_0 &= \mathcal{A}_0(GL_2(K) \backslash GL_2(\mathbf{A}_K)) \\ &= \text{the space of } (\bar{\mathbf{Q}}_l\text{-valued) cusp forms on } GL_2(\mathbf{A}_K), \end{aligned}$$

$$V_{\text{sp}} = \{f : \mathbf{P}^1(K_{\infty}) \rightarrow \bar{\mathbf{Q}}_l \mid \text{locally constant}\} / \{\text{constant functions}\}$$

(which gives an irreducible admissible representation σ_{sp} of $GL_2(K_{\infty})$ called the special representation), and

W_{∞} : the 2-dimensional l -adic representation of $\text{Gal}(K_{\infty}^{\text{sep}}/K_{\infty})$ which is determined up to isomorphism by the existence of the following non-split exact sequence of $\text{Gal}(K_{\infty}^{\text{sep}}/K_{\infty})$ -modules :

$$0 \rightarrow \mathbf{Q}_l \rightarrow W_{\infty} \rightarrow \mathbf{Q}_l(-1) \rightarrow 0.$$

Further, considering the decomposition

$$\mathcal{A}_0 = \bigoplus_{\pi \in \Pi} \pi, \quad \pi = \bigotimes_{v \in \Sigma} \pi_v,$$

where Π is a set of irreducible representations of $GL_2(\mathbf{A}_K)$, we obtain the following isomorphism of $GL_2(\mathbf{A}_K^f) \times \text{Gal}(K^{\text{sep}}/K)$ -modules :

$$(3.2) \quad \mathcal{H} \simeq \bigoplus_{\substack{\pi \in \Pi \\ \pi_{\infty} = \sigma_{\text{sp}}}} \left(\bigotimes_{v \in \Sigma - \{\infty\}} \pi_v \right) \otimes \rho(\pi),$$

where $\rho(\pi)$ is a 2-dimensional representation of $\text{Gal}(K^{\text{sep}}/K)$ over $\bar{\mathbf{Q}}_l$ which is determined by π and whose restriction to $\text{Gal}(K_{\infty}^{\text{sep}}/K_{\infty})$ is isomorphic to W_{∞} .

The Galois representation $\rho(\pi)$ corresponds to π in the sense of Langlands, that is to say, for each $v \in \Sigma$,

$$(3.3) \quad L\left(s - \frac{1}{2}, \pi_v\right) = L(s, \rho(\pi)_v).$$

Here we fixed an isomorphism $\bar{\mathbf{Q}}_l \simeq \mathbf{C}$ (and hereafter also). The equality (3.3) at an unramified place results from the Eichler-Shimura type congruence relation and

the general case is proved by using a result of [5] (cf. remark of [10]).

For a non-zero ideal \mathfrak{n}_v of \mathcal{O}_v , we set

$$H_0^v(\mathfrak{n}_v) = \left\{ \begin{pmatrix} a_v & b_v \\ c_v & d_v \end{pmatrix} \in GL_2(\mathcal{O}_v) \mid c_v \equiv 0 \pmod{\mathfrak{n}_v} \right\}$$

and for a non-zero ideal \mathfrak{n} of A , we set

$$H_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\hat{A}) \mid c \equiv 0 \pmod{\mathfrak{n}\hat{A}} \right\}.$$

Then $H_0(\mathfrak{n}) = \prod_{v \in \Sigma - \{\infty\}} H_0^v(\mathfrak{n}\mathcal{O}_v)$ is an open subgroup of $GL_2(\hat{A})$. Let $M_0(\mathfrak{n})$, $Y_0(\mathfrak{n})$, and $X_0(\mathfrak{n})$ denote $M_{H_0(\mathfrak{n})}$, $Y_{H_0(\mathfrak{n})}$, and $X_{H_0(\mathfrak{n})}$ respectively. These schemes have geometrically connected fibers over $\text{Spec } A$, $\text{Spec } K$ and $\text{Spec } K$ respectively, since $\text{Pic}(A) = 1$. We have the following isomorphisms (of rigid analytic spaces over C_∞):

$$(3.4) \quad \begin{array}{ccc} Y_0(\mathfrak{n})(C_\infty) & \simeq & \Gamma_0(\mathfrak{n}) \backslash \Omega \\ \downarrow & & \downarrow \\ X_0(\mathfrak{n})(C_\infty) & \simeq & \Gamma_0(\mathfrak{n}) \backslash (\Omega \cup \mathbf{P}^1(K)), \end{array}$$

where

$$\begin{aligned} \Gamma_0(\mathfrak{n}) &= H_0(\mathfrak{n}) \cap GL_2(A) \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A) \mid c \equiv 0 \pmod{\mathfrak{n}} \right\}. \end{aligned}$$

We denote by $J_0(\mathfrak{n})$ the Jacobian variety of $X_0(\mathfrak{n})$ and by $\mathcal{J}_0(\mathfrak{n})$ the Néron model over S of $J_0(\mathfrak{n})$. It is known that $J_0(\mathfrak{n})$ has good reduction at each $v \in \Sigma - \{\infty\}$ which does not divide \mathfrak{n} .

Remark (3.5). The moduli problem on (Sch/A) corresponding to $H_0(\mathfrak{n})$ is a functor

$$T \longmapsto \{\text{isomorphism classes of } (E, H)\},$$

where E is a Drinfeld A -module of rank 2 over an A -scheme T and H is an A -subgroup scheme of $E[n]$ which is locally free of constant rank $\#(A/\mathfrak{n})$ over T and which satisfies the following condition: there exist a morphism $T' \rightarrow T$ faithfully flat locally of finite presentation and an A -homomorphism $\phi: \mathfrak{n}^{-1}A/A \rightarrow H(T')$ such that $\sum_{\alpha \in \mathfrak{n}^{-1}A/A} \phi(\alpha) = H \times_T T'$ as effective Cartier divisors in $E \times_T T'$ (cf. [16], [18]).

Remark (3.6).

(i) From (3.1), (3.2), we obtain the following isomorphisms :

$$(3.7) \quad H_{\text{ét}}^1(X_0(\mathfrak{n}) \otimes_K K^{\text{sep}}, \overline{\mathbf{Q}}_l) \\ \simeq \text{Hom}_{GL_2(K_\infty)}(V_{\text{sp}}, \mathcal{A}_0(GL_2(K) \backslash GL_2(\mathbf{A}_K) / (H_0(\mathfrak{n}) \times 1))) \otimes W_\infty \\ \text{as Gal}(K_\infty^{\text{sep}}/K_\infty)\text{-modules,}$$

$$(3.8) \quad H_{\text{ét}}^1(X_0(\mathfrak{n}) \otimes_K K^{\text{sep}}, \overline{\mathbf{Q}}_l) \\ \simeq \bigoplus_{\substack{\pi \in \Pi \\ \pi_\infty = \sigma_\pi}} \left(\bigotimes_{\nu \in \mathcal{L}^-(\infty)} \pi_\nu \right)^{H_0(\mathfrak{n})} \otimes \rho(\pi) \\ \text{as Gal}(K^{\text{sep}}/K)\text{-modules.}$$

(ii) By definition, the center of $GL_2(K_\infty)$ acts trivially on V_{sp} . Therefore, noting that $\mathbf{A}_K^\times = K^\times \cdot \left(\prod_{\nu \in \mathcal{L}^-(\infty)} \mathcal{O}_\nu^\times \times K_\infty^\times \right)$ as $\text{Pic}(A) = 1$, we see that

$$\mathcal{A}_0(GL_2(K) \backslash GL_2(\mathbf{A}_K) / (H_0(\mathfrak{n}) \times 1))$$

in (3.7) can be replaced by

$$\mathcal{A}_0(GL_2(K) \backslash GL_2(\mathbf{A}_K) / (H_0(\mathfrak{n}) \times 1), 1),$$

the part on which the center of $GL_2(\mathbf{A}_K)$ acts trivially. Similarly, in (3.8) it is sufficient that π runs over the representations with trivial central character.

⟨Hecke operators and congruence relation⟩

Definition. (*Hecke operators.*)

(i) $w_{\mathfrak{q}}$ for a maximal ideal \mathfrak{q} of A which divides \mathfrak{n} :

Let m be the maximal natural number such that \mathfrak{q}^m divides \mathfrak{n} . We define $w_{\mathfrak{q}} \in \text{Aut}_A(M_0(\mathfrak{n}))$ by the rule

$$(E, H) \longmapsto (E/H[\mathfrak{q}^m], (E[\mathfrak{q}^m] + H)/H[\mathfrak{q}^m])$$

under the notation of (3.5). (We see that $w_{\mathfrak{q}}^2 = 1$ since $\text{Pic}(A) = 1$.)

We denote also by the same symbol $w_{\mathfrak{q}}$ the element of $\text{Aut}_K(X_0(\mathfrak{n}))$ or $\text{Aut}_K(J_0(\mathfrak{n}))$ etc. induced by $w_{\mathfrak{q}}$.

(ii) $T_{\mathfrak{p}}$ for a maximal ideal \mathfrak{p} of A which does not divide \mathfrak{n} :

Let $b : X_0(\mathfrak{np}) \rightarrow X_0(\mathfrak{n})$ be the morphism induced by the injection $H_0(\mathfrak{np}) \subset H_0(\mathfrak{n})$. We define an algebraic correspondence $T_{\mathfrak{p}}$ of $X_0(\mathfrak{n})$ by the formula $T_{\mathfrak{p}} = (b \circ w_{\mathfrak{p}}) \circ 'b$, where $w_{\mathfrak{p}} \in \text{Aut}_K(X_0(\mathfrak{np}))$.

We denote also by the same symbol T_p the element of $\text{End}_K(J_0(\mathfrak{n}))$ induced by T_p .

Proposition (3.9). (*Eichler-Shimura type congruence relation.*)

$$T_p = f_p + {}^t f_p \text{ in } \text{End}_{\kappa(\mathfrak{p})}(\mathcal{J}_0(\mathfrak{n}) \times_{\mathfrak{S}} \kappa(\mathfrak{p})),$$

where f_p denotes the Frobenius endomorphism attached to the finite field $\kappa(\mathfrak{p})$.

Proof. It follows from the result of [13] as in the classical case. ■

Remark (3.10). Since $f_p \cdot {}^t f_p = {}^t f_p \cdot f_p = q^{\text{deg } p} \cdot \text{id}$, $X = f_p$ satisfies the following equation in $\text{End}_{\kappa(\mathfrak{p})}(\mathcal{J}_0(\mathfrak{n}) \times_{\mathfrak{S}} \kappa(\mathfrak{p})) : X^2 - T_p X + q^{\text{deg } p} = 0$.

Let \mathfrak{n} , \mathfrak{q} , and \mathfrak{p} be as in the definition above and let $P_{\mathfrak{q}}$ (resp. $P_{\mathfrak{p}}$) be the monic polynomial in $A = \mathbb{F}_q[T]$ which generates the ideal \mathfrak{q} (resp. \mathfrak{p}). For each $f \in \mathcal{A}_0(\text{GL}_2(K) \backslash \text{GL}_2(\mathbf{A}_K) / (H_0(\mathfrak{n}) \times 1))$, we define $w_{\mathfrak{q}} f$ and $T_p f$ as follows :

$$(w_{\mathfrak{q}} f)(x) = f\left(x \begin{pmatrix} 0 & 1 \\ -P_{\mathfrak{q}}^m & 0 \end{pmatrix}\right) \quad (m : \text{as above}),$$

$$(T_p f)(x) = \sum_{\eta} f(x\eta),$$

where η runs over a system of representatives of

$$H_0^{\mathfrak{p}}(\mathfrak{p}) \begin{pmatrix} P_{\mathfrak{p}} & 0 \\ 0 & 1 \end{pmatrix} H_0^{\mathfrak{p}}(\mathfrak{p}) / H_0^{\mathfrak{p}}(\mathfrak{p}).$$

Then we can easily check that $w_{\mathfrak{q}} f$ and $T_p f$ are in $\mathcal{A}_0(\text{GL}_2(K) \backslash \text{GL}_2(\mathbf{A}_K) / (H_0(\mathfrak{n}) \times 1))$.

On the other hand, $w_{\mathfrak{q}}, T_p \in \text{End}_K(J_0(\mathfrak{n}))$ act on

$$H_{\text{ét}}^1(X_0(\mathfrak{n}) \otimes_{\bar{K}} K^{\text{sep}}, \bar{\mathbf{Q}}_l) \simeq (V_l(J_0(\mathfrak{n}) \overline{(\mathbf{K})}))^* \otimes_{\bar{\mathbf{Q}}_l} \bar{\mathbf{Q}}_l.$$

Lemma (3.11). *The isomorphisms (3.7), (3.8) commute with the action of $w_{\mathfrak{q}}$ and T_p .*

Proof. Using the fact that the isomorphisms (3.1), (3.2) commute with the action of $\text{GL}_2(\mathbf{A}_{\bar{K}})$, we can check the statement. ■

In the next section, we shall investigate the Hecke algebra (=the algebra generated by Hecke operators) in detail, assuming that \mathfrak{n} is a maximal ideal of A .

⟨ ε -factor of the L -series⟩

Next we give the calculation of the ε -factor of the L -series attached to a 2-dimensional subrepresentation of $\text{Gal}(K^{\text{sep}}/K)$ in $H_{\text{ét}}^1(X_0(\mathfrak{n}) \otimes_{\mathbb{K}} K^{\text{sep}}, \overline{\mathbb{Q}}_l)$, using the equality (3.3).

Let U be a $\overline{\mathbb{Q}}_l[\text{Gal}(K^{\text{sep}}/K)]$ -submodule of $H_{\text{ét}}^1(X_0(\mathfrak{n}) \otimes_{\mathbb{K}} K^{\text{sep}}, \overline{\mathbb{Q}}_l)$ of dimension 2 over $\overline{\mathbb{Q}}_l$ and let ρ denote the representation of $\text{Gal}(K^{\text{sep}}/K)$ associated to U .

Since in (3.8) each $\rho(\pi)$ is 2-dimensional and irreducible, we see that there exists a $\pi \in \Pi$ with $\pi_{\infty} \simeq \sigma_{\text{sp}}$ such that ρ is isomorphic to $\rho(\pi)$. Such π is uniquely determined because of (3.3) and of the strong multiplicity one theorem ([3, Theorem 2] + [17, 11.1.1]). Now consider the following condition :

$$(3.12) \quad \text{the conductor of } \pi_v \text{ (in the sense of [3]) is } n\mathcal{O}_v \text{, for each } v \in \Sigma - \{\infty\}.$$

If we denote by U' the image of U in the right-hand side of (3.8), there exists an $f' \in (\bigotimes_{v \in \Sigma - \{\infty\}} \pi_v)^{H_0(\mathfrak{n})}$ such that $U' = f' \otimes \rho(\pi)$. Further, we denote by f_{∞} a new vector of $\pi_{\infty} \simeq \sigma_{\text{sp}}$ and we set $f = f' \otimes f_{\infty} \in \pi$. (Note that f' , f_{∞} , and f are determined by U up to scalar multiplication.) The condition (3.12) says that f is a new form belonging to π .

Remark (3.13).

(i) The conductor of σ_{sp} is $\infty (= T^{-1}\mathcal{O}_{\infty})$. We can see this fact by observing that the action of $H_0^{\infty}(1) = GL_2(\mathcal{O}_{\infty})$ on $\mathbb{P}^1(K_{\infty})$ is transitive, while that of $H_0^{\infty}(\infty)$ is not transitive. A new vector of σ_{sp} is realized in V_{sp} as the characteristic function of one of the two orbits of the action of $H_0^{\infty}(\infty)$ on $\mathbb{P}^1(K_{\infty})$.

(ii) When \mathfrak{n} is a maximal ideal, the condition (3.12) is always satisfied. In fact, by (3.8)

$$\bigoplus_{\substack{\pi \in \Pi \\ \pi_{\infty} \simeq \sigma_{\text{sp}}}} (\bigotimes_{v \in \Sigma - \{\infty\}} \pi_v)^{H_0(1)} \otimes \rho(\pi) \simeq H_{\text{ét}}^1(X_0(1) \otimes_{\mathbb{K}} K^{\text{sep}}, \overline{\mathbb{Q}}_l),$$

which is reduced to zero, since $M_0(1) \simeq \mathbb{A}_A^1 = \text{Spec } A[j]$ ([11, § 3]) and then $X_0(1) \simeq \mathbb{P}_k^1$.

We define

$$Z(u, \rho) := \prod_{\substack{x : \text{closed} \\ \text{point of } S}} \det(id - \varphi_x^{-1} u^{\deg x} \mid U^L_x; \overline{\mathbb{Q}}_l)^{-1} \in \overline{\mathbb{Q}}_l[[u]].$$

In fact, $Z(u, \rho) \in \overline{\mathbb{Q}}_l((u))$, which can be seen as in § 2. Note that $L(s, \rho) = Z(q^{-s}, \rho)$ by definition.

Proposition (3.14). *Assuming the condition (3.12), we have*

$$Z(u, \rho) = \delta(u, \rho) Z\left(\frac{1}{q^2 u}, \rho\right)$$

with

$$\delta(u, \rho) = - \prod_{\substack{q : \text{maximal ideal of } A \\ \text{which divides } n}} \varepsilon_q \cdot (qu)^{\deg n - 3},$$

where $\varepsilon_q \in \{\pm 1\}$ is determined by the formula $w_q f = \varepsilon_q f$.

Proof. Since the central character of π is trivial ((3.6) (ii)), the functional equation of $L(s, \pi)$ reads as follows :

$$L(s, \pi) = \varepsilon(s, \pi) L(1-s, \pi),$$

where $\varepsilon(s, \pi)$ is the ε -factor of π . Considering (3.3), we see that the statement is equivalent to the following equality :

$$\varepsilon(s, \pi) = - \prod_{q | n} \varepsilon_q \cdot q^{(3-\deg n)(s-1/2)}.$$

Lemma (3.15). *Let π_v be an irreducible admissible representation of $GL_2(K_v)$ with trivial central character and f , a new vector of π_v ($v \in \Sigma$). Let $w_v = \begin{pmatrix} 0 & 1 \\ -a_v & 0 \end{pmatrix} \in GL_2(K_v)$, where we choose $a_v \in \mathcal{O}_v$ so that $a_v \mathcal{O}_v$ is the conductor of π_v . If*

$$w_v f_v = \varepsilon_v f_v$$

with $\varepsilon_v \in \{\pm 1\}$, then, for an additive character ϕ_v of K_v of order 0, the ε -factor of π_v is as follows :

$$\varepsilon(s, \pi_v, \phi_v) = \varepsilon_v |a_v|_v^{s-\frac{1}{2}},$$

where $|\cdot|_v$ is a valuation of K_v normalized so that

$$|b_v|_v = \frac{1}{\#(\mathcal{O}_v / b_v \mathcal{O}_v)}$$

for $b_v \in \mathcal{O}_v$.

Proof. This seems to be well-known and is easily computed by using [15, Proposition 6.17] ■

Corollary (3.16). (cf. [32].) *Let $\pi = \bigotimes_{v \in \Sigma} \pi_v$ be an irreducible admissible representation of $GL_2(\mathbb{A}_K)$ with trivial central character. Under the notation of (3.15) for each π_v , we have the following formula for the ε -factor of π :*

$$\varepsilon(s, \pi) = \prod_{v \in \Sigma} \varepsilon_v \cdot \left\{ \prod_{v \in \Sigma} |a_v|_v \cdot \left(\prod_{v \in \Sigma} |d_v|_v \right)^2 \right\}^{s - \frac{1}{2}},$$

where $(d_v)_v \in \mathbb{A}_K^\times$ is a differential idele attached to a non-trivial additive character τ of \mathbb{A}_K which is trivial on K ([33, VII, Definition 4]).

Proof. By definition, $\phi_v = \tau_v(d_v^{-1} \cdot)$ is of order 0, so

$$\begin{aligned} \varepsilon(s, \pi) &= \prod_{v \in \Sigma} \varepsilon(s, \pi_v, \tau_v) \\ &= \prod_{v \in \Sigma} \varepsilon(s, \pi_v, \phi_v(d_v \cdot)) \\ &= \prod_{v \in \Sigma} |d_v|_v^{2s-1} \varepsilon(s, \pi_v, \phi_v) \\ &= \prod_{v \in \Sigma} |d_v|_v^{2s-1} \cdot \varepsilon_v |a_v|_v^{s-\frac{1}{2}} \\ &= \prod_{v \in \Sigma} \varepsilon_v \cdot \left\{ \prod_{v \in \Sigma} |a_v|_v \cdot \left(\prod_{v \in \Sigma} |d_v|_v \right)^2 \right\}^{s-\frac{1}{2}}. \end{aligned}$$

We return to the proof of (3.14). Here

$$\prod_{v \in \Sigma} |a_v|_v = q^{-1} \cdot q^{-\deg n} = q^{-1-\deg n} \quad ((3.12), (3.13)),$$

$$\prod_{v \in \Sigma} |d_v|_v = q^{2-2 \cdot 0} = q^2 \quad ([33, VII, Proposition 6]),$$

so

$$\prod_{v \in \Sigma} |a_v|_v \cdot \left(\prod_{v \in \Sigma} |d_v|_v \right)^2 = q^{3-\deg n}.$$

Hence it suffices to show that

- (i) for $v \in \Sigma - \{\infty\}$ which does not divide n , $w_v f_v = f_v$,
- (ii) $w_\infty f_\infty = -f_\infty$.

(i) is clear because $w_v \in GL_2(\mathcal{O}_v) = H_0^v(1)$ for $v \in \Sigma - \{\infty\}$ which does not divide n . If we realize f_∞ in V_{sp} as in (3.13) (i),

$$f_\infty + w_\infty f_\infty = \text{constant function} = 0 \text{ in } V_{sp},$$

which implies (ii). This completes the proof of (3.14). ■

Corollary (3.17). *Let ν be the order at $u=q^{-1}$ of $Z(u, \rho)$. Then*

- (i) $0 \leq \nu \leq \deg n - 3$,
- (ii) $(-1)^\nu = -\prod_{q|n} \epsilon_q$.

Proof. Since π is a constituent of \mathcal{A}_0 , $L(s, \pi)$ is a polynomial function of q^{-s} ([17, 11.1]), so $Z(u, \rho)$ is a polynomial of u . Now (3.14) implies that the degree of the polynomial is $\deg n - 3$. (Note that $Z(0, \rho) = 1$.) Hence (i) follows.

Next we set

$$Z(u, \rho) = (u - q^{-1})^\nu Y(u, \rho).$$

Then we have

$$Z\left(\frac{1}{q^2 u}, \rho\right) = \left(\frac{1}{q^2 u} - q^{-1}\right)^\nu Y\left(\frac{1}{q^2 u}, \rho\right) = \left\{-\frac{1}{qu}(u - q^{-1})\right\}^\nu Y\left(\frac{1}{q^2 u}, \rho\right),$$

so

$$\delta(u, \rho) = \frac{Z(u, \rho)}{Z\left(\frac{1}{q^2 u}, \rho\right)} = (-qu)^\nu \frac{Y(u, \rho)}{Y\left(\frac{1}{q^2 u}, \rho\right)}.$$

Since $Y(q^{-1}, \rho) \neq 0$, we obtain $\delta(q^{-1}, \rho) = (-1)^\nu$ by setting $u = q^{-1}$. On the other hand, from (3.14)

$$\delta(q^{-1}, \rho) = -\prod_{q|n} \epsilon_q,$$

which completes the proof of (3.17). ■

§ 4. Hecke Algebra and Its Eisenstein Ideal

We follow the notations of § 3. Moreover, we assume that n is a maximal ideal of A (cf. (3.13) (ii)), and set $d = \deg n = [\kappa(n) : \mathbb{F}_q]$. Then the genus g of $X_0(n)$ (= the dimension of $J_0(n)$) is given by the following formula ([11, 3.4.18]):

$$(4.1) \quad g = \begin{cases} q \cdot \frac{q^{d-1} - 1}{q^2 - 1} & d : \text{odd} \\ q^2 \cdot \frac{q^{d-2} - 1}{q^2 - 1} & d : \text{even.} \end{cases}$$

We write J instead of $J_0(n)$ for simplicity.

Definition. The Hecke algebra \mathbf{T} is the subalgebra of $\text{End}_K(J)$ generated by $\{T_p \mid p \neq n\} \cup \{w_n\}$ over \mathbf{Z} .

Proposition (4.2).

- (i) \mathbf{T} is a finitely generated \mathbf{Z} -module.
 - (ii) $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q}$ is a commutative semi-simple algebra of dimension g over \mathbf{Q} .
 - (iii) $\mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q} = \text{End}_K(J) \otimes_{\mathbf{Z}} \mathbf{Q}$.
- (In fact, in (iii), End_K can be replaced by $\text{End}_{\bar{K}}$. See Appendix.)

Proof. (i) results from the well-known fact that $\text{End}(J)$ is a finitely generated \mathbf{Z} -module.

Next, in the isomorphism (3.8)

$$H_{\text{ét}}^1(X_0(n) \otimes_K K^{\text{sep}}, \bar{\mathbf{Q}}_l) \simeq \bigoplus_{\substack{\pi \in \Pi \\ \pi_v \simeq \sigma_{\infty}}} \left(\bigotimes_{v \in \Sigma - \{\infty\}} \pi_v \right)^{H_0(n)} \otimes \rho(\pi),$$

$\left(\bigotimes_{v \in \Sigma - \{\infty\}} \pi_v \right)^{H_0(n)}$ is of dimension ≤ 1 for each π . This follows from (3.13) (ii) (cf. [3, Theorem 1]). Therefore, there exist just g such π 's and if we call them π_1, \dots, π_g , we have the following isomorphism of $\text{Gal}(K^{\text{sep}}/K)$ -modules :

$$H_{\text{ét}}^1(X_0(n) \otimes_K K^{\text{sep}}, \bar{\mathbf{Q}}_l) \simeq \bigoplus_{j=1}^g \rho(\pi_j).$$

Then

$$\begin{aligned} \text{End}_K(J) \otimes_{\mathbf{Z}} \bar{\mathbf{Q}}_l &\hookrightarrow \text{End}_{\text{Gal}(K^{\text{sep}}/K)}(V_l(J(\bar{K})) \otimes_{\bar{\mathbf{Q}}_l} \bar{\mathbf{Q}}_l) \\ &\simeq \text{End}_{\text{Gal}(K^{\text{sep}}/K)}(V_l(J(\bar{K}))^* \otimes_{\bar{\mathbf{Q}}_l} \bar{\mathbf{Q}}_l) \quad (\text{anti-isomorphism}) \\ &\simeq \text{End}_{\text{Gal}(K^{\text{sep}}/K)}(H_{\text{ét}}^1(X_0(n) \otimes_K K^{\text{sep}}, \bar{\mathbf{Q}}_l)) \\ &\simeq \text{End}_{\text{Gal}(K^{\text{sep}}/K)}\left(\bigoplus_{j=1}^g \rho(\pi_j)\right) \\ &\simeq \prod_{j=1}^g \bar{\mathbf{Q}}_l, \end{aligned}$$

where the last isomorphism follows from the fact that each $\rho(\pi_j)$ is irreducible and that $\rho(\pi_j) \neq \rho(\pi_{j'})$ unless $j=j'$.

Now define \mathbf{T}' to be the subalgebra of \mathbf{T} generated by $\{T_p \mid p \neq n\}$ over \mathbf{Z} . For each π_j , the 1-dimensional $\bar{\mathbf{Q}}_l$ -vector space $\left(\bigotimes_{v \in \Sigma - \{\infty\}} \pi_{j,v} \right)^{H_0(n)}$ is generated by $\otimes f_{j,v}$, where $f_{j,v}$ is a fixed new vector of $\pi_{j,v}$ ($v \in \Sigma - \{\infty\}$) and the action of \mathbf{T}' on this space (in other words, the set of eigenvalues of T_p 's ($p \neq n$)) determines π_j uniquely (the strong multiplicity one theorem). Hence the image of

$$\mathbf{T}' \otimes_{\mathbf{Z}} \bar{\mathbf{Q}}_l \hookrightarrow \text{End}_K(J) \otimes_{\mathbf{Z}} \bar{\mathbf{Q}}_l \hookrightarrow \prod_{j=1}^g \bar{\mathbf{Q}}_l$$

should be the whole $\prod_{j=1}^g \overline{\mathbf{Q}}_l$. Since $\mathbf{T}' \subset \mathbf{T} \subset \text{End}_K(J)$, we obtain

$$\mathbf{T} \otimes_{\mathbf{Z}} \overline{\mathbf{Q}}_l = \text{End}_K(J) \otimes_{\mathbf{Z}} \overline{\mathbf{Q}}_l \simeq \prod_{j=1}^g \overline{\mathbf{Q}}_l.$$

We can easily show the statement of (ii) and (iii) by using this isomorphism. ■

Remark (4.3). From (4.2) (ii), we obtain

$$(4.4) \quad \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q} \simeq F_1 \times \cdots \times F_s, \quad F_i : \text{algebraic number field},$$

$$\sum_{i=1}^s [F_i : \mathbf{Q}] = g,$$

and this decomposition gives the following isogeny over K :

$$(4.5) \quad J \longrightarrow J_1 \times \cdots \times J_s,$$

where $J_i = J/\mathfrak{P}_i J$ with $\mathfrak{P}_i = \text{Ker}(\mathbf{T} \rightarrow F_i)$. Here we have

$$(4.6) \quad \dim J_i = [F_i : \mathbf{Q}].$$

In fact, since

$$(V_l(J(\overline{K})))^* \otimes_{\mathbf{Q}_l} \overline{\mathbf{Q}}_l \simeq \bigoplus_{i=1}^s (V_l(J_i(\overline{K})))^* \otimes_{\mathbf{Q}_l} \overline{\mathbf{Q}}_l$$

as $\text{Gal}(K^{\text{sep}}/K)$ -modules, we have

$$(V_l(J_i(\overline{K})))^* \simeq \bigoplus_{j \in S_i} \rho(\pi_j), \quad \prod_{i=1}^s S_i = \{1, \dots, g\},$$

accordingly

$$\begin{aligned} \dim J_i &= \frac{1}{2} \dim_{\mathbf{Q}_l} V_l(J_i(\overline{K})) \\ &= \#S_i \\ &= \dim_{\overline{\mathbf{Q}}_l} \prod_{j \in S_i} \overline{\mathbf{Q}}_l \\ &= \dim_{\overline{\mathbf{Q}}_l} \text{End}_{\text{Gal}(K^{\text{sep}}/K)}((V_l(J_i(\overline{K})))^* \otimes_{\mathbf{Q}_l} \overline{\mathbf{Q}}_l) \\ &= \dim_{\overline{\mathbf{Q}}_l} F_i \otimes_{\mathbf{Q}} \overline{\mathbf{Q}}_l \\ &= [F_i : \mathbf{Q}]. \end{aligned}$$

The set of cusps $X_0(n) - Y_0(n)$ consists of two K -rational points corresponding to the points of $\Gamma_0(n) \backslash \mathbb{P}^1(K)$ (cf. (3.4)). (See [13, 3.4] for the K -rationality.) We denote by ∞ (resp. 0) the K -rational point corresponding to $(1 : 0)$ (resp. $(0 : 1) \in \mathbb{P}^1(K)$) and define $c \in J(K)$ to be the class of the divisor $(0) - (\infty)$ of degree 0. The subgroup C of $J(K)$ generated by c is finite cyclic and its order N is given by the following formula ([13]) :

$$(4.7) \quad N = \begin{cases} \frac{q^d - 1}{q - 1} & d : \text{odd} \\ \frac{q^d - 1}{q^2 - 1} & d : \text{even.} \end{cases}$$

Lemma (4.8).

$$T_p c = (1 + q^{\text{deg } p})c \quad (p \neq n),$$

$$w_n c = -c.$$

In particular, C is preserved by the action of $\mathbf{T} : \mathbf{T}C \subset C$.

Proof. Immediate from definitions (cf. [31]). ■

Definition. The *Eisenstein ideal* I of \mathbf{T} is the kernel of $\mathbf{T} \rightarrow \text{End}_{\mathbf{Z}}(C)$ (i.e. the annihilator of c).

By definition $\mathbf{T}/I \simeq \mathbf{Z}/N\mathbf{Z}$, and from (4.8) we can see that I contains $T_p - (1 + q^{\text{deg } p})$ ($p \neq n$) and $w_n + 1$.

Definition.

- (i) An *Eisenstein prime number* is a (rational) prime number which divides N .
- (ii) An *Eisenstein prime ideal* of \mathbf{T} is a prime ideal of \mathbf{T} which includes the Eisenstein ideal I .

Remark (4.9).

- (i) By (4.7), an Eisenstein prime number l does not divide q .
- (ii) Since $\mathbf{T}/I \simeq \mathbf{Z}/N\mathbf{Z}$, we have the following one-to-one correspondence

$$\begin{array}{ccc} \{\text{Eisenstein prime numbers}\} & \longleftrightarrow & \{\text{Eisenstein prime ideals}\} \\ l & \longmapsto & (I, l) \\ \text{the prime number which generates } \mathcal{L} \cap \mathbf{Z} & \longleftarrow & \mathcal{L} \end{array}$$

Definition.

(i) Let \mathfrak{A} be an ideal of \mathbf{T} . Then we define

$$\begin{aligned} \hat{\mathbf{T}}_{\mathfrak{A}} &:= \varprojlim \mathbf{T}/\mathfrak{A}^r, \\ \mathfrak{b}_{\mathfrak{A}} &:= \text{Ker}(\mathbf{T} \longrightarrow \hat{\mathbf{T}}_{\mathfrak{A}}) = \bigcap_{r \geq 1} \mathfrak{A}^r, \\ J^{(\mathfrak{A})} &:= J/\mathfrak{b}_{\mathfrak{A}}J, \\ J^{(\mathfrak{A})^-} &:= J^{(\mathfrak{A})}/(w_{\pi} + 1)J^{(\mathfrak{A})} = J/(\mathfrak{b}_{\mathfrak{A}}, w_{\pi} + 1)J. \end{aligned}$$

(ii) We write \tilde{J} (resp. \tilde{J}^-) instead of $J^{(l)}$ (resp. $J^{(l)^-}$). The abelian variety \tilde{J} is called the *Eisenstein quotient* of J .

(iii) For each Eisenstein prime number l , we write $\tilde{J}^{(l)}$ instead of $J^{(\mathcal{L})}$, where \mathcal{L} is the Eisenstein prime ideal corresponding to l .

Lemma (4.10). *Let \mathfrak{b} be an ideal of \mathbf{T} . Under the notation of (4.3),*

$$J/\mathfrak{b}J \longrightarrow \prod_{i \in \Lambda} J_i$$

is an isogeny, where $\Lambda = \{i = 1, \dots, s \mid \mathfrak{b} \subset \mathfrak{P}_i\}$

Proof. Since $(\mathbf{T}/\mathfrak{b}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quotient of $\mathbf{T} \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \prod_{i=1}^s F_i$, we have the following commutative diagram for suitable $\Lambda' \subset \{1, \dots, s\}$.

$$\begin{array}{ccc} \mathbf{T} \otimes_{\mathbb{Z}} \mathbb{Q} & \simeq & \prod_{i=1}^s F_i \\ \downarrow & & \downarrow \text{proj} \\ (\mathbf{T}/\mathfrak{b}) \otimes_{\mathbb{Z}} \mathbb{Q} & \simeq & \prod_{i \in \Lambda'} F_i. \end{array}$$

Here we can easily see that $i \in \Lambda' \Leftrightarrow i \in \Lambda$, hence

$$(\mathbf{T}/\mathfrak{b}) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \prod_{i \in \Lambda} F_i \simeq \prod_{i \in \Lambda} (\mathbf{T}/\mathfrak{P}_i) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

From this the statement follows immediately. ■

Proposition (4.11). *We follow the notation of (4.3).*

(i) *Let l be an Eisenstein prime number and \mathcal{L} the Eisenstein prime ideal corresponding to l . Then*

$$\tilde{J}^{(l)} \longrightarrow \prod_{i \in \Lambda} J_i$$

is an isogeny, where $\Lambda_l = \{i = 1, \dots, s \mid \mathfrak{P}_i \subset \mathcal{L}\}$.

(ii) The following two homomorphisms are isogenies :

$$\begin{aligned} \tilde{J} &\longrightarrow \prod_{i \in \tilde{\Lambda}} J_i, & \text{where } \tilde{\Lambda} &= \{i = 1, \dots, s \mid \exists \mathcal{L} : \text{Eisenstein prime ideal s.t. } \mathfrak{P}_i \subset \mathcal{L}\}, \\ \tilde{J}^- &\longrightarrow \prod_{i \in \tilde{\Lambda}^-} J_i, & \text{where } \tilde{\Lambda}^- &= \{i = 1, \dots, s \mid \exists \mathcal{L} : \text{Eisenstein prime ideal s.t. } \mathfrak{P}_i \subset \mathcal{L} \\ & & & \text{and } w_n + 1 \in \mathfrak{P}_i\}. \end{aligned}$$

Proof. (i) By (4.10), it suffices to show that $\mathfrak{b}_{\mathcal{L}} \subset \mathfrak{P}_i \iff \mathfrak{P}_i \subset \mathcal{L}$. Set $\mathbf{T}_{\mathcal{L}} = (\mathbf{T} - \mathcal{L})^{-1} \mathbf{T}$, then $\hat{\mathbf{T}}_{\mathcal{L}}$ may be identified with the completion of $\mathbf{T}_{\mathcal{L}}$ at its maximal ideal $\mathcal{L} \mathbf{T}_{\mathcal{L}}$, since \mathcal{L} is a maximal ideal of \mathbf{T} . (Note that $\mathbf{T}/\mathcal{L} \simeq \mathbf{Z}/l\mathbf{Z}$, which is a field.) Now $\mathbf{T}_{\mathcal{L}}$ is a noetherian local ring, so $\mathbf{T}_{\mathcal{L}} \rightarrow \hat{\mathbf{T}}_{\mathcal{L}}$ is injective.

We have the following commutative diagram :

$$\begin{array}{ccc} \mathbf{T} & \hookrightarrow & \prod_{i=1}^s \mathbf{T}/\mathfrak{P}_i \\ \downarrow & & \downarrow \\ \mathbf{T}_{\mathcal{L}} & \hookrightarrow & \prod_{i=1}^s (\mathbf{T}/\mathfrak{P}_i)_{\mathcal{L}}, \end{array}$$

where

$$\begin{aligned} (\mathbf{T}/\mathfrak{P}_i)_{\mathcal{L}} &:= (\mathbf{T} - \mathcal{L})^{-1} (\mathbf{T}/\mathfrak{P}_i) \\ &= \begin{cases} 0 & \mathfrak{P}_i \not\subset \mathcal{L} \\ (\mathbf{T}/\mathfrak{P}_i - \mathcal{L}/\mathfrak{P}_i)^{-1} (\mathbf{T}/\mathfrak{P}_i) (\subset F_i) & \mathfrak{P}_i \subset \mathcal{L}. \end{cases} \end{aligned}$$

Hence

$$\begin{aligned} \mathfrak{b}_{\mathcal{L}} &= \text{Ker}(\mathbf{T} \longrightarrow \hat{\mathbf{T}}_{\mathcal{L}}) \\ &= \text{Ker}(\mathbf{T} \longrightarrow \mathbf{T}_{\mathcal{L}}) \\ &= \bigcap_{i \in \Lambda_l} \mathfrak{P}_i. \end{aligned}$$

Noting that each \mathfrak{P}_i is a minimal prime ideal of \mathbf{T} , we obtain $\mathfrak{b}_{\mathcal{L}} \subset \mathfrak{P}_i \iff \mathfrak{P}_i \subset \mathcal{L}$.

(ii) Since $\hat{\mathbf{T}}_l \xrightarrow{\sim} \prod_{\substack{\mathcal{L} : \text{Eisenstein} \\ \text{prime ideal}}} \hat{\mathbf{T}}_{\mathcal{L}}$, we have $\mathfrak{b}_l = \bigcap_{\substack{\mathcal{L} : \text{Eisenstein} \\ \text{prime ideal}}} \mathfrak{b}_{\mathcal{L}}$. Then, from the proof of (i),

we can see that $\mathfrak{b}_l = \bigcap_{i \in \Lambda} \mathfrak{P}_i$. This implies that the first homomorphism of (ii) is an isogeny, as in the proof of (i). From this, it follows immediately that the second homomorphism is also an isogeny. This completes the proof. ■

Proposition (4.12).

(i) Let l be an Eisenstein prime number $\neq 2$. Then the homomorphism $\tilde{J} \rightarrow \tilde{J}^{(l)}$ factors through $\tilde{J} \rightarrow \tilde{J}^-$.

$$\begin{array}{ccc}
 \tilde{J} & \longrightarrow & \tilde{J}^- \\
 & \searrow \quad \swarrow & \\
 & \mathbb{Q} & \\
 & \tilde{J}^{(l)} &
 \end{array}$$

(ii) If N is odd, then $\tilde{J} = \tilde{J}^-$.

Proof. (i) First we note that $w_n - 1 = (w_n + 1) - 2$ is invertible in $\hat{\mathbf{T}}_{\mathcal{L}}$ since $w_n + 1 \in \mathcal{L}$ and $2 \in \hat{\mathbf{T}}_{\mathcal{L}}^\times$. Then $(w_n - 1)(w_n + 1) = w_n^2 - 1 = 0$ implies that $w_n + 1 = 0$ in $\hat{\mathbf{T}}_{\mathcal{L}}$, that is to say $w_n + 1 \in \mathfrak{b}_{\mathcal{L}}$. This proves (i).

(ii) If N is odd, we obtain from (i) that $w_n + 1 \in \bigcap_{\substack{\mathcal{L} : \text{Eisenstein} \\ \text{prime ideal}}} \mathfrak{b}_{\mathcal{L}} = \mathfrak{b}_l$. ■

Remark (4.13). By the formula (4.7),

$$\begin{array}{l}
 \text{either} \\
 N \text{ is odd} \iff q \text{ is odd and } d \text{ is not divided by } 4, \\
 \text{or} \\
 q \text{ is even.}
 \end{array}$$

Proposition (4.14).

- (i) For each Eisenstein prime number l , $\tilde{J}^{(l)} \neq 0$.
- (ii) The following are all equivalent :
 - (a) $d \geq 3$; (b) $g > 0$; (b') $g \geq q$; (c) $N > 1$; (c') $N \geq 5$; (d) $\tilde{J} \neq 0$;
 - (e) $\tilde{J}^- \neq 0$.

Proof. (i) By (4.11)(i), it suffices to prove $\Lambda_l \neq \emptyset$. As in the proof of (4.11)(i), $\Lambda_l = \emptyset$ implies $\mathbf{T}_{\mathcal{L}} = 0$. This is absurd, since $\mathbf{T}/\mathcal{L} \simeq \mathbf{Z}/l\mathbf{Z} \neq 0$.
 (ii) We can see (a) \Leftrightarrow (b) \Leftrightarrow (b') from (4.1) and (a) \Leftrightarrow (c) \Leftrightarrow (c') from (4.7). (e) \Rightarrow (d) \Rightarrow (c) is clear. We shall show (c) \Rightarrow (e). By (i) and (4.12)(i), it suffices to check that if $N > 1$, then there exists an odd prime number l which divides N . If this is not so, then $N = 2^M$ with $M \geq 1$. In particular, N is even and then (4.13) implies that q is odd and d is divided by 4. Hence $q^4 - 1$ divides $q^d - 1$ and $q^2 + 1$ divides $\frac{q^d - 1}{q^2 - 1} = N = 2^M$, so $\frac{q^2 + 1}{2}$ divides 2^{M-1} . This is absurd since $\frac{q^2 + 1}{2}$ is an odd number > 1 . ■

Let l be an Eisenstein prime number and \mathcal{L} the Eisenstein prime ideal corresponding to l . Since \mathbf{T} is finite over \mathbf{Z} , only finitely many prime ideals of \mathbf{T} contain l and, when we call them $\mathcal{L}_1 = \mathcal{L}, \mathcal{L}_2, \dots, \mathcal{L}_t$, the following decomposition exists :

$$(4.15) \quad \hat{\mathbf{T}}^{(l)} \simeq \hat{\mathbf{T}}_{\mathcal{L}_1} \times \dots \times \hat{\mathbf{T}}_{\mathcal{L}_t}$$

$$= \widehat{\mathbf{T}}_{\mathcal{L}} \times (\widehat{\mathbf{T}}_{\mathcal{L}})',$$

where we set $(\widehat{\mathbf{T}}_{\mathcal{L}})' = \widehat{\mathbf{T}}_{\mathcal{L}_2} \times \cdots \times \widehat{\mathbf{T}}_{\mathcal{L}_t}$. From now on, we denote by $\varepsilon_{\mathcal{L}}$ the idempotent of $\widehat{\mathbf{T}}_{(l)}$ which corresponds to $(1, 0) \in \widehat{\mathbf{T}}_{\mathcal{L}} \times (\widehat{\mathbf{T}}_{\mathcal{L}})'$.

Proposition (4.16).

- (i) *The composition of $C \rightarrow J(K) \rightarrow \tilde{J}(K)$ is injective.*
- (ii) *The kernel of the composition of $C \rightarrow J(K) \rightarrow \tilde{J}(K) \rightarrow \tilde{J}^-(K)$ is contained in $C[2]$. In particular, if one of the equivalent conditions of (4.14) (ii) is satisfied, then the image of C in $\tilde{J}^-(K)$ is not reduced to zero.*

Proof. (i) Let l be an Eisenstein prime number and \mathcal{L} the Eisenstein prime ideal corresponding to l . The following exact sequence of $\mathbb{T}/l\mathbb{T} (\simeq \widehat{\mathbf{T}}_{(l)}/l\widehat{\mathbf{T}}_{(l)})$ -modules exists :

$$0 \rightarrow (\mathfrak{b}_{\mathcal{L}}J)(\overline{K})[l] \rightarrow J(\overline{K})[l] \rightarrow \tilde{J}^{(l)}(\overline{K})[l].$$

Taking the \mathcal{L} -primary part of this sequence, we obtain

$$0 \rightarrow \varepsilon_{\mathcal{L}}((\mathfrak{b}_{\mathcal{L}}J)(\overline{K})[l]) \rightarrow \varepsilon_{\mathcal{L}}(J(\overline{K})[l]) \rightarrow \varepsilon_{\mathcal{L}}(\tilde{J}^{(l)}(\overline{K})[l]),$$

which is again exact.

Claim. $\varepsilon_{\mathcal{L}}((\mathfrak{b}_{\mathcal{L}}J)(\overline{K})[l]) = 0$.

In fact, let $x = b_1 y_1 + \cdots + b_k y_k \in (\mathfrak{b}_{\mathcal{L}}J)(\overline{K})[l]$ with $b_1, \dots, b_k \in \mathfrak{b}_{\mathcal{L}}, y_1, \dots, y_k \in J(\overline{K})$. Then there exists a finite extension L/K in \overline{K}/K such that y_1, \dots, y_k are all in $J(L)$. For each $r \geq 1$, fix $\varepsilon_{\mathcal{L}, r} \in \mathbb{T}$ which is congruent to $\varepsilon_{\mathcal{L}}$ modulo $l^r \widehat{\mathbf{T}}_{\mathcal{L}}$. Since x is an l -torsion element, we have

$$\varepsilon_{\mathcal{L}} x = \varepsilon_{\mathcal{L}, r} x = \varepsilon_{\mathcal{L}, r} b_1 y_1 + \cdots + \varepsilon_{\mathcal{L}, r} b_k y_k.$$

Here, by definition $\varepsilon_{\mathcal{L}} \mathfrak{b}_{\mathcal{L}} = 0$ in $\widehat{\mathbf{T}}_{(l)}$, hence $\varepsilon_{\mathcal{L}, r} \mathfrak{b}_{\mathcal{L}} \subset l^r \mathbb{T} = l^r \widehat{\mathbf{T}}_{(l)} \cap \mathbb{T}$ for each $r \geq 1$. Therefore $\varepsilon_{\mathcal{L}} x \in l^r J(L)$ for each $r \geq 1$, which implies

$$\varepsilon_{\mathcal{L}} x \in (l^r J(L))[l] = l^r (J(L)[l^{r+1}]) \subset l^r (J(L)[l^\infty]).$$

Thus

$$\varepsilon_{\mathcal{L}} x \in \bigcap_{r \geq 1} l^r (J(L)[l^\infty]) = 0,$$

since $J(L)$ is a finitely generated \mathbb{Z} -module.

In particular, $J(\bar{K})[\mathcal{L}] \rightarrow \tilde{J}^{(l)}(\bar{K})$ is injective, since

$$J(\bar{K})[\mathcal{L}] \subset \varepsilon_{\mathcal{L}}(J(\bar{K})[I]).$$

Now, turn to the proof of (i). If the map is not injective, then there exists a prime number l which divides N and $x \in C[I]$ which is a non-trivial element of the kernel. Since the Eisenstein prime ideal \mathcal{L} corresponding to l is generated by I and l , and since $IC=0$ by definition, we see that $x \in J(\bar{K})[\mathcal{L}]$. By definition, the image of x in $\tilde{J}(\bar{K})$ is zero, a fortiori so is the image of x in $\tilde{J}^{(l)}(\bar{K})$. This is contradictory to the injectivity of $J(\bar{K})[\mathcal{L}] \rightarrow \tilde{J}^{(l)}(\bar{K})$.

(ii) Let x be an element of the kernel of the map of (ii) and x' be the image of x in $\tilde{J}(\bar{K})$. Since $\tilde{J}^- = \tilde{J}/(w_n + 1)\tilde{J}$ implies $\tilde{J}^-(\bar{K}) = \tilde{J}(\bar{K})/(w_n + 1)(\tilde{J}(\bar{K}))$, there exists $y \in \tilde{J}(\bar{K})$ satisfying $x' = (w_n + 1)y$. On the other hand, $x \in C$ implies $w_n x = -x$, so

$$2x' = (1 - w_n)x' = (1 - w_n)(w_n + 1)y = (1 - w_n^2)y = 0.$$

Since $C \rightarrow \tilde{J}(\bar{K})$ is injective from (i), we have $2x = 0$.

As we have seen in the proof of (4.14) (ii), N can never be equal to 2. Thus the second statement of (ii) follows. ■

Proposition (4.17). *Let \mathfrak{b} be an ideal of \mathbb{T} and set $B = J/\mathfrak{b}J$. Let \mathcal{B} denote the Néron model over S of B . Then for each $r \geq 0$, $\varepsilon_{\mathcal{L}}(\mathcal{B}[l^r])$ and $\varepsilon_{\mathcal{L}}(\mathcal{B}^0[l^r])$ are admissible for $(S, S') = (\mathbb{P}_{\mathbb{F}_q}^1, \mathbb{P}_{\mathbb{F}_q}^1 - \{\infty, n\})$ in the sense of § 1.*

Proof. From (1.3), these are objects of the category \mathcal{C} of § 1, so it suffices to show that $(\varepsilon_{\mathcal{L}}(\mathcal{B}[l^r]))(K^{\text{sep}})$ and $(\varepsilon_{\mathcal{L}}(\mathcal{B}^0[l^r]))(K^{\text{sep}})$ are admissible as $\text{Gal}(K^{\text{sep}}/K)$ -modules. Note that both of these modules coincide with $\varepsilon_{\mathcal{L}}(B(K^{\text{sep}})[l^r])$.

Now since $\hat{\mathbb{T}}_{\mathcal{L}}/l^r \hat{\mathbb{T}}_{\mathcal{L}}$ is an artinian local ring, there exists $m > 0$ satisfying $\mathcal{L}^m \subset l^r \hat{\mathbb{T}}_{\mathcal{L}}$. Then we have

$$\varepsilon_{\mathcal{L}}(B(K^{\text{sep}})[l^r]) \subset B(K^{\text{sep}})[\mathcal{L}^m],$$

accordingly it suffices to prove the following statement (m) for each $m > 0$:

(m) : $B(K^{\text{sep}})[\mathcal{L}^m]$ is admissible as a $\text{Gal}(K^{\text{sep}}/K)$ -module.

If we admit that (1) is true, then for each $m > 1$, from the exact sequence

$$0 \rightarrow B(K^{\text{sep}})[\mathcal{L}] \rightarrow B(K^{\text{sep}})[\mathcal{L}^m] \xrightarrow{(a_1, \dots, a_k)} \bigoplus_{i=1}^k B(K^{\text{sep}})[\mathcal{L}^{m-1}],$$

where $\{a_1, \dots, a_k\} \subset \mathbf{T}$ is a fixed set of generators of \mathcal{L} (i.e. $\mathcal{L} = \mathbf{T}a_1 + \dots + \mathbf{T}a_k$), we can reduce (m) to $(m-1)$. Thus we have only to prove (1).

Set $L = K(B[\mathcal{L}], \mu_l)$, that is to say L is the subfield of K^{sep} corresponding to the kernel of

$$\text{Gal}(K^{\text{sep}}/K) \rightarrow \text{Aut}(B(K^{\text{sep}})[\mathcal{L}]) \times \text{Aut}(\mu_l(K^{\text{sep}})).$$

The extension L/K is a Galois extension and $G = \text{Gal}(L/K)$ is a finite group.

For each $p \in \Sigma - \{\infty, n\}$, B has good reduction at p . Therefore L/K is unramified at p and the Frobenius element $\varphi_p \in G$ is defined (up to conjugacy). Note that

$$B(K^{\text{sep}})[\mathcal{L}] \xleftarrow{\sim} B(\mathcal{O}_{S, p}^{\text{sh}})[\mathcal{L}] \xrightarrow{\sim} (\mathcal{B} \times_S \kappa(p))(\overline{\kappa(p)})[\mathcal{L}]$$

since B has good reduction at p . Then from (3.10), we see that the action of φ_p on this finite module satisfies $\varphi_p^2 - T_p \cdot \varphi_p + q^{\text{deg } p} = 0$. Moreover, since $T_p - (1 + q^{\text{deg } p}) \in I$ by (4.8) it satisfies

$$\begin{aligned} \varphi_p^2 - (1 + q^{\text{deg } p})\varphi_p + q^{\text{deg } p} &= 0, \quad \text{or} \\ (\varphi_p - 1)(\varphi_p - q^{\text{deg } p}) &= 0. \end{aligned}$$

This implies that the characteristic polynomial of φ_p in the $\mathbf{Z}/l\mathbf{Z}$ -vector space $B(K^{\text{sep}})[\mathcal{L}]$ can be written as follows :

$$(X - 1)^{\alpha_p}(X - q^{\text{deg } p})^{\beta_p}, \quad \alpha_p + \beta_p = \gamma,$$

where γ is the dimension of $B(K^{\text{sep}})[\mathcal{L}]$ over $\mathbf{Z}/l\mathbf{Z}$.

Now set

$$\mathcal{W} = B(K^{\text{sep}})[\mathcal{L}] \oplus (B(K^{\text{sep}})[\mathcal{L}])^\vee,$$

where $(B(K^{\text{sep}})[\mathcal{L}])^\vee = \text{Hom}_{\mathbf{Z}/l\mathbf{Z}}(B(K^{\text{sep}})[\mathcal{L}], \mu_l(K^{\text{sep}}))$. (Note that the action of $\text{Gal}(K^{\text{sep}}/K)$ on \mathcal{W} factors through G , so φ_p acts on \mathcal{W} .) The characteristic polynomial of φ_p in \mathcal{W} is

$$(X - 1)^{\alpha_p}(X - q^{\text{deg } p})^{\beta_p} \cdot (X - q^{\text{deg } p})^{\alpha_p}(X - 1)^{\beta_p} = (X - 1)^\gamma(X - q^{\text{deg } p})^\gamma,$$

which coincides with the characteristic polynomial of φ_p in $(\mathbf{Z}/l\mathbf{Z})^\gamma \oplus (\mu_l(K^{\text{sep}}))^\gamma$. Moreover, the density theorem of Chebotarev type (cf. [33, XIII, Theorem 12]) implies that for any $g \in G$, its characteristic polynomial in \mathcal{W} coincides with that of $(\mathbf{Z}/l\mathbf{Z})^\gamma \oplus (\mu_l(K^{\text{sep}}))^\gamma$. Hence the semi-simplification of the G -module \mathcal{W} is isomorphic to $(\mathbf{Z}/l\mathbf{Z})^\gamma \oplus (\mu_l(K^{\text{sep}}))^\gamma$, by the Brauer-Nesbitt theorem ([4, 30.16]).

Since $B(K^{\text{sep}})[\mathcal{L}] \subset W$, this completes the proof. ■

§ 5. Main Results

We follow the notations of the preceding sections (especially § 3 and § 4).

Let l be an Eisenstein prime number and \mathcal{L} the Eisenstein prime ideal corresponding to l . Let \mathfrak{P} be a minimal prime ideal of \mathbf{T} (i.e. $\mathfrak{P} \in \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ in the notation of (4.5)). We assume that $\mathfrak{P} \subset \mathcal{L}$. Set $B = J/\mathfrak{P}J$ and let \mathcal{B} be the Néron model over S of B . The factor ring $R := \mathbf{T}/\mathfrak{P}$ may be regarded as a subring of $\text{End}_K(B)$. Note that R is an order of the (algebraic number) field F of fractions of R .

The decomposition (4.15) :

$$\hat{\mathbf{T}}_{(l)} \simeq \hat{\mathbf{T}}_{\mathcal{L}} \times (\hat{\mathbf{T}}_{\mathcal{L}})', \quad \varepsilon_{\mathcal{L}} = (1, 0)$$

induces

$$R \otimes_{\mathbb{Z}} \mathbf{Z}_l \simeq \hat{\mathbf{T}}_{\mathcal{L}} / \mathfrak{P} \hat{\mathbf{T}}_{\mathcal{L}} \times (\hat{\mathbf{T}}_{\mathcal{L}})' / \mathfrak{P} (\hat{\mathbf{T}}_{\mathcal{L}})'$$

and

$$F \otimes_{\mathbb{Q}} \mathbf{Q}_l = R \otimes_{\mathbb{Z}} \mathbf{Q}_l \simeq E \times E',$$

where $E = \hat{\mathbf{T}}_{\mathcal{L}} / \mathfrak{P} \hat{\mathbf{T}}_{\mathcal{L}} \otimes_{\mathbb{Z}_l} \mathbf{Q}_l$ and $E' = (\hat{\mathbf{T}}_{\mathcal{L}})' / \mathfrak{P} (\hat{\mathbf{T}}_{\mathcal{L}})' \otimes_{\mathbb{Z}_l} \mathbf{Q}_l$. Let $E = E_1 \times \dots \times E_h$ be the decomposition of E into fields E_1, \dots, E_h of finite degree over \mathbf{Q}_l . The assumption $\mathfrak{P} \subset \mathcal{L}$ implies that $E \neq 0$.

For an E -module V , we define

$$\dim_E V := (\dim_{E_1}(e_1 V), \dots, \dim_{E_h}(e_h V)),$$

where $e_i = (0, \dots, \underset{i}{1}, \dots, 0) \in E_1 \times \dots \times E_h = E$.

Theorem (5.1). *Notations and assumptions as above. Set*

$$V = \varepsilon_{\mathcal{L}} H_{\text{ét}}^1(S, V_l(\mathcal{B})),$$

where $H_{\text{ét}}^1(S, V_l(\mathcal{B})) = (\varprojlim_{l'} H_{\text{ét}}^1(S, \mathcal{B}[l'])) \otimes_{\mathbb{Z}_l} \mathbf{Q}_l$ by definition. Then

- (i) $\dim_E V = (0, \dots, 0)$ or $(1, \dots, 1)$ (i.e. V is a free E -module of rank ≤ 1).
- (ii) $\dim_E V = (0, \dots, 0)$ if and only if $w_n + 1 \in \mathfrak{P}$,
 $\dim_E V = (1, \dots, 1)$ if and only if $w_n - 1 \in \mathfrak{P}$.

Proof. (i) First we note that

$$V = \varepsilon_{\mathcal{F}} H_{\text{ét}}^1(S, V_l(\mathcal{B})) = \varepsilon_{\mathcal{F}} H_{\text{ét}}^1(S, V_l(\mathcal{B}^0)) \simeq (\varprojlim H_{\text{ét}}^1(S, \varepsilon_{\mathcal{F}} \mathcal{B}^0[l^r])) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

Now $\varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^r])$ is admissible from (4.17), so it follows from (1.11) that

$$\begin{aligned} h^1(\varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^r])) &\leq \delta_n(\varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^r])) + h^0(\varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^r])) \\ &\leq \delta_n(\varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^r])) + L_0, \end{aligned}$$

where we define $L_0 = \text{length}_{\mathbf{Z}\text{-mod}} B(K)[l^\infty]$. (Note that $L_0 < \infty$ since $B(K)$ is a finitely generated \mathbf{Z} -module.)

Lemma (5.2). $\mathcal{B}^0 \times_S \kappa(\mathfrak{n})$ is a torus. In other words,

$$\mathcal{B}^0 \times_S \overline{\kappa(\mathfrak{n})} \simeq (\mathbf{G}_m)^b,$$

where b is the dimension of B .

Proof. By the result of [13], we see that the special fiber of \mathcal{F}^0 , the “connected component” of the Néron model \mathcal{F} over S of J , is a torus. From this, the statement follows immediately. ■

From (2.1) and (5.2), we conclude that

$$\begin{aligned} \delta_n(\varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^r])) &= r \cdot 2 \dim_{\mathbb{Q}_l} E - r \cdot \dim_{\mathbb{Q}_l} E \\ &= r \cdot \dim_{\mathbb{Q}_l} E. \end{aligned}$$

Now from the exact sequence

$$H^1(S, \varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^m])) \rightarrow H^1(S, \varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^{m+r}])) \rightarrow H^1(S, \varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^r])),$$

we obtain the following exact sequence for each $r \geq 0$

$$\begin{aligned} T \xrightarrow{l^r} T \rightarrow H^1(S, \varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^r])) \\ (\text{i.e. } T/l^r T \hookrightarrow H^1(S, \varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^r])), \end{aligned}$$

where $T = \varprojlim H^1(S, \varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^m]))$. Thus, for each $r \geq 0$, we have

$$\begin{aligned} r \dim_{\mathbb{Q}_l} V &\leq \text{length}_{\mathbf{Z}} T/l^r T \quad (\text{Note that } V = T \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.) \\ &\leq h^1(\varepsilon_{\mathcal{F}}(\mathcal{B}^0[l^r])) \end{aligned}$$

$$\begin{aligned} &\leq \delta_n(\mathcal{E}_{\mathcal{L}}(\mathcal{B}^0[I^r])) + L_0 \\ &= r \dim_{\mathbf{Q}_l} E + L_0. \end{aligned}$$

Since $r \geq 0$ is arbitrary, we obtain $\dim_{\mathbf{Q}_l} V \leq \dim_{\mathbf{Q}_l} E$, or

$$\sum_{i=1}^h [E_i : \mathbf{Q}_l] \dim_{E_i}(e_i V) \leq \sum_{i=1}^h [E_i : \mathbf{Q}_l].$$

Case 1 : $\dim_{E_i}(e_i V) > 0$ for all $i=1, \dots, h$.

In this case, the inequality above forces $\dim_E(V)$ to be $(1, \dots, 1)$.

Case 2 : There exists an $i_0 \in \{1, \dots, h\}$ such that $\dim_{E_{i_0}}(e_{i_0} V) = 0$.

Let ρ'_F (resp. σ'_{F, l, E_i}) denote ρ_F (resp. σ_{F, l, E_i}) for B'/K and $R \rightarrow \text{End}_K(B) \xrightarrow{\prime} \text{End}_K(B')$ (cf. § 2). Since $\sigma'_{F, l, E_{i_0}} = 0$, we obtain that $\rho'_F = 0$ from (2.4) (ii). This implies that for all $i=1, \dots, h$, $\sigma'_{F, l, E_i} = 0$ ((2.4) (i)), i.e. $\dim_E V = (0, \dots, 0)$.

(ii) Fix a polarization $\lambda : B \rightarrow B'$ over K .

Lemma (5.3). *The ring homomorphism $R \rightarrow \text{End}_K(B)$ satisfies the condition (2.6).*

Proof. Take a prime number l' which does not divide q (e.g. $l' = l$) and let

$$e_{l'}^\lambda : T_{l'}(B(\overline{K})) \times T_{l'}(B(\overline{K})) \rightarrow \mathbf{Z}_{l'}(1)$$

be the Weil pairing associated to λ . It is well-known that the condition (2.6) is equivalent to :

$$e_{l'}^\lambda(ax, y) = e_{l'}^\lambda(x, ay) \quad \text{for all } x, y \in T_{l'}(B(\overline{K})), a \in R.$$

Now for each maximal ideal $\mathfrak{p} \neq \mathfrak{n}$ of A , we have an isomorphism

$$T_{l'}(B(\overline{K})) \simeq T_{l'}((B \times_{\mathfrak{S}} \kappa(\mathfrak{p}))(\overline{\kappa(\mathfrak{p})})),$$

via which we shall identify these two modules with each other. Denoting by $\varphi_{\mathfrak{p}}$ the $\#(\kappa(\mathfrak{p}))$ -th power Frobenius element in $\text{Gal}(\overline{\kappa(\mathfrak{p})}/\kappa(\mathfrak{p}))$, we obtain

$$\begin{aligned} e_{l'}^\lambda(T_{\mathfrak{p}}x, y) &= e_{l'}^\lambda((\varphi_{\mathfrak{p}} + q^{\deg \mathfrak{p}} \varphi_{\mathfrak{p}}^{-1})x, y) \\ &= e_{l'}^\lambda(\varphi_{\mathfrak{p}}x, y) + q^{\deg \mathfrak{p}} e_{l'}^\lambda(\varphi_{\mathfrak{p}}^{-1}x, y) \\ &= \varphi_{\mathfrak{p}} e_{l'}^\lambda(x, \varphi_{\mathfrak{p}}^{-1}y) + q^{\deg \mathfrak{p}} \varphi_{\mathfrak{p}}^{-1} e_{l'}^\lambda(x, \varphi_{\mathfrak{p}}y) \end{aligned}$$

$$\begin{aligned}
 &= q^{\deg p} e_i^\lambda(x, \varphi_p^{-1}y) + e_i^\lambda(x, \varphi_p y) \\
 &= e_i^\lambda(x, (q^{\deg p} \varphi_p^{-1} + \varphi_p)y) \\
 &= e_i^\lambda(x, T_p y)
 \end{aligned} \tag{3.9}$$

Since $T' \otimes_{\mathbf{Q}} \mathbf{Q} \supset T$ in the notation of the proof of (4.2), this completes the proof of the statement. ■

Because of (5.3), we have $\sigma_{F, l, E_i} = \sigma'_{F, l, E_i}$ for each $i = 1, \dots, h$. (Note that $\rho_F = \rho'_F$ is clear from (2.3) without (5.3), since λ induces a $\mathbf{Q}_l[\text{Gal}(K^{\text{sep}}/K)]$ -isomorphism $V_i(B(\overline{K})) \simeq V_i(B'(\overline{K}))$.)

Now for each $i = 1, \dots, h$, we have

$$(5.4) \quad \sigma_{F, l, E_i} \leq 1$$

from (i), and

$$(5.5) \quad \sigma_{F, l, E_i} \equiv \rho_F \pmod{2}$$

from (2.7). Further we define $\varepsilon_n \in \{\pm 1\}$ by the condition $w_n - \varepsilon_n \in \mathfrak{P}$. (Observe that $(w_n - 1)(w_n + 1) = 0 \in \mathfrak{P}$ and \mathfrak{P} is a prime ideal of \mathbf{T} .) Fixing an inclusion $E_i \hookrightarrow \overline{\mathbf{Q}}_l$ and applying (3.17) (ii), we obtain

$$(5.6) \quad (-1)^{\rho_F} = -\varepsilon_n.$$

Then

$$\varepsilon_n = -1 \Rightarrow \rho_F \equiv 0 \pmod{2} \tag{5.6}$$

$$\Rightarrow \sigma_{F, l, E_i} \equiv 0 \pmod{2} \tag{5.5}$$

$$\Rightarrow \sigma_{F, l, E_i} = 0 \tag{5.4}$$

and

$$\varepsilon_n = 1 \Rightarrow \rho_F \equiv 1 \pmod{2} \tag{5.6}$$

$$\Rightarrow \sigma_{F, l, E_i} \equiv 1 \pmod{2} \tag{5.5}$$

$$\Rightarrow \sigma_{F, l, E_i} = 1. \tag{5.4} \blacksquare$$

The following is the main theorem of the present paper.

Theorem (5.7).

- (i) $\tilde{J}^-(K)$ is finite.
- (ii) $\text{III}(\tilde{J}^-/K) \otimes_{\mathbb{Z}} \mathbb{Z}[q^{-1}]$ is finite.

Proof. From (4.11) (ii), it suffices to prove, in the situation of (5.1), the finiteness of $B(K)$ and $\text{III}(B/K) \otimes_{\mathbb{Z}} \mathbb{Z}[q^{-1}]$ under the assumption $w_n + 1 \in \mathfrak{P}$. Note that $E \neq 0$. From (5.1), $\sigma_{E, l, E_1} = 0$, which implies that $\sigma_l = r = 0$ by (2.5) (i). Here $r = 0$ means the finiteness of $B(K)$ and $\sigma_l - r = 0$ implies the finiteness of $\text{III}(B/K) \otimes_{\mathbb{Z}} \mathbb{Z}[q^{-1}]$ ([27]). ■

Remark (5.8).

- (i) Define I_0 to be the ideal of \mathbf{T} which is generated by $\{T_p - (1 + q^{\deg p}) \mid p \neq n\} \cup \{w_n + 1\}$. By definition, $\mathbf{T}/I_0 \simeq \mathbb{Z}/N_0\mathbb{Z}$ for some natural number $N_0 \geq 0$. We claim that $N_0 \neq 0$. In fact if $N_0 = 0$, then $E = J/I_0 J$ is a non-zero abelian variety over K and (3.10) implies that the action of φ_p on $V_l(E(\bar{K}))$ satisfies the equation $(\varphi_p - 1)(\varphi_p - q^{\deg p}) = 0$, where $p \in \Sigma - \{\infty, n\}$ and l is a fixed prime number prime to q . This contradicts the well-known (and already proved) ‘‘Riemann hypothesis’’.

From definitions and from (4.8), we obtain that $I_0 \supset I$ and that N divides N_0 .

Question (5.9). $I_0 = I$? (In other words, $N_0 = N$?)

In the case of the modular curve $X_0(p)/\mathbb{Q}$ (p : prime number), Mazur has settled the corresponding question ([19, II, (9.7)]).

Note that if we define I'_0 to be the kernel of $\mathbf{T} \rightarrow (\mathbf{T}/I_0) \otimes_{\mathbb{Z}} \mathbb{Z}[q^{-1}]$, then $I_0 \subset I'_0 \subset I$ from (4.7) and (4.8), and the results of this section still hold in case I is replaced by I'_0 .

- (ii) We ask another:

Question (5.10). $\tilde{J} = \tilde{J}^-$?

(We have seen in (4.13) that this is true *unless* q is odd and d is divided by 4.)

The corresponding question in the case of the modular curve $X_0(p)$ over \mathbb{Q} (p : prime number) has also been settled by Mazur ([19, II, (17.10)]). Without the equality (5.10), however, we may hope that \tilde{J}^- will play some role in the study of rational points on Drinfeld modular curves (cf. [20, § 3, Axiom 2]).

- (iii) Roughly speaking, our theory is concerned only with the Hecke algebra tensored with \mathbb{Q} . (It might sound strange because the Eisenstein ideal does not make sense after tensored by \mathbb{Q} , though.) In fact, the finiteness of the Mordell-Weil group and the Shafarevich-Tate group only involves the Hecke algebra tensored by \mathbb{Q} .

On the other hand, in [19], to settle the questions corresponding to (5.9) and (5.10) above, it is necessary to develop an elaborate theory of the Hecke algebra

itself, and, for that, the theory of modular forms defined over an arbitrary commutative ring, not only over a field of characteristic 0, is indispensable.

This is the main reason why (5.9) and (5.10) remain open in our case. Drinfeld's theory only involves automorphic forms defined over a field of characteristic 0, like $\overline{\mathbf{Q}}_l$, and no satisfactory theory of automorphic forms defined over an arbitrary commutative ring has been established so far in the function field case. ■

Appendix. The Endomorphism Ring of $J_0(\mathfrak{n})$ (\mathfrak{n} : Maximal)

Notations as in the text. We prove the following theorem (cf. (4.2) (iii)).

Theorem (A.1). *If \mathfrak{n} is a maximal ideal of A , then*

$$\text{End}_{\overline{K}}(J_0(\mathfrak{n})) = \text{End}_K(J_0(\mathfrak{n})).$$

Corollary (A.2).

$$\mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q} = \text{End}_{\overline{K}}(J_0(\mathfrak{n})) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Proof. Immediate from (A.1) and (4.2) (iii). ■

Corollary (A.3). *There exist the following one-to-one correspondences*

$$\begin{aligned} & \{\overline{K}\text{-isogeny classes of } \overline{K}\text{-simple abelian variety factors of } J_0(\mathfrak{n})\} \\ \longleftrightarrow & \{\overline{K}\text{-isogeny classes of } K\text{-simple abelian variety factors of } J_0(\mathfrak{n})\} \\ \longleftrightarrow & \{K\text{-isogeny classes of } K\text{-simple abelian variety factors of } J_0(\mathfrak{n})\} \\ \longleftrightarrow & \{\text{fields occurring in the direct product decomposition of } \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{Q}\} \\ \longleftrightarrow & \{\text{minimal ideals of } \mathbb{T}\}. \end{aligned}$$

Proof. Easy to see from (A.1) and (A.2). (Note that \mathbb{T} is commutative.) ■

Remark (A.4). It is known that for an abelian variety B over a field K ,

$$\text{End}_L(B) = \text{End}_{K^{\text{sep}}}(B)$$

holds, where L is an arbitrary extension field of K including K^{sep} . Therefore (A.1)–(A.3) still hold if we replace \overline{K} by such L (especially by K^{sep}).

Now let us begin the proof of (A.1). Write J instead of $J_0(\mathfrak{n})$ as in the text.

First by using the result of [24], we shall show that the endomorphism ring is defined over an extension field of K which is “quite small”.

Lemma (A.5). *J has semi-stable reduction at any $v \in \Sigma$.*

Proof. At $v \in \Sigma - \{n, \infty\}$, J has good reduction. At $v = n$, the result of [13] implies that J has semi-stable reduction (cf. (5.2)). At $v = \infty$, (3.7) implies the following $\text{Gal}(K_{\infty}^{\text{sep}}/K_{\infty})$ -isomorphism :

$$V_l(J(\overline{K}_{\infty}))^* \otimes_{\mathbb{Q}_l} \overline{\mathbf{Q}}_l \simeq W_{\infty}^{\oplus g},$$

where W_{∞} is as in § 3 and g is the dimension of J . Therefore we obtain a $\text{Gal}(K_{\infty}^{\text{sep}}/K_{\infty})$ -isomorphism :

$$V_l(J(\overline{K}_{\infty})) \otimes_{\mathbb{Q}_l} \overline{\mathbf{Q}}_l \simeq (W_{\infty}^*)^{\oplus g},$$

which implies that the action of the inertia group on $V_l(J(\overline{K}_{\infty}))$ is unipotent, since there exists an exact sequence :

$$0 \rightarrow \overline{\mathbf{Q}}_l(1) \rightarrow W_{\infty}^* \rightarrow \overline{\mathbf{Q}}_l \rightarrow 0. \quad \blacksquare$$

From [24, Theorem 1.1] and from (A.5), we can see that all the elements of $\text{End}_{\overline{K}}(J)$ are defined over the maximal unramified extension field \tilde{K} of K . Note that the field \tilde{K} coincides with $\overline{\mathbb{F}}_q K (= \overline{\mathbb{F}}_q(T))$, as $\pi_1(\mathbb{P}_{\overline{\mathbb{F}}_q}^1, *) = 1$. Since $\text{End}_{\overline{K}}(J)$ is finitely generated over \mathbf{Z} , we have

$$\text{End}_{\overline{K}}(J) = \text{End}_{\tilde{K}}(J) = \text{End}_{\mathbb{F}_{q^r} K}(J)$$

for sufficiently large r . \blacksquare

Remark (A.6). For a polarization $\lambda : J \rightarrow J'$ over K , $\mathbf{T}_{\mathbb{Z}} \otimes \mathbf{Q}$ is invariant under the Rosati involution, as we can see by using (3.9) (cf. (5.3)). Therefore the pairing $(x, y) \mapsto \text{Tr}_{\mathbf{T}_{\mathbb{Z}} \otimes \mathbf{Q}}(xy)$ on $\mathbf{T}_{\mathbb{Z}} \otimes \mathbf{Q}$ is positive definite, hence, in the decomposition (4.4) $\mathbf{T}_{\mathbb{Z}} \otimes \mathbf{Q} \simeq F_1 \times \cdots \times F_s$, each F_i is a totally real algebraic number field. On the other hand, each K -simple abelian variety factor of J has semi-stable bad reduction at n , as can be seen just as in (5.2). So, no such factor has complex multiplication in the sense of [28].

Thus the assumptions of [24, Theorem 2.3] are all satisfied and the conclusion is that all the elements of $\text{End}_{\overline{K}}(J)$ are defined over the compositum of quadratic extension fields of K . So, we obtain

$$\text{End}_{\overline{K}}(J) = \text{End}_{\mathbb{F}_{q^2} K}(J) ;$$

in other words, we may assume $r=2$. (But this result will not be used in the proof below.)

Since $\text{End}_{\bar{K}}(J)/\text{End}_K(J) = \text{End}_{K^{\text{sep}}}(J)/\text{End}_K(J)$ is a torsion-free \mathbf{Z} -module as can be seen by considering the action of $\text{Gal}(K^{\text{sep}}/K)$, it suffices to show

$$\text{End}_{\bar{K}}(J) \otimes_{\mathbf{Z}} \mathbf{Q} = \text{End}_K(J) \otimes_{\mathbf{Z}} \mathbf{Q} = \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Q},$$

or

$$\text{End}_{\bar{K}}(J) \otimes_{\mathbf{Z}} \bar{\mathbf{Q}}_l = \mathbf{T} \otimes_{\mathbf{Z}} \bar{\mathbf{Q}}_l$$

for a prime number l not dividing q .

Notation (for simplicity). Let k be a field and let V and V' be $\bar{\mathbf{Q}}_l[\text{Gal}(k^{\text{sep}}/k)]$ -modules. For an extension field k' of k which is included in k^{sep} , we define

$$\text{Hom}_{(k')} (V, V') := \text{Hom}_{\bar{\mathbf{Q}}_l[\text{Gal}(k^{\text{sep}}/k)]} (V, V').$$

Lemma (A.7). *Let V and V' be $\bar{\mathbf{Q}}_l[\text{Gal}(K^{\text{sep}}/K_{\infty})]$ -modules both of which are isomorphic to W_{∞} . Let L be a finite extension field of K_{∞} which is included in K_{∞}^{sep} . Then*

$$\text{Hom}_{(L)} (V, V') = \text{Hom}_{(K_{\infty})} (V, V').$$

Proof. We may assume that $V = V' = W_{\infty}$. We have the following non-split exact sequence of $\text{Gal}(K^{\text{sep}}/K_{\infty})$ -modules :

$$0 \rightarrow \bar{\mathbf{Q}}_l \rightarrow W_{\infty} \rightarrow \bar{\mathbf{Q}}_l(-1) \rightarrow 0.$$

This exact sequence is non-split also as a sequence of $\text{Gal}(K^{\text{sep}}/L)$ -modules, since the image of the inertia group of $\text{Gal}(K^{\text{sep}}/K_{\infty})$ in $\text{Aut}(W_{\infty})$ is infinite. Let D be the image of $\bar{\mathbf{Q}}_l \rightarrow W_{\infty}$ above.

Now $f \in \text{Hom}_{(L)}(W_{\infty}, W_{\infty})$ acts on D since $\text{Hom}_{(L)}(\bar{\mathbf{Q}}_l, \bar{\mathbf{Q}}_l(-1)) = 0$. As D is of dimension 1 over $\bar{\mathbf{Q}}_l$, $f - a \cdot \text{id}_{W_{\infty}}$ kills D for some $a \in \bar{\mathbf{Q}}_l$. If $f - a \cdot \text{id}_{W_{\infty}}$ does not kill the whole space W_{∞} , then $(f - a \cdot \text{id}_{W_{\infty}})W_{\infty}$ is a $\text{Gal}(K^{\text{sep}}/L)$ -submodule of W_{∞} of dimension 1 over $\bar{\mathbf{Q}}_l$. Since the exact sequence above is non-split, $(f - a \cdot \text{id}_{W_{\infty}})W_{\infty}$ must coincide with D .

$$\begin{array}{ccccccc} 0 & \rightarrow & \bar{\mathbf{Q}}_l & \rightarrow & W_{\infty} & \rightarrow & \bar{\mathbf{Q}}_l(-1) \rightarrow 0 \\ & & \downarrow & \swarrow & \downarrow f-a \cdot \text{id}_{W_{\infty}} & & \\ 0 & \rightarrow & \bar{\mathbf{Q}}_l & \rightarrow & W_{\infty} & \rightarrow & \bar{\mathbf{Q}}_l(-1) \rightarrow 0. \end{array}$$

Hence $f - a \cdot id_{W_\infty}$ induces a non-trivial element of $\text{Hom}_{(L)}(\overline{\mathbf{Q}}_l(-1), \overline{\mathbf{Q}}_l)$, which is absurd.

Thus $f - a \cdot id_{W_\infty}$ kills W_∞ , that is to say $f \in \overline{\mathbf{Q}}_l \cdot id_{W_\infty}$. This shows that $\text{Hom}_{(L)}(W_\infty, W_\infty) = \overline{\mathbf{Q}}_l \cdot id_{W_\infty} \subset \text{Hom}_{(K_\infty)}(W_\infty, W_\infty)$, which implies (A.7). ■

Each element $f \in \text{End}_{\overline{K}}(J)$ defines an element of $\text{End}_{\overline{\mathbf{Q}}_l}(\bigoplus_{j=1}^g \rho(\pi_j))$ in the proof of (4.2). It suffices to show that the image of f belongs to $\prod_{j=1}^g \overline{\mathbf{Q}}_l$ ($\subset \text{End}_{\overline{\mathbf{Q}}_l}(\bigoplus_{j=1}^g \rho(\pi_j))$). Thus the following lemma (A.8) completes the proof of (A.1), since $\text{End}_{\overline{K}}(J) = \text{End}_{\mathbb{F}_{q^r K}}(J)$, as we have already seen.

Lemma (A.8).

$$\text{Hom}_{(\mathbb{F}_{q^r K})}(\rho(\pi_j), \rho(\pi_{j'})) = \begin{cases} \overline{\mathbf{Q}}_l \cdot id_{\rho(\pi_j)} & j=j' \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Fixing an embedding $K^{\text{sep}} \hookrightarrow K_\infty^{\text{sep}}$, we have

$$\begin{aligned} & \text{Hom}_{(\mathbb{F}_{q^r K})}(\rho(\pi_j), \rho(\pi_{j'})) \\ & \subset \text{Hom}_{(\mathbb{F}_{q^r K_\infty})}(\rho(\pi_j), \rho(\pi_{j'})) \\ & = \text{Hom}_{(K_\infty)}(\rho(\pi_j), \rho(\pi_{j'})) \end{aligned} \tag{A.7},$$

so

$$\begin{aligned} & \text{Hom}_{(\mathbb{F}_{q^r K})}(\rho(\pi_j), \rho(\pi_{j'})) \\ & = \text{Hom}_{(\mathbb{F}_{q^r K} \cap K_\infty)}(\rho(\pi_j), \rho(\pi_{j'})) \\ & = \text{Hom}_{(K)}(\rho(\pi_j), \rho(\pi_{j'})), \end{aligned}$$

which implies the statement, just as we have seen in the proof of (4.2). ■

References

[1] Barsotti, I., Structure theorems for group-varieties, *Ann. Mat. Pura Appl.*, **38** (1955), 77–119.
 [2] Bruhat, F., *Lectures on some aspects of p-adic analysis, Lectures on Mathematics and Physics*, **27**, Tata Institute, 1963.
 [3] Casselman, W., On some results of Atkin and Lehner, *Math. Ann.*, **201** (1973), 301–314.
 [4] Curtis, C. W., Reiner, I., *Representation theory of finite groups and associative algebras*, Interscience, 1962.
 [5] Deligne, P., Les constantes des equations fonctionelles des fonctions L , in *Modular Functions of One Variable II, Lecture Notes in Math.*, **349**, Springer-Verlag, 1973, 501–597.
 [6] ———, La conjecture de Weil II, *Publ. Math. IHES*, **52** (1980), 137–252.
 [7] Deligne, P., Husemoller, D., Survey of Drinfeld modules, *Contemp. Math.*, **67** (1987).

- [8] Demazure, M., Gabriel, P., *Groupes Algébriques, I*, North-Holland, 1970.
- [9] Drinfeld, V. G., Elliptic modules, *Math. USSR Sbornik*, **23** (1974), 4, 561–592.
- [10] ———, Two dimensional l -adic representations of the Galois group of a global field of characteristic p and automorphic forms on $GL(2)$, *J. Soviet Math.*, **36**, No. 1 (1987), 93–105.
- [11] Gekeler, E.-U., Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern, *Bonner Math. Schriften*, **119** (1980).
- [12] ———, Automorphe Formen über $F_q(T)$ mit kleinem Führer, *Abh. Math. Sem. Univ. Hamburg*, **55** (1985), 111–146.
- [13] Gekeler, E.-U., Über Drinfeld'sche Modulkurven vom Hecke-Type, *Compositio Math.*, **57** (1986), 219–236.
- [14] ———, *Drinfeld modular curves, Lecture Notes in Math.*, **1231**, Springer-Verlag, 1986.
- [15] Gelbart, S. S., *Automorphic forms on adèle groups, Ann. of Math. Stud.*, **83**, Princeton, 1975.
- [16] Goss, D., π -adic Eisenstein series for function fields, *Compositio Math.*, **41** (1980), 3–38.
- [17] Jacquet, H., Langlands, R. P., *Automorphic forms on $GL(2)$, Lecture Notes in Math.*, **114**, Springer-Verlag, 1970.
- [18] Katz, N. M., Mazur, B., *Arithmetic moduli of elliptic curves, Ann. of Math. Stud.*, **108**, Princeton, 1985.
- [19] Mazur, B., Modular curves and the Eisenstein ideal, *Publ. Math. IHES*, **47** (1978), 35–193.
- [20] ———, Rational points on modular curves, in *Modular Functions of One Variable V, Lecture Notes in Math.*, **601**, Springer-Verlag, 1977, 107–148.
- [21] Milne, J. S., *Étale cohomology*, Princeton, 1980.
- [22] Mumford, D., *Abelian varieties*, Oxford, 1970.
- [23] Ribet, K. A., Galois action on division points of abelian varieties with real multiplications, *Amer. J. Math.*, **98** (1976), 751–804.
- [24] ———, Endomorphisms of semi-stable abelian varieties over number fields, *Ann. of Math.*, **101** (1975), 555–562.
- [25] Robert, A., Formes automorphes sur GL_2 (Travaux de H. Jacquet et R. P. Langlands), *Sém. Bourbaki 1971/72*, **415**.
- [26] Rosenlicht, M., Some basic theorems on algebraic groups, *Amer. J. Math.*, **78** (1956), 2, 401–443.
- [27] Schneider, P., Zur Vermutung von Birch und Swinnerton-Dyer über globalen Funktionenkörpern, *Math. Ann.*, **260** (1982), 495–510.
- [28] Serre, J.-P., Tate, J., Good reduction of abelian varieties, *Ann. of Math.*, **88** (1968), 3, 492–517.
- [29] Shimura, G., Algebraic number fields and symplectic discontinuous groups, *Ann. of Math.*, **86** (1967), 503–592.
- [30] Shimura, G., Taniyama, Y., *Complex multiplication of abelian varieties and its application to number theory*, 2nd printing corrected, Math. Soc. of Japan, 1975.
- [31] Teitelbaum, J. T., Modular symbols for $F_q(T)$, *Duke Math. J.*, **68** (1992), 271–295.
- [32] Weil, A., *Dirichlet series and automorphic forms, Lecture Notes in Math.*, **189**, Springer-Verlag, 1971.
- [33] ———, *Basic Number Theory*, 3rd ed., Springer-Verlag, 1974.