F. Momose
Nagoya Math. J.
Vol. 91 (1983), 19–36

GALOIS ACTION ON SOME IDEAL SECTION POINTS OF THE ABELIAN VARIETY ASSOCIATED WITH A MODULAR FORM AND ITS APPLICATION

FUMIYUKI MOMOSE

Introduction

For an integer N, let $X_1(N)$ be the modular curve defined over $\boldsymbol{Q}$ which corresponds to the modular group $\Gamma_1(N)$. To each primitive cusp form $f = \sum a_m q^m$, $a_1 = 1$, (= normalized new form in the sense of [1]) on $\Gamma_1(N)$ of weight 2, there corresponds a factor J_f of the jacobian variety of $X_1(N)$ (cf. Shimura [19]). Shimura [20] and Ohta [11] etc. investigated the Galois action on some ideal section points of J_f. They treated the case when f is a primitive cusp form on $\Gamma_1(l)$ with the neben typus character $\left(\frac{l}{\ }\right)$ for a prime number l, $l \equiv 1 \bmod 4$. We here treat the forms on $\Gamma_0(l^n)$ (*i.e.*, the Haupt form) for a prime number $l \neq 2$. Put $K_f = \boldsymbol{Q}(a_m \mid 1 \leqq m \in \boldsymbol{Z})$ and δ_f be the ideal of the ring of integers $\mathcal{O}$ of K_f generated by a_q for all primes q such that $\left(\frac{\pm l}{q}\right) = -1$. Here, the sign $\pm$ is chosen so that $\pm l \equiv 1 \bmod 4$. When a form f is associated with a Grössen-character of an imaginary quadratic field (cf. [18]), we say that f has C.M. or f is a form with C.M. One of the results is the following, which was conjectured in Saito [17]:

Proposition (cf. (1.10), (1.16)). *Let f be a primitive cusp form on $\Gamma_0(l^n)$ of weight 2 for a prime number l, $l \equiv -1 \bmod 4$. Assume tket there exists a prime $\mathfrak{P}$ of K_f which divides δ_f but not divide $2l$. Then, there exists a primitive cusp form Θ with C.M. on $\Gamma_0(l^n)$ of weight 2 such that*

$$f \equiv \Theta \bmod \bar{\mathfrak{P}},$$

where $\bar{\mathfrak{P}}$ is an extension of $\mathfrak{P}$ to $\bar{\boldsymbol{Q}}$. Further, if $\mathfrak{P} \nmid (l-1)\cdot l$, f and Θ belong to the same direct factor in Saito's decomposition of the space $S_2^0(\Gamma_0(l^n))$

Received August 26, 1981.

https://doi.org/10.1017/S0027763000020444 Published online by Cambridge University Press

in [17] (*cf.* (1.14), (1.15)).

The other topic considered in this paper concerns the endomorphism algebra of J_f. If f does not have C.M., $\delta_f \neq (0)$ (cf. [14]). There are many examples of the forms f without C.M. such that $\delta_f \neq (1)$, which have non-trivial twists (cf. [4], [8], [17] etc.). *Let* f be a primitive cusp form on $\Gamma_0(l^n)$ without C.M. and put $F_f = \boldsymbol{Q}(a_q^2 \,|\, q\colon \text{primes})$. Then, the endomorphism algebra $\operatorname{End} J_f \otimes \boldsymbol{Q}$ is isomorphic to K_f or a quaternion algebra over F_f which contains K_f as a maximal commutative subfield (cf. [10], [15]). In the latter case, $n \geqq 2$ (cf. [13]) and the algebra is generated by K_f and the twisting operator (cf. [10], [15]). If $l \equiv 1 \bmod 4$, the algebra is isomorphic to a matrix algebra (cf. [16]). Except for the one example of Koike [8], we have not known the example such that the corresponding algebra is a division algebra. We give here other two examples (which were calculated by Saito [17]) and their discriminants.

Notation. For an algebraic number field L of finite degree or a finite extension L of $\boldsymbol{Q}_p$, $\mathcal{O}_L$, G_L denote the ring of integers of L and the Galois group $\operatorname{Gal}(\bar{L}/L)$, respectively. For a prime $\mathfrak{p}$ of $\mathcal{O}_L$, $L_\mathfrak{p}$, $\mathcal{O}_{L_\mathfrak{p}}$, $\kappa(\mathfrak{p})$ and $\sigma_\mathfrak{p}$ respectively denote the $\mathfrak{p}$-adic completion of L, the maximal order of $L_\mathfrak{p}$, the residue field $\mathcal{O}_L/\mathfrak{p}$ and a Frobenius element of the prime $\mathfrak{p}$, and often denote by $\mathcal{O}_\mathfrak{p}$ instead of $\mathcal{O}_{L_\mathfrak{p}}$ and by G instead of $G_{\boldsymbol{Q}}$. For an abelian variety A defined over a finite extension L of $\boldsymbol{Q}$ or $\boldsymbol{Q}_p$, $A_{/\mathcal{O}_L}$ denotes the Néron model of A over $\mathcal{O}_L$. Further, if the ring of the endomorphisms $\operatorname{End} A$ of A contains an order $\mathcal{O}$ of an algebraic number field, for an ideal $\mathfrak{P}$ of $\mathcal{O}$, ${}_\mathfrak{P}A$ denotes the $\mathfrak{P}$-ideal section points $\bigcap_{x \in \mathfrak{P}} \ker(x\colon A \to A)$ of A, and ${}_\mathfrak{P}A_{/\mathcal{O}_L}$ denotes the schematic closure of ${}_\mathfrak{P}A$ in the Néron model $A_{/\mathcal{O}_L}$. For a prime number p, μ_p denotes the group consisting of the p-th roots of 1, and χ_p denotes the character of G induced from the Galois action on μ_p.

§ 1. Galois action on division points

Let $l \geqq 3$ be a prime number, $n \geqq 1$ be an integer and $f = \sum a_m q^m$, $a_1 = 1$, be a primitive cusp form on $\Gamma_0(l^n)$ of weight 2. Let $J = J_f$ be the abelian variety (defined over $\boldsymbol{Q}$) associated with f (cf. Shimura [19]) and put $K = K_f = \boldsymbol{Q}(a_m \,|\, 1 \leqq m \in \boldsymbol{Z})$, $F = F_f = \boldsymbol{Q}(a_q^2 \,|\, q\colon \text{primes})$. Denote by $V_p = V_{f,p}$ the Tate module $T_p(J)(\bar{\boldsymbol{Q}}) \otimes \boldsymbol{Q}_p$ for each prime p, and put $V_\mathfrak{P} = V_p \otimes K_\mathfrak{P}$ for each prime $\mathfrak{P}$ of $\mathcal{O} = \mathcal{O}_K$ lying over p. The Néron model $J_{/\boldsymbol{Z}[1/l]}$ is an abelian scheme (cf. [3]). We can choose an abelian variety

$J'(\ /\boldsymbol{Q})$ on which $\mathcal{O}$ operates and which is isogenous to J over $\boldsymbol{Q}$ (cf. [21] § 7). Put $k = \boldsymbol{Q}(\sqrt{\pm l})$ and $G = \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$, $G_k = \mathrm{Gal}(\bar{\boldsymbol{Q}}/k)$, where the sign $\pm$ is chosen such that $\pm\, l \equiv 1 \mod 4$.

LEMMA (1.1). *Under the notation as above, let* $\mathfrak{p}$ *be a prime of* k *lying over* p *and put* $\overline{M} = {}_{\mathfrak{P}}J'(\bar{\boldsymbol{Q}})$. *Assume that* $p \nmid 2 \cdot l$ *and* $\overline{M}$ *decomposes into a direct sum of* $\kappa(\mathfrak{P})[G_{k_\mathfrak{p}}]$*-modules* $\overline{M}_1$ *and* $\overline{M}_2$:

$$\overline{M} = \overline{M}_1 \oplus \overline{M}_2 ,$$

where $\kappa(\mathfrak{P}) = \mathcal{O}/\mathfrak{P}$. *Then,* ${}_{\mathfrak{P}}J'_{/\mathcal{O}_\mathfrak{p}}$ *decomposes into a product of finite flat group schemes "en* $\kappa(\mathfrak{P})$*-vectoriels"* X_1 *and* X_2:

$${}_{\mathfrak{P}}J'_{/\mathcal{O}_\mathfrak{p}} = X_1 \times_{\mathcal{O}_\mathfrak{p}} X_2 .$$

Proof. By our assumption, ${}_{\mathfrak{P}}J' \otimes k_\mathfrak{p}$ decomposes into a product of two finite group schemes X'_1 and X'_2:

$${}_{\mathfrak{P}}J' \otimes k_\mathfrak{p} = X'_1 \times X'_2 .$$

Let X_i $(i = 1, 2)$ be the schematic closure of X'_i in the Néron model $J'_{/\mathcal{O}_\mathfrak{p}}$ (, then X_i are finite flat group schemes, because $J'_{/\mathcal{O}_\mathfrak{p}}$ is proper (cf. [3], [12])). Consider the following morphism g induced from the canonical morphism of J' onto $J'' = J'/X_2$ by the universal property of the Néron models:

$$g\colon\ J'_{/\mathcal{O}_\mathfrak{p}} \longrightarrow J''_{/\mathcal{O}_\mathfrak{p}} .$$

The morphism $g|X_1$: $X_1 \to g(X_1)$ $(\subset J''_{/\mathcal{O}_\mathfrak{p}})$ is isomorphic over the generic point of Spec $\mathcal{O}_\mathfrak{p}$. As $\mathrm{ord}_\mathfrak{p}\, p = 1 < p - 1$, by the fundamental property of the finite flat group schemes (cf. [12]), $g|X_1$ is an isomorphism. Then, we have the following exact sequence:

$$\begin{array}{ccccc} X_2 & \hookrightarrow & {}_{\mathfrak{P}}J'_{/\mathcal{O}_\mathfrak{p}} & \xrightarrow{\ g\ } & g(X_1) . \\ & & \cup & \overset{\sim}{\nearrow} & \\ & & X_1 & & \end{array}$$

Therefore, ${}_{\mathfrak{P}}J'_{/\mathcal{O}_\mathfrak{p}} = X_1 \times_{\mathcal{O}_\mathfrak{p}} X_2$. Q.E.D.

Let $\delta = \delta_f$ be the ideal of $\mathcal{O} = \mathcal{O}_K$ generated by a_q for all primes q which remain primes in $k = \boldsymbol{Q}(\sqrt{\pm l})$. For a prime $\mathfrak{P}|p$ of $\mathcal{O} = \mathcal{O}_K$, choose a lattice M of $V_\mathfrak{P} = V_p \otimes K_\mathfrak{P}$ on which $\mathcal{O}$ and $G = \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ operate. Let $\bar{\rho}$ be the representation of G on $\overline{M} = M/\mathfrak{P}M$:

$$\bar{\rho}\colon G \longrightarrow \mathrm{Aut}_{\kappa(\mathfrak{P})}\bar{M} \hookrightarrow \mathrm{Aut}_{\bar{F}_p}(\bar{M}\otimes \bar{F}_p) \simeq GL(2, \bar{F}_p)\,.$$

We set the following condition (C) of the prime $\mathfrak{P}$ of $\mathcal{O} = \mathcal{O}_K$:

$$\text{(C)} \qquad \begin{cases} (1) & \mathfrak{P}\,|\,\delta \\ (2) & \begin{cases} \mathfrak{P}\nmid 2\cdot l & \text{if } l \equiv -1 \bmod 4\,, \\ \mathfrak{P}\nmid 2 & \text{if } l \equiv 1 \bmod 4\,. \end{cases} \end{cases}$$

LEMMA (1.2). *Let $\mathfrak{P}$ be a prime of $\mathcal{O}$ satisfying the condition* (C) *above and $\bar{\rho}$ be as above. Then, $\bar{\rho}(G_k)$ is contained in a Cartan subgroup and $\bar{\rho}(G)$ is not contained in any Borel subgroup.*

Proof. Put $R = \bar{F}_p[\bar{\rho}(G_k)]$, then for all $x \in R$ and $g \in G - G_k$, $\mathrm{tr}\,\bar{\rho}(g)x = 0$ so that $R \neq M_2(\bar{F}_p)$ and $\bar{\rho}(G_k)$ is contained in a Borel subgroup of $GL(2, \bar{F}_p)$. Let V be a 1-dimensional subspace of $\bar{M}\otimes \bar{F}_p$ which is a R-module. If $V = \bar{\rho}(g)V$ for $g \in G - G_k$, V is an $\bar{F}_p[\bar{\rho}(G)]$-module and $\bar{\rho}(G)$ is contained in a Borel subgroup. If $V \neq \bar{\rho}(g)V$ for $g \in G - G_k$, then $\bar{M}\otimes \bar{F}_p$ decomposes into a direct sum of R-modules

$$\bar{M}\otimes \bar{F}_p = V \oplus \bar{\rho}(g)V\,.$$

Then, $\bar{\rho}(G_k)$ is contained in the Cartan subgroup $\mathrm{Aut}\,V \times \mathrm{Aut}\,\bar{\rho}(g)V$ and $\bar{\rho}(G)$ is contained in the normalizer of this Cartan subgroup. If $\bar{\rho}(G)$ is contained in a Borel subgroup of $GL(2, \bar{F}_p)$, the semi-simplification of $\bar{\rho}$ is equivalent to $\mu \oplus \mu \otimes \chi_l^{\otimes(l-1)/2}$ for a character μ of G. Denote also by μ the corresponding Dirichlet character and put $\mu_p = \mu_{|Z_p^\times}$. If $p \neq l$, by the fact that $\mu^{\otimes 2} \otimes \chi_l^{\otimes(l-1)/2} = \det\cdot\bar{\rho} = \chi_p$, we should have $\mu_p^{\otimes 2} = \chi_p$, but such a character μ does not exist. If $p = l$ and $l \equiv 1 \bmod 4$, then $\mu_p^{\otimes 2} = \chi_p^{\otimes(p+1)/2}$, but such a character μ does not exist. Q.E.D.

By this lemma (1.2), as a representation on $\bar{M}\otimes \bar{F}_p$, $\bar{\rho}|G_k$ is equivalent to $\nu_1 \oplus \nu_2$ for some characters ν_i of G_k and $\nu_1 \otimes \nu_2 = \chi_{p|G_k}$. Let φ_i be the character of $k_A^\times$ (= the idèle group of k) corresponding to ν_i. For an integer $m \neq 0$, denote by $e(m)$ the idèle of k whose components dividing m are 1 and the other components are all m.

LEMMA (1.3) (cf. [21]). *Let $\mathfrak{P}\,|\,p$ be a prime of $\mathcal{O} = \mathcal{O}_K$ satisfying the condition* (C). *Then,*

$$\varphi_i(e(m)) \equiv \left(\frac{\pm\, l}{m}\right)m \mod \mathfrak{P}\,,$$

for all integers $m > 0$, $(m, p\cdot l) = 1$, and

https://doi.org/10.1017/S0027763000020444 Published online by Cambridge University Press

$$\varphi_1(\alpha^\varepsilon) - \varphi_2(\alpha)$$

for all $\alpha = (\alpha_v)_v \in k_A^\times$ *such that* $\alpha_{\infty_i} > 0$ $(i = 1, 2)$ *if* $l = 1 \bmod 4$. *Here,* $\pm l \equiv 1 \bmod 4$ *and* $1 \neq \varepsilon \in \mathrm{Gal}(k/\boldsymbol{Q})$.

Proof. For a prime $\mathfrak{q}$ of k dividing a prime $q \in \boldsymbol{Z}$, denote by $e(\mathfrak{q})$ the idèle whose $\mathfrak{q}$-component is 1 and the other components are all q. It is enough to treat the primes $\mathfrak{q} \mid q$ prime to $l \cdot p$. If $\left(\frac{\pm l}{q}\right) = -1$, by our assumption, $a_q \equiv 0 \bmod \mathfrak{P}$ and $\bar{\rho}(\sigma_q^2) \equiv -q$, where σ_q is a Frobenius element of the prime q. If $\left(\frac{\pm l}{q}\right) = 1$, put $q\mathcal{O}_k = \mathfrak{q} \cdot \mathfrak{q}^\varepsilon$, then

$$\begin{pmatrix} \varphi_1(e(\mathfrak{q}^\varepsilon)) & 0 \\ 0 & \varphi_2(e(\mathfrak{q}^\varepsilon)) \end{pmatrix} = \bar{\rho}(\sigma_{\mathfrak{q}^\varepsilon}) = \bar{\rho}(g\sigma_{\mathfrak{q}}g^{-1}) = \begin{pmatrix} \varphi_2(e(\mathfrak{q})) & 0 \\ 0 & \varphi_1(e(\mathfrak{q})) \end{pmatrix}$$

for $g \in G - G_k$, where $\sigma_{\mathfrak{q}}$, $\sigma_{\mathfrak{q}^\varepsilon}$ are the Frobenius elements of $\mathfrak{q}$ and $\mathfrak{q}^\varepsilon$, respectively. Therefore,

$$\varphi_1(e(\mathfrak{q}^\varepsilon)) = \varphi_2(e(\mathfrak{q})) \quad \text{and} \quad \varphi_1(e(q)) = \varphi_1(e(\mathfrak{q})e(\mathfrak{q}^\varepsilon)) = \varphi_1(e(\mathfrak{q}))\varphi_2(e(\mathfrak{q})) \equiv q \bmod \mathfrak{P}.$$

Q.E.D.

Corollary (1.4) (cf. [11]). *Under the assumption* (C) *and the notation as above, if* $l \equiv 1 \bmod 4$, $p \neq l$.

Proof. Let ∞_1, ∞_2 be the infinite places of $k = \boldsymbol{Q}(\sqrt{l})$ and put $\varphi_{\infty_i} = \varphi_{1|k_{\infty_i}^\times}$. Here, we also denote by φ_i the corresponding Grössen-characters of k. Then, $1 = \varphi_1((-1)) = \varphi_{\infty_1}(-1)\varphi_{\infty_2}(-1)\cdot(-1)$ (cf. (1.3)). We may assume that $\varphi_{\infty_1}(-1) = -1$ and $\varphi_{\infty_2}(-1) = +1$. Let $u = (a + b\sqrt{l})/2$ be the fundamental unit of k such that $\varphi_{\infty_1}(u) = -1$ for some integers a and b. If $p = l$, the values of φ_1 on the principal ideal group of k are determined by φ_{∞_1} and a character mod $(\sqrt{l})$. Then,

$$\varphi_1((\alpha)) \equiv \varphi_{\infty_1}(\alpha)\alpha^m \bmod \overline{\mathfrak{P}}, \qquad \text{for } \alpha \in k^\times,\ (\alpha, l) = 1\,,$$

and a fixed integer m. But then, we have $1 \equiv \varphi_{\infty_1}(u)u^m \equiv -u^m$ and $1 \equiv \varphi_{\infty_1}(u^\varepsilon)(u^\varepsilon)^m \equiv (u^\varepsilon)^m \bmod \overline{\mathfrak{P}}$, so that $l \neq p$, where $1 \neq \varepsilon \in \mathrm{Gal}(k/\boldsymbol{Q})$. Q.E.D.

Let $\mathfrak{P} \mid p$ be a prime of $\mathcal{O} = \mathcal{O}_K$ satisfying the condition (C) and $\bar{\rho}$, $\overline{M} = M/\mathfrak{P}M$ and φ_i be as before. We also denote by φ_i the Grössen-character of k corresponding to φ_i and let $m_i \cdot n_i$, $(m_i, p) = 1$ and $n_i \mid p$, be the conductor of φ_i. The values of φ_i on the principal ideal group is determined by a character ψ_i of $(\mathcal{O}_k/m_i)^\times$, a character λ_i of $(\mathcal{O}_k/n_i)^\times$ (and

https://doi.org/10.1017/S0027763000020444 Published online by Cambridge University Press

a character of $k^{\times}_{\infty_i}$ ($i = 1, 2$) if $l \equiv 1 \bmod 4$). If $\left(\frac{\pm l}{p}\right) = -1$, put

$$(\lambda_1, \lambda_2) = (\chi_{p^2}^{a_1 + b_1 p}, \chi_{p^2}^{a_2 + b_2 p})$$

for some integers a_j and b_j, $0 \leqq a_j, b_j \leqq p - 1$. Here,

$$\chi_{p^r}\colon \mathrm{Gal}(\bar{\boldsymbol{Q}}_p/\boldsymbol{Q}_p^{un}) \longrightarrow \mu_{p^r-1}(\bar{\boldsymbol{Q}}_p) \xrightarrow{\sim} \boldsymbol{F}_{p^r}^{\times}$$

is the fundamental character (of degree $p^r - 1$ for $r \geqq 1$) (cf. [12]). If $\left(\frac{\pm l}{p}\right) = 1$, put $p\mathcal{O}_k = \mathfrak{p}\cdot\mathfrak{p}^{\varepsilon}$ and

$$(\lambda_{1|\mathcal{O}_\mathfrak{p}^\times}, \lambda_{2|\mathcal{O}_\mathfrak{p}^\times}) = (\chi_p^{c_1}, \chi_p^{c_2}),$$

$$(\lambda_{1|\mathcal{O}_{\mathfrak{p}^\varepsilon}^\times}, \lambda_{2|\mathcal{O}_{\mathfrak{p}^\varepsilon}^\times}) = (\chi_p^{d_1}, \chi_p^{d_2})$$

for some integers c_j and d_j, $0 \leqq c_j, d_j \leqq p - 1$, where $\mathcal{O}_\mathfrak{p} = (\mathcal{O}_k)_\mathfrak{p}$ and $\mathcal{O}_{\mathfrak{p}^\varepsilon} = (\mathcal{O}_k)_{\mathfrak{p}^\varepsilon}$.

LEMMA (1.5) (cf. [11]). *Under the notation as above, we have*

$$(a_1, a_2, b_1, b_2) = (1, 0, 0, 1) \quad \text{or} \quad (0, 1, 1, 0) \quad \text{if } \left(\frac{\pm l}{p}\right) = -1,$$

$$(c_1, c_2, d_1, d_2) = (1, 0, 0, 1) \quad \text{or} \quad (0, 1, 1, 0) \quad \text{if } \left(\frac{\pm l}{p}\right) = 1.$$

Proof. We can choose an abelian variety $J'(\ /\boldsymbol{Q})$ on which $\mathcal{O} = \mathcal{O}_K$ operates and which is isogenous to J over $\boldsymbol{Q}$. As $p \neq l$ (cf. (1.4)), the Néron model $J'_{/\mathcal{O}_k \otimes \boldsymbol{Z}_p}$ is an abelian scheme (cf. [3]) and ${}_{\mathfrak{P}}J'_{/\mathcal{O}_k \otimes \boldsymbol{Z}_p}$ is a finite flat group scheme. Let $\mathfrak{p}'$ be a prime of k lying over p and r be the degree of $\kappa(\mathfrak{P})/\boldsymbol{F}_p$, where $\kappa(\mathfrak{P}) = \mathcal{O}/\mathfrak{P}$. If $\bar{M} = {}_{\mathfrak{P}}J'(\bar{\boldsymbol{Q}})$ is a simple $\kappa(\mathfrak{P})[\bar{\rho}(G_k)]$-module, $\lambda_{i|\mathcal{O}_{\mathfrak{p}'}^\times}$ is a character induced from the Galois action on $({}_{\mathfrak{P}}J'_{/\mathcal{O}_\mathfrak{p}})(\bar{\boldsymbol{Q}}_p)$ and ${}_{\mathfrak{P}}J'_{/\mathcal{O}_{\mathfrak{p}'}}$ is a finite flat group scheme "en $\boldsymbol{F}_{p^{2r}}$-vectoriels" (cf. (1.2)). Then,

$$\lambda_{i|\mathcal{O}_{\mathfrak{p}'}^\times} = \chi_{p^{2r}}^{a_{i,1} + a_{i,2}\cdot p + \cdots + a_{i,2r}\cdot p^{2r-1}}$$

for $a_{i,j} = 0$ or 1 ($= \mathrm{ord}_{\mathfrak{p}'}\, p$) ($1 \leqq j \leqq 2r$) (cf. [12]). If $\bar{M}$ decomposes into a direct sum of two $\kappa(\mathfrak{P})[\bar{\rho}(G_k)]$-modules

$$\bar{M} = \bar{M}_1 \oplus \bar{M}_2,$$

then λ_i is the representation into Aut $\bar{M}_1$ or into Aut $\bar{M}_2$. We may assume that λ_i ($i = 1, 2$) corresponds to $\bar{M}_i$. Then, ${}_{\mathfrak{P}}J'_{/\mathcal{O}_{\mathfrak{p}'}}$ decomposes into a product of two finite flat group schemes "en $\boldsymbol{F}_{p^r}$-vectoriels", say X_1 and X_2,

$$J'_{/\mathcal{O}_{\mathfrak{p}'}} = X_1 \times_{\mathcal{O}_{\mathfrak{p}'}} X_2,$$

https://doi.org/10.1017/S0027763000020444 Published online by Cambridge University Press

where $X_i(\bar{Q}_p) = \bar{M}_i$ (cf. Lemma (1.1)), and

$$\lambda_{i|\mathcal{O}_{\mathfrak{p}'}^{\times}} = \chi_{p^r}^{b_{i,1}+b_{i,2}\cdot p+\cdots+b_{i,r}\cdot p^{r-1}}$$

for $b_{i,j} = 0$ or 1 $(1 \leqq j \leqq r)$. We must treat the following four cases. In the following discussion, note that $\mathrm{ord}_{\mathfrak{p}'}\, p = 1 < p-1$.

(1.5.1). The case when $\left(\frac{\pm l}{p}\right) = -1$.

(1.5.1.1). If $\bar{M}$ is irreducible,

$$\chi_{p^2}^{a_i+b_i\cdot p} = \chi_{p^{2r}}^{a_{i,1}+a_{i,2}\cdot p+\cdots+a_{i,2r}\cdot p^{2r-1}},$$

so that $a_{i,1} = a_{i,3} = \cdots = a_{i,2r-1}$ and $a_{i,2} = a_{i,4} = \cdots = a_{i,2r}$. Then, we may assume that a_i, $b_i = 0$ or 1.

(1.5.1.2). If $\bar{M}$ is decomposable,

$$\chi_{p^2}^{a_i+b_i\cdot p} = \chi_{p^r}^{b_{i,1}+b_{i,2}\cdot p+\cdots+b_{i,r}\cdot p^{r-1}},$$

so that $b_{i,1} = b_{i,2} = \cdots = b_{i,r}$ if r is odd and $b_{i,1} = b_{1,3} = \cdots = b_{i,r-1}$, $b_{i,2} = b_{i,4} = \cdots = b_{i,r}$ if r is even. Then, we may assume that a_i, $b_i = 0$ or 1.

(1.5.2). The case when $\left(\frac{\pm l}{p}\right) = 1$.

(1.5.2.1). If $\bar{M}$ is irreducible,

$$\chi_p^{c_i} = \chi_{p^{2r}}^{a_{i,1}+\cdots+a_{i,2r}\cdot p^{2r-1}}$$

so that $a_{i,1} = \cdots = a_{i,2r}$ and $c_i = 0$ or 1. By the same way, we get $d_i = 0$ or 1.

(1.5.2.2). If $\bar{M}$ is decomposable,

$$\chi_p^{c_i} = \chi_{p^r}^{b_{i,1}+\cdots+b_{i,r}\cdot p^{r-1}}$$

so that $b_{i,1} = \cdots = b_{i,r}$ and $c_i = 0$ or 1. By the same way, we get $d_i = 0$ or 1.

Therefore, we have a_i, b_i, c_i and $d_i = 0$ or 1 $(i = 1, 2)$. Using the relation that $\lambda_1 \otimes \lambda_2 = \chi_p$ and (1.3), we get the followings: If $\left(\frac{\pm l}{p}\right) = -1$, $\chi_{p^2}^{a_1+a_2+p(b_1+b_2)} = \chi_p$ and $m^{a_i+b_i} \equiv m \bmod p$ for all $m \in Z$, $(m, p) = 1$. Then, $(a_1, a_2, b_1, b_2) = (1, 0, 0, 1)$ or $(0, 1, 1, 0)$. If $\left(\frac{\pm l}{p}\right) = 1$, $\chi_p^{c_1+c_2} = \chi_p^{d_1+d_2} = \chi_p$ and $m^{c_i+d_i} \equiv m \bmod p$ for all $m \in Z$, $(m, p) = 1$. Then, $(c_1, c_2, d_1, d_2) = (1, 0, 0, 1)$ or $(0, 1, 1, 0)$. Q.E.D.

Under the notation as in Lemma (1.5), changing φ_1 by φ_ι, if necessary, we may assume that

$$(1.6)\qquad \begin{cases} (\lambda_1, \lambda_2) = (\chi_{p^2}, \chi_{p^2}^p) & \text{if } \left(\dfrac{\pm l}{p}\right) = -1\,. \\ \left.\begin{array}{l}(\lambda_{1|\mathcal{O}_{\mathfrak{p}}^\times}, \lambda_{2|\mathcal{O}_{\mathfrak{p}}^\times}) = (\chi_p, 1) \\ (\lambda_{1|\mathcal{O}_{\mathfrak{p}^\varepsilon}^\times}, \lambda_{2|\mathcal{O}_{\mathfrak{p}^\varepsilon}^\times}) = (1, \chi_p)\end{array}\right\} & \text{if } \left(\dfrac{\pm l}{p}\right) = 1\,. \end{cases}$$

Then, for all $\alpha \in k^\times$ such that $(\alpha, n_1 \cdot l) = 1$ $\left(n_1 = p \text{ if } \left(\dfrac{\pm l}{p}\right) = -1,\ n_1 = \mathfrak{p} \text{ if } \left(\dfrac{\pm l}{p}\right) = 1\right)$ and $\alpha \gg 0$ (totally positive, if $l \equiv 1 \bmod 4$),

$$(1.7)\qquad \varphi_1((\alpha)) \equiv \psi(\alpha)\alpha \mod \mathfrak{P}\,,$$

where ψ is a character of $(\mathcal{O}_k/m_1)^\times$ and $\mathfrak{P} \cap \mathcal{O}_k = p\mathcal{O}_k$ if $\left(\dfrac{\pm l}{p}\right) = -1$ and $= \mathfrak{p}\mathcal{O}_k$ if $\left(\dfrac{\pm l}{p}\right) = 1$. Let $\tilde{\psi}$ be the lifting of ψ to be a $\boldsymbol{C}^\times$-valued character

$$(1.8)\qquad \tilde{\psi}\colon (\mathcal{O}_k/m_1)^\times \xrightarrow{\ \psi\ } \bar{\boldsymbol{F}}_p^\times \hookrightarrow \bar{\boldsymbol{Q}}_p^\times \hookrightarrow \boldsymbol{C}^\times\,.$$

COROLLARY (1.9) (cf. [11]). *Assume that there is a prime* $\mathfrak{P}$ *of* $\mathcal{O} = \mathcal{O}_K$ *satisfying the condition* (C). *Then,* $n \geqq 2$ (*the level of the form* f *is* l^n), *and if* $l \equiv 1 \bmod 4$, $\left(\dfrac{l}{p}\right) = 1$.

Proof. Let ρ_p be the representation of the inertia group I_l of the prime l on the Tate module $T_p = T_p(J')(\bar{\boldsymbol{Q}}_l)$, then $\bar{\rho} \equiv \rho_p \bmod \mathfrak{P}$. If the level of the form f is the prime l, the Néron model $J'_{/\boldsymbol{Z}}$ is semi-stable (cf. [3]) and the characteristic roots of $\rho_p(x)$ are all 1 for all $x \in I_l$ (cf. e.g. [14], note. $p \neq l$ (1.4)). But in our case, the characteristic roots of $\bar{\rho}(x)$ are not 1 for some $x \in I_l$ (cf. (1.7)). When $l \equiv 1 \bmod 4$, let ∞_1, ∞_2 be the infinite places of $k = \boldsymbol{Q}(\sqrt{l})$ and put $\varphi_{\infty_i} = \varphi_{1|k_{\infty_i}^\times}$. Then,

$$\varphi_{\infty_1}(-1)\cdot\varphi_{\infty_2}(-1) = -1 \quad (\text{cf. } (1.7))\,.$$

We may assume that $\varphi_{\infty_1}(-1) = -1$ and $\varphi_{\infty_2}(-1) = 1$. Let $u = (a + b\sqrt{l})/2$ be the fundamental unit of k such that $\varphi_{\infty_1}(u) = -1$ for integers a, b. Then,

$$\varphi_1((\alpha)) \equiv \varphi_{\infty_1}(\alpha)\psi(\alpha)\alpha \mod \mathfrak{P}$$

for all $\alpha \in k^\times$, $(\alpha, p\cdot l) = 1$ (cf. (1.7)). Here, ψ is a character mod $(\sqrt{l})^r$ for an integer $r > 0$, satisfying the following condition: $\psi(m) \equiv \left(\dfrac{l}{m}\right) \bmod \mathfrak{P}$

for all $m \in \boldsymbol{Z}$ $(m, l) = 1$ (cf. (1.3)). As $\psi(u) = \psi(a/2)\psi(1 + (b/a)\sqrt{l})$, the order of $\psi(u)^2$ is l^s for an integer s, and $1 \equiv \psi(u)^2 u^2 \bmod \mathfrak{P}$. If $s = 0$, $u^2 \equiv 1 \bmod \mathfrak{P}$. If $s > 0$, l divides $p^2 - 1$. Therefore, $\left(\frac{l}{p}\right) = 1$. Q.E.D.

PROPOSITION (1.10). *Let l be a prime congruent to* -1 mod 4. *Assume that there exists a prime $\mathfrak{P}$ of $\mathcal{O} = \mathcal{O}_K$ satisfying the condition* (C). *Then, there exists a primitive cusp form Θ with C.M. (i.e., Θ is associated with a primitive Grössen-characrer of $k = \boldsymbol{Q}(\sqrt{-l})$ (cf.* [18])) *on $\Gamma_0(l^n)$ of weight* 2 *such that*

$$f \equiv \Theta \bmod \mathfrak{P}.$$

Proof. Under the notation in (1.7) and (1.8), the character φ_1 can be lifted to be a primitive Grössen-character $\tilde{\varphi}$ of k: Define $\tilde{\varphi}$ by

$$\tilde{\varphi}((\alpha)) = \tilde{\psi}(\alpha)\alpha$$

for all $\alpha \in k^\times$, $(\alpha, l) = 1$, which is well defined (, because $p \nmid 2 \cdot l$). Then, $\tilde{\varphi}$ is lifted to be a primitive Grössen-character such that $\tilde{\varphi}(\mathfrak{a}) \equiv \varphi_1(\mathfrak{a}) \bmod \overline{\mathfrak{P}}$ for all ideal $\mathfrak{a}$ of k, $(\mathfrak{a}, n_1 \cdot l) = 1$ (cf. (1.7)). Let

$$\Theta(z) = \textstyle\sum_{(\mathfrak{a}, l)=1} \tilde{\varphi}(\mathfrak{a}) \exp(2\pi\sqrt{-1} \cdot N(\mathfrak{a})z) = \sum_{m \geqq 1} b_m q^m$$

be the form associated with the primitive Grössen-character $\tilde{\varphi}$, where $N = N_{k/Q}$ and $q = \exp(2\pi\sqrt{-1} \cdot z)$. The form Θ is a new-form on $\Gamma_0(l^{n'})$ for $n' = 1 + \mathrm{ord}_{(\sqrt{-l})} m_1$ and $m_1 =$ the conductor of $\tilde{\psi}$ (cf. [20]). By the definition of Θ, we have the congruences: $a_q \equiv b_q$ for all primes $q \nmid l \cdot p$. As $n \geqq 2$ (cf. (1.4)) and $n' \geqq 2$, $a_l = b_l = 0$ (cf. [1]). If $\left(\frac{-l}{p}\right) = -1$, by our assumption, $a_p \equiv 0 \bmod \mathfrak{P}$, so that $a_p \equiv b_p$ $(=0) \bmod \mathfrak{P}$. If $\left(\frac{-l}{p}\right) = 1$, put $p\mathcal{O}_k = \mathfrak{p} \cdot \mathfrak{p}'$. By (1.6) above, $\overline{M}$ decomposes into a direct sum of two $\kappa(\mathfrak{P})[\bar{\rho}(\mathrm{Gal}(\bar{k}_\mathfrak{p}/k_\mathfrak{p}))]$-modules: $\overline{M} = M_1 \oplus M_2$ (, because, if not, $\lambda_2 = \lambda_1^{p^r}$, which contradicts to (1.6), where r is the degree of $\kappa(\mathfrak{P})/\boldsymbol{F}_p$). Therefore, $J'_{/\mathcal{O}_\mathfrak{p}}$ decomposes into a product of two finite flat group schemes "en $\boldsymbol{F}_{p^r}$-vectoriels" (cf. (1.1))

$$_{\mathfrak{P}}J'_{/\mathcal{O}_\mathfrak{p}} = X_1 \times_{\mathcal{O}_\mathfrak{p}} X_2,$$

one of them is étale and the other is multiplicative (cf. (1.6), [12]). By the congruence relation: $\pi_\mathfrak{p} + \pi_\mathfrak{p}^* = a_p$ (cf. [2], [21] chapter 7), a_p acts on $_{\mathfrak{P}}(J'/_{\mathcal{O}_\mathfrak{p}})(\bar{\kappa}(\mathfrak{p})) = X_2(\bar{\kappa}(\mathfrak{p}))$ as $\varphi_2(e(\mathfrak{p}))$, where $e(\mathfrak{p})$ is the idèle of k whose $\mathfrak{p}$-component is 1 and the other components are all p. Then,

$$a_p \equiv \varphi_1(e(\mathfrak{p}')) \bmod \overline{\mathfrak{P}} \tag{1.11}$$

(cf. [11], (1.3)). On the other hand, by the definition of $\tilde{\varphi}$, we know that $b_p = \tilde{\varphi}(\mathfrak{p}) + \tilde{\varphi}(\mathfrak{p}') \equiv \tilde{\varphi}(\mathfrak{p}') \equiv \varphi_1(e(\mathfrak{p}'))$ mod $\mathfrak{P}$. Therefore, we get the congruence: $f \equiv \Theta$ mod $\mathfrak{P}$. The rest of this proposition owes to the following sublemma.

For each $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \boldsymbol{Q})$, det $g > 0$, put

$$f|[g]_2 = (ad - bc)(cz + d)^{-2} f\left(\frac{az + b}{cz + d}\right).$$

SUBLEMMA (1.12). *Let f and g be primitive cusp forms on $\Gamma_0(l^n)$ and on $\Gamma_0(l^{n'})$ of weight 2, respectively. Let p be a prime number which does not divide $2 \cdot l$, and R be the ring of integers of $\bar{\boldsymbol{Q}}_p$ with the maximal ideal $\mathfrak{P}$. Regard K_f and K_g as subfields of $\bar{\boldsymbol{Q}}_p$. Assume that $f \equiv g$ mod $\mathfrak{P}$, then $n = n'$. Further, $f|[w]_2 = f$ (resp. $= -f$), then $g|[w]_2 = g$ (resp. $= -g$), where $w = \begin{pmatrix} 0 & -1 \\ l^n & 0 \end{pmatrix}$.*

Proof of Sublemma (1.12). We may assume that $n \geqq n'$. Put $h = f - g$, then $h = \alpha \cdot h_1$ for $\alpha \in \mathfrak{P}$ and a cusp form h_1 on $\Gamma_0(l^n)$ whose Fourier coefficients are integers of R. By the general theory (cf. [7] Corollary (1.6.2)), $h_1|[w]_2$ has the integral coefficients. As $h|[w]_2 = \pm f \pm l^{n-n'} \cdot g(q^{l^{n-n'}})$, $f \equiv \pm l^{n-n'} \cdot g(q^{l^{n-n'}})$ mod $\mathfrak{P}$. Comparing the first coefficients, we have $n = n'$. If f and g have the different eigen values of $[w]_2$, then $f - g \equiv f + g \equiv 0$ mod $\mathfrak{P}$, so that $f \equiv g \equiv 0$ mod $\mathfrak{P}$, which is a contradiction.

Q.E.D.

COROLLARY (1.13). *Assume that there exists a prime $\mathfrak{P}$ satisfying the condition* (C). *Then, $n = 2$ or $n \geqq 3$* odd.

Proof. Under the notation in (1.8), $\tilde{\psi}$ is a character of conductor $(\sqrt{\pm l})^r$ which satisfies the condition

$$\tilde{\psi}(m) = \left(\frac{\pm l}{m}\right)$$

for $m \in \boldsymbol{Z}$, $(m, l) = 1$. Then, $r = 1$ or $r \geqq 2$ even. If $l \equiv -1$ mod 4, by (1.11) above, $n = n' = 1 + r$. If $l \equiv 1$ mod 4, put $p\mathcal{O}_k = \mathfrak{p} \cdot \mathfrak{p}'$ and let $\tilde{\varphi}_1$ be the lifting of the character φ_1:

$$\tilde{\varphi}_1 \colon k_A^\times \xrightarrow{\varphi_1} \bar{\boldsymbol{F}}_p^\times \hookrightarrow \bar{\boldsymbol{Q}}_p^\times \hookrightarrow \boldsymbol{C}^\times .$$

Then, $g(z) = \sum_{(\mathfrak{a},p\cdot l)=1} \tilde{\varphi}_1(\mathfrak{a}) \exp(2\pi\sqrt{-1}\cdot N(\mathfrak{a})z)$ (cf. (1.6)) is a new form on $\Gamma_1(l^{n'}\cdot p)$ of weight 1 with the neben typus character χ such that $\chi(a) \equiv a \bmod \mathfrak{P}$ for all $a \in \boldsymbol{Z}$, $(a, p) = 1$, where $n' = 1 + r$. By the method of Koike [9] Ishii [5], we get a primitive cusp form $\tilde{f}$ on $\Gamma_0(l^{n'})$ of weight 2 such that

$$f \equiv g \equiv \tilde{f} \mod \mathfrak{P}.$$

(cf. (1.9), (1.11)). Then, by Sublemma (1.12), $n = n'$. Q.E.D.

Now consider the case when $n \geqq 3$. Following Ishikawa [6] and Saito [17], we can decompose the space $S_2^0(l^n)$ (= the $\boldsymbol{C}$-vector space spanned by the new-forms on $\Gamma_0(l^n)$ of weight 2). Denote by W the automorphism $\left[\begin{pmatrix} 0 & -1 \\ l^n & 0 \end{pmatrix}\right]_2$ of $S_2^0(l^n)$. For a primitive character $\chi \bmod l^\nu$, $0 \leqq \nu \leqq n/3$, let R_χ be the twisting operator (cf. [17], [21] Chapter 3)

$$R_\chi = \frac{1}{g(\bar{\chi})} \sum_{u \bmod l^\nu} \bar{\chi}(u) \left[\begin{pmatrix} 1 & u/l^\nu \\ 0 & 1 \end{pmatrix}\right]_2,$$

where $g(\bar{\chi})$ is the Gauss sum associated with $\bar{\chi} = \chi^{-1}$. Define the operator U_χ by

$$U_\chi = R_\chi \cdot W \cdot R_\chi \cdot W.$$

Then, any primitive cusp form belonging to $S_2^0(l^n)$ is an eigen form of U_χ (cf. [17] § 1). Let ε be the character $\left(\frac{\pm l}{\quad}\right)$, $\pm l \equiv 1 \bmod 4$, and define the subspaces S_{I}, S_{II}, $S_{\mathrm{II}_\varepsilon}$ and S_{III} of $S_2^0(l^n)$ by

$$\text{(1.14)} \qquad \begin{aligned} S_{\mathrm{I}} &= \{f \in S_2^0(l^n) \mid f|W = f,\ f|U_\varepsilon = f\} \\ S_{\mathrm{II}} &= \{f \in S_2^0(l^n) \mid f|W = f,\ f|U_\varepsilon = -f\} \\ S_{\mathrm{II}_\varepsilon} &= \{f \in S_2^0(l^n) \mid f|W = -f,\ f|U_\varepsilon = -f\} \\ S_{\mathrm{III}} &= \{f \in S_2^0(l^n) \mid f|W = -f,\ f|U_\varepsilon = f\}. \end{aligned}$$

Then $S_2^0(l^n)$ decomposes into a direct sum

$$S_2^0(l^n) = S_{\mathrm{I}} \oplus S_{\mathrm{II}} \oplus S_{\mathrm{II}_\varepsilon} \oplus S_{\mathrm{III}},$$

which is compatible with the action of the Hecke algebra $\boldsymbol{T} = \boldsymbol{Z}[T_q]_{q \neq l}$, where T_q is the Hecke operator for each prime q (cf. [17] § 1). Further, these spaces S_{I} and S_{III} have the finer decompositions. Put $\mu = [n/3]$ ($\geqq 1$) and $X(l^n)$ be the group of the characters whose conductors divide p^μ. Define the subspaces $S_2(l^n, a, \pm 1)$ of $S_2^0(l^n)$ by

$$S_2(l^n, a, 1) = \{f \in S_2^0(l^n) \mid f \mid W = f,\ f \mid U_\chi = \chi(a) f \text{ for all } \chi \in X(l^n)\}$$
$$S_2(l^n, a, -1) = \{f \in S_2^0(l^n) \mid f \mid W = -f,\ f \mid U_\chi = \chi(a) f \text{ for all } \chi \in X(l^n)\},$$

which are the T-modules (cf. [17] § 3). Then,

$$(1.15)\qquad \begin{aligned} S_{\mathrm{I}} &= \bigoplus_{\substack{a \bmod p \\ \varepsilon(a)=1}} S_2(l^n, a, 1) \\ S_{\mathrm{III}} &= \bigoplus_{\substack{a \bmod p \\ \varepsilon(a)=1}} S_2(l^n, a, -1). \end{aligned}$$

LEMMA (1.16). *Under the notation and the assumption as above. Let f and g be primitive cusp forms belonging to $S_2^0(l^n)$, R be the ring of integers of $\bar{\boldsymbol{Q}}_p$ with the maximal ideal $\mathfrak{P}$. Suppose that $f \equiv g \bmod \mathfrak{P}$ and p does not divide $l \cdot (l-1)$. Then, f and g belong to the same subspace in the decomposition of* (1.14). *If f and g belong to S_{I} or S_{III}, f and g belong to the same subspace in the decomposition of* (1.15).

Proof. Let h be a cusp form on $\Gamma_1(l^n)$ of weight 2. If the Fourier coefficients are integers of R, then $h \mid W$ and $h \left| \left[\begin{pmatrix} 1 & u/l^\nu \\ 0 & 1 \end{pmatrix}\right]_2\right.$ have also the integral coefficients for integers μ and ν, $0 \leqq \nu \leqq \mu$ (cf. [7] Corollary (1.6.2)). Therefore, we have

$$f \mid U_\chi \equiv g \mid U_\chi \mod \mathfrak{P},$$

for all $\chi \in X(l^n)$, so that f and g belong to the same direct factor in (1.14) (cf. (1.13)). If $f \mid U_\chi = \chi(a) f$ and $g \mid U_\chi = \chi(b) g$ for some $a, b \in (\boldsymbol{Z}/l^\mu \boldsymbol{Z})^\times$ and for all $\chi \in X(l^n)$, then $\chi(a \cdot b^{-1}) \equiv 1 \bmod \mathfrak{P}$ for all $\chi \in X(l^n)$. By our assumption $p \nmid (l-1) \cdot l$, the congruences above lead the rest of this Lemma (1.16). Q.E.D.

In the rest of this section, we consider the Galois action on ${}_{\mathfrak{P}}J'(\bar{\boldsymbol{Q}})$, for the prime $\mathfrak{P}$ dividing (l, δ). Let $l = p$ be a prime number congruent to $-1 \bmod 4$ and $f = \sum a_m q^m$ be a primitive cusp form on $\Gamma_0(l^n)$ of weight 2 ($n \geqq 2$). We assume that f does not have C.M. and has a twist $\left(\sigma, \left(\frac{-p}{\ }\right)\right)$ (cf. [10], [15]). Then, the endomorphism algebra End $J_f \otimes \boldsymbol{Q}$ is isomorphic to $K \oplus K\eta$, where η is the twisting operator defined over $k = \boldsymbol{Q}(\sqrt{-p})$ and $\eta^\varepsilon = -\eta$ for $1 \neq \varepsilon \in \mathrm{Gal}(k/\boldsymbol{Q})$ (cf. [19]). The algebraic structure of $D = K \oplus K\eta$ is defined by

$$\eta^2 = -p$$
$$\eta \cdot a_q = \left(\frac{-p}{q}\right) a_q \cdot \eta,$$

https://doi.org/10.1017/S0027763000020444 Published online by Cambridge University Press

for all primes $q \neq p$. Let $d = d_f$ be the discriminant of D, and $\delta = \delta_f$ be the ideal of $\mathcal{O} = \mathcal{O}_{K_f}$ defined before (cf. (C)). Let ρ_l be the l-adic representation on the Tate module $T_l(J')(\bar{\boldsymbol{Q}})$ and put $a(q, r) = \rho_l(\sigma_q^r) + q^r\rho_l(\sigma_q^{-r})$, for each prime $q \neq l = p$, where σ_q is a Frobenius element of q. Then, $a(q, 1) = a_q$ and $a(q, r) \in K$.

LEMMA (1.17). *Let $\mathfrak{p}$ be a prime of $F = F_f$ dividing (p, d) and $\mathfrak{P}$ be the prime of $K = K_f$ lying over $\mathfrak{p}$. Then we have the following congruences*

$$a(q, h) \equiv q^{(p-1+2h)/4} + q^{(1-p+2h)/4} \mod \mathfrak{P}$$

for all primes $q \neq p$, where $h = h(-p)$ is the class number of $k = \boldsymbol{Q}(\sqrt{-p})$. Further $\mathfrak{p}$ divides δ.

Proof. Let ρ be the representation of $G = \mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$ on $V_{\mathfrak{P}} = V_p \otimes K_{\mathfrak{P}}$

$$\rho\colon G \longrightarrow \mathrm{Aut}_{K_{\mathfrak{P}}} V_{\mathfrak{P}} = GL(2, K_{\mathfrak{P}}) .$$

By our assumption, the prime ideal $\mathfrak{p}$ remains a prime or is ramified in K. There is an element $a \in F_{\mathfrak{p}}\cdot\eta$ such that $a^2 \in \mathcal{O}_{\mathfrak{p}}$, $\mathrm{ord}_{\mathfrak{p}}\, a^2 = 0$ or 1 and $a^{\varepsilon} = -a$ for $1 \neq \varepsilon \in \mathrm{Gal}(k/\boldsymbol{Q})$. There is an element $b \in K_{\mathfrak{P}}^{\times}$ such that $b^2 \in \mathcal{O}_{\mathfrak{p}}$, $\mathrm{ord}_{\mathfrak{p}}\, b^2 = 0$ or 1 and $a \cdot b = -b \cdot a$. First assume that $\mathrm{ord}_{\mathfrak{P}}\, \delta$ is even, then $\mathrm{ord}_{\mathfrak{p}}\, b^2 = 0$, so that $\mathrm{ord}_{\mathfrak{p}}\, a^2 = 1$ and $\mathfrak{P} = \mathfrak{p}\mathcal{O}_K$. As $\mathcal{O}_{\mathfrak{P}} + \mathcal{O}_{\mathfrak{P}}a$ is a ring, we can choose a lattice M of $V_{\mathfrak{P}}$ on which $\mathcal{O}_{\mathfrak{P}}[a]$ and G operate. Put $\bar{M} = M/\mathfrak{P}M$, and let $\bar{\rho}$ be the representation of G induced from ρ by the reduction mod $\mathfrak{P}$

$$\bar{\rho}\colon G \longrightarrow \mathrm{Aut}_{\kappa(\mathfrak{P})}\bar{M} \xrightarrow{\ \sim\ } GL(2, \kappa(\mathfrak{P})) .$$

where $\kappa(\mathfrak{P}) = \mathcal{O}/\mathfrak{P}$. Then, $a\cdot\bar{M}$ is a 1-dimensional vector subspace of $\bar{M}$ (as $\kappa(\mathfrak{P})$-vector spaces), and is G-invariant, because $\mathrm{ord}_{\mathfrak{p}}\, a^2 = 1$ and $\rho(g)\cdot a = \chi_p^{\otimes(p-1)/2}(g)a\cdot\rho(g)$ for all $g \in G$. Choose an element $m_1 \in \bar{M}$ such that $a\cdot m_1 \neq 0$, and put $m_2 = a\cdot m_1$. Then $\{m_1, m_2\}$ is a basis of $\bar{M}$ as a $\kappa(\mathfrak{P})$-vector space and a operates on $\bar{M}$ as follows: $xm_1 + ym_2 \mapsto x^{\sigma}m_2$ for $x, y \in \kappa(\mathfrak{P})$. Let λ be the representation of G on $\bar{M}/a\cdot\bar{M}$

$$\lambda\colon G \longrightarrow \mathrm{Aut}_{\kappa(\mathfrak{P})}\bar{M}/a\cdot\bar{M} \xrightarrow{\ \sim\ } \kappa(\mathfrak{P})^{\times} ,$$

then G operates on $a\cdot\bar{M}$ by the character $\chi_p^{\otimes(p-1)/2} \otimes \lambda^{\sigma}$, where λ^{σ} is a character defined by $\lambda^{\sigma}(g) = \lambda(g)^{\sigma}$ for all $g \in G$. But λ is unramified outside of p, so that λ is a character mod $\sqrt{-p}$ valued in $\boldsymbol{F}_p^{\times}(\hookrightarrow \kappa(\mathfrak{P})^{\times})$, hence $\lambda^{\sigma} = \lambda$. Further, by the relation $\chi_p = \det\cdot\bar{\rho} = \lambda^{\otimes 2} \otimes \chi_p^{\otimes(p-1)/2}$, we have

$\lambda^{\otimes 2} = \chi_p^{\otimes (p+1)/2}$ and

$$a(q, 1) \equiv q^{(p+1)/4} + q^{(3-p)/4} \mod \mathfrak{P}$$

for all primes $q \neq p$. Since h is odd, we get congruences to be proved. Now consider the case when $\mathrm{ord}_{\mathfrak{P}}\, \delta$ is odd, so $\mathrm{ord}_{\mathfrak{p}}\, b^2 = 1$. Put $\mathcal{O}^* = \mathcal{O}_{\mathfrak{p}}[a]$ if $\mathrm{ord}_{\mathfrak{p}}\, a^2 = 0$ and $\mathcal{O}^* = \mathcal{O}_{\mathfrak{p}}[a \cdot b/a^2]$ if $\mathrm{ord}_{\mathfrak{p}}\, a^2 = 1$, and put $\mathfrak{P}^* = \mathfrak{p}\mathcal{O}^*$. Then $\mathcal{O}^* + \mathcal{O}^* b$ is a ring and $\mathfrak{P}^*$ is a prime ideal, because $\mathfrak{p} | d$ and $\mathfrak{p} \nmid 2$. Choose a lattice M of $V_{\mathfrak{P}}$ on which $\mathcal{O}^*[b]$ and G operate, then $b \cdot M$ is a $\mathcal{O}^*[b]$-submodule of M and which is G-invariant. Put $\overline{M} = M/\mathrm{b} \cdot M$, which is a 1-dimensional vector space over $\kappa(\mathfrak{P}^*) = \mathcal{O}^*_{/\mathfrak{P}^*}$. Consider the representation $\bar{\rho}$ of G on $\overline{M}$ induced from ρ

$$\bar{\rho}\colon G \longrightarrow \mathrm{Aut}_{\kappa(\mathfrak{p})} \overline{M} \xrightarrow{\ \sim\ } GL(2, \kappa(\mathfrak{p}))\,.$$

Then $\bar{\rho}(G_k)$ is contained in the non-split Cartan subgroup $\simeq \kappa(\mathfrak{P}^*)^{\times}$, so that $\bar{\rho}(G)$ is contained in the normalizer of the non-split Cartan subgroup. The automorphism of $\kappa(\mathfrak{P}^*)$: $x \mapsto \rho(g) x \rho(g)^{-1}$ is non-trivial for $g \in G - G_k$, because $\rho(g) a \rho(g)^{-1} = \chi_p^{\otimes (p-1)/2}(g) a$ for all $g \in G$. Therefore, $\bar{\rho}(G)$ is not contained in this Cartan subgroup. Let λ be the character of G_k corresponding to $\bar{\rho} | G_k$

$$\lambda\colon G_k \longrightarrow \mathrm{Aut}_{\kappa(\mathfrak{P}^*)} \overline{M} \xrightarrow{\ \sim\ } \kappa(\mathfrak{P}^*)^{\times} \hookrightarrow \bar{F}_p^{\times}\,,$$

then $\bar{\rho} \simeq \mathrm{Ind}\,{}^{G}_{G_k}\, \lambda$, where $\mathrm{Ind}\,{}^{G}_{G_k}$ is the induced representation. As λ is unramified outside of p, so that $\lambda^{\otimes h}$ is a character of the conductor $(\sqrt{-p})$ valued in $F_p^{\times}$. Then, $\mathrm{Ind}\,{}^{G}_{G_k}\, \lambda^{\otimes h}$ is an abelian representation, which is equivalent to $\mu \oplus \mu \otimes \chi_p^{\otimes (p-1)/2}$ for a character μ of G. For a prime q splitting in k, put $q\mathcal{O}_k = \mathfrak{q} \cdot \mathfrak{q}^{\epsilon}$, then $\lambda(\sigma_{\mathfrak{q}})\lambda(\sigma_{\mathfrak{q}^{\epsilon}}) \equiv q$ and $\lambda^{\otimes h}(\sigma_{\mathfrak{q}}) = \lambda^{\otimes h}(\sigma_{\mathfrak{q}^{\epsilon}}) = \mu(\sigma_q)$, so that $\mu(\sigma_q) \equiv q^{((p-1)m+2h)/4}$ for an odd integer m. Therefore,

$$a(q, h) \equiv q^{(p-1+2h)/4} + q^{(1-p+2h)/4} \mod \mathfrak{P}$$

for all primes $q \neq p$. Q.E.D.

§ 2. Discriminant of End $J_f \otimes Q$

Let l be a prime number congruent to -1 mod 4, $n \geqq 2$ be an integer, and f, $J = J_f$, $K = K_f$, $F = F_f$ and $\delta = \delta_f$ be as in Section 1. Assume that f has a twist $\left(*, \left(\frac{-l}{\ }\right)\right)$ (cf. [10], [15]) but does not have

C.M. Let d be the discriminant of $D = K + K\eta \simeq \mathrm{End}\, J \otimes \boldsymbol{Q}$, d_0 be the product of primes $\mathfrak{p}$ of F such that $\mathrm{ord}_{\mathfrak{P}}\, \delta$ is odd, $\mathfrak{p} \nmid l$ and $\left(\frac{-l}{N(\mathfrak{p})}\right) = -1$, where $N = N_{F\mathfrak{p}/Q_p}$ for $\mathfrak{p} | p$. Further, let d_1 be the product of the primes of F dividing (l, δ).

LEMMA (2.1). *Under the notation and assumption as above, we have* (i) $d_0 | d$ *and* (ii) $d | d_0 \cdot d_1$.

Proof. There is $\alpha \in K^\times$ such that $\alpha^2 \in \mathcal{O}_F$ and $\alpha \cdot \eta = -\eta \cdot \alpha$ (then, $D = F + F\alpha + F\eta + F\alpha \cdot \eta$). If $\mathfrak{p} | (l, d)$, by Lemma (1.17), $\mathfrak{p} | \delta$. When $\mathfrak{p} | l$, the prime $\mathfrak{p}$ is unramified in $F[\eta]$, so that $(\alpha^2, -l)_{\mathfrak{p}} = -1$ if and only if $\mathrm{ord}_{\mathfrak{p}}\, \alpha^2$ is odd and $\left(\frac{-l}{N(\mathfrak{p})}\right) = -1$. Q.E.D.

Using the results in Section 1 and Lemma (2.1) above, we can determine the discriminants of the algebras of the examples in [17]. Let $f = \sum a_m q^m$ be a primitive cusp form on $\Gamma_0(l^n)$, $n \geqq 3$, then K_f contains $\alpha_l = \exp(2\pi\sqrt{-1}/l) + \exp(-2\pi\sqrt{-1}/l)$ (cf. [17] Corollary (3.4)). First discuss the case for $l = 11$. From the table in [17],

$$S_2(11^3, 4, +1) = \boldsymbol{C}\Theta_{\mathrm{I}} \oplus S_{\mathrm{I}}^0$$
$$S_2(11^3, 4, -1) = \boldsymbol{C}\Theta_{\mathrm{III}} \oplus S_{\mathrm{III}}^0$$

where Θ_{I} and Θ_{III} are the forms associated with some primitive Grössen-characters of $\boldsymbol{Q}(\sqrt{-11})$ with conductor (11), and S_{I}^0 and S_{III}^0 are the orthogonal complements of $\boldsymbol{C}\Theta_{\mathrm{I}}$ and $\boldsymbol{C}\Theta_{\mathrm{III}}$, respectively. The space S_{I}^0, whose dimension is 2, is spanned by a primitive cusp form $f = \sum a_m q^m$ and its conjugate $\sigma f = \sum a_m^\sigma q^m$, for an isomorphism σ of K_f into $\boldsymbol{C}$, and $N_{K_f/Q}(a_2) = -199$. By Lemma (2.1), End $J_f \otimes \boldsymbol{Q}$ is a matrix algebra. Denote by g_{T_q} the characteristic polynomial of the Hecke operator T_q on S_{III}^0, then

$$N_{Q(\alpha_{11})/Q}(g_{T_2}(0)) = -2^5 \cdot 99527\,,$$

and dim $S_{\mathrm{III}}^0 = 2 \cdot 3$. As $\left(\frac{-11}{2}\right) = \left(\frac{-11}{99527}\right) = -1$ and the degree of the ideal (2) in $\boldsymbol{Q}(\alpha_{11})$ is 5, so that by Lemma (2.1), there is a primitive cusp form $g = \sum b_m q^m \in S_{\mathrm{III}}^0$ such that $N_{F_g/Q}(d_g) = 2^5 \cdot 99527$ (unique up to conjugation). Therefore, we get the following.

PROPOSITION (2.2). *Under the notation as above,*

$$d_f = (1), \quad d_g = \mathfrak{p}_2 \cdot \mathfrak{p}_{99527}\,,$$

https://doi.org/10.1017/S0027763000020444 Published online by Cambridge University Press

where $\mathfrak{p}_q = (q, b_2)$ *for the primes* q.

Next consider the case for $l = 19$.

$$S_2(19^3,\ 4,\ +1) = C\Theta_{\mathrm{I}} \oplus S_{\mathrm{I}}^0$$
$$S_2(19^3,\ 4,\ -1) = C\Theta_{\mathrm{III}} \oplus S_{\mathrm{III}}^0\,,$$

where Θ_{I} and Θ_{III} are the forms associated with some primitive Grössen-characters of $\boldsymbol{Q}(\sqrt{-19})$ with conductor (19), and S_{I}^0 and S_{III}^0 are the orthogonal complements of $C\Theta_{\mathrm{I}}$ and $C\Theta_{\mathrm{III}}$, respectively. Denote by f_{T_q} (resp. g_{T_q}) the characteristic polynomial of the Hecke operator T_q on S_{I}^0 (resp. S_{III}^0). From the table in [17], we know that

$$N_{\boldsymbol{Q}(\alpha_{19})/\boldsymbol{Q}}(f_{T_2}(0)) = -37^2\cdot 56536856647$$
$$N_{\boldsymbol{Q}(\alpha_{19})/\boldsymbol{Q}}(g_{T_2}(0)) = -2^9\cdot 19^2\cdot 5736557\cdot 6463381\,,$$

and $\dim S_{\mathrm{I}}^0 = 2\cdot 6$, $\dim S_{\mathrm{III}}^0 = 2\cdot 8$. Let $f = \sum a_m q^m$ be a primitive cusp form belonging to S_{I}^0. If $d_f \neq (1)$, by Lemma (2.1), $\sqrt{37\mathcal{O}_{F_f}} = \mathfrak{P}_1\cdot\mathfrak{P}_2$, $\mathfrak{P}_1 \neq \mathfrak{P}_2$, where $\sqrt{}$ is the radical of the ideal

$$\left(\text{, because, } \left(\frac{-19}{56536856647}\right) = +1\right).$$

Then, by virtue of Proposition (1.2) and Lemma (1.15), we should have the following congruences

$$\Theta_{\mathrm{I}} \equiv f \mod \overline{\mathfrak{P}}_i\,,$$

where $\overline{\mathfrak{P}}_i$ $(i = 1, 2)$ are the primes of $\mathcal{O}_{K_f}$ lying over $\mathfrak{P}_i$. Let λ be the Grössen-character corresponding to Θ_{I}, then

$$a_5 \equiv \lambda\left(\left(\frac{1+\sqrt{-19}}{2}\right)\right) + \lambda\left(\left(\frac{1-\sqrt{-19}}{2}\right)\right) \mod \overline{\mathfrak{P}}_i$$

for $i = 1, 2$, so that 37^2 must divides

$$N_{F_f/\boldsymbol{Q}}\left(a_5 - \lambda\left(\left(\frac{1+\sqrt{-19}}{2}\right)\right) - \lambda\left(\left(\frac{1-\sqrt{-19}}{2}\right)\right)\right).$$

But we know that

$$\left|N_{F_f/\boldsymbol{Q}}\left(a_5 - \lambda\left(\left(\frac{1+\sqrt{-19}}{2}\right)\right) - \lambda\left(\left(\frac{1-\sqrt{-19}}{2}\right)\right)\right)\right| = 37\cdot 227\cdot 150707\cdot 56536856647$$

(cf. [17] § 4). Hence, $d_f = (1)$. Next consider the forms belonging to S_{III}^0.

https://doi.org/10.1017/S0027763000020444 Published online by Cambridge University Press

The degree of the ideal (2) in $\boldsymbol{Q}(\alpha_{19})$ is 9, and

$$\left(\frac{-19}{2}\right)=\left(\frac{-19}{6463381}\right)=-1 \quad \text{and} \quad \left(\frac{-19}{5736557}\right)=+1.$$

Therefore, by Lemma (2.1), there is a primitive cusp form $g=\sum b_m q^m \in S^0_{\mathrm{III}}$ such that $d_g \neq (1)$. To determine the discriminant d_g, we must consider the primes $\mathfrak{p}|19$. If a prime $\mathfrak{p}$ of F_g divides $(d_g, 19)$, we should have the following congruence

$$b_5 \equiv 5^5+5^{14} \mod \mathfrak{p}$$

(cf. Lemma (1.17)). But, we know by a calculation that

$$19 \nmid N_{Q(\alpha_{19})/Q}(g_{T_5}(5^5+5^{14})),$$

hence $N_{F_g/Q}(d_g)=2^9\cdot 6463381$ (and g is unique up to conjugation). Therefore, we get the following.

PROPOSITION (2.3). *Under the notation as above,*

$$d_f=(1), \quad d_g=\mathfrak{p}_2\cdot\mathfrak{p}_{6463381},$$

where $\mathfrak{p}_q=(q, b_2)$ *for the primes* q.

REFERENCES

[1] A. O. L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann., **185** (1970), 134–160.

[2] P. Deligne, Formes modulaires et représentations l-adiques, sém. Bourbaki, 1968/1969, exposé n° 355, Lecture Notes in Math., **179**, 139–172. Berlin-Heidelberg-New York: Springer 1971.

[3] P. Deligne and M. Rapoport, Schémas de modules des courbes elliptiques, vol. II of the Proceedings of the International Summer School on Modular Functions, Antwerp (1972). Lecture Notes in Math., **349**, Berlin-Heidelberg-New York: Springer 1973.

[4] K. Doi and M. Yamauchi, On the Hecke operators for $\Gamma_0(N)$ and class fields over quadratic number fields, J. Math. Soc. Japan, **25** (1973), 629–643.

[5] H. Ishii, Congruences between cusp forms and the fundamental units of real quadratic number fields, to appear.

[6] H. Ishikawa, Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$, J. Fac. Sci. Univ. Tokyo, **21** (1974), 357–376.

[7] N. Katz, p-adic properties of modular schemes and modular forms, vol. III of Proceedings of the International Summer School on Modular Functions, Antwerp (1972), Lecture Notes in Math., **350**, Berlin-Heidelberg-New York, 69–190 (1973).

[8] M. Koike, On certain abelian varieties obtained from new forms of weight 2 on $\Gamma_0(3^4)$ and $\Gamma_0(3^5)$, Nagoya Math. J., **62** (1976), 29–39.

[9] ——, Congruences between cusp forms and linear representations of Galois group, Nagoya Math. J., **64** (1976), 63–85.

[10] F. Momose, On the l-adic representations attached to modular forms, J. Fac. Sci. Univ. Tokyo, **28** (1981), 89–109.
[11] M. Ohta, The representation of Galois group attached to certain finite group schemes, and its application to Shimura's theory, Algebraic Number Theory, Papers contributed for the International Symposium, Kyoto 1976, Japan Society for the Promotion for Science.
[12] M. Raynaud, Schémas en groupes de type $(p, \cdots, p)$, Bull. Soc. Math. France, **102** (1974), 241–280.
[13] K. A. Ribet, Endomorphisms of semi-stable abelian varieties over number fields, Ann. of Math., **101** (1975), 555–562.
[14] ——, On l-adic representations attached to modular forms, Invent. Math., **28** (1975), 245–275.
[15] ——, Twists of modular forms and endomorphisms of abelian varieties, Math. Ann., (1980), 239–244.
[16] ——, Endomorphism algebras of abelian varieties attached to newforms of weight 2, Séminaire D.P.P., 1979–80.
[17] H. Saito, On a decomposition of spaces of cusp forms and trace formula of Hecke operators, Nagoya Math. J., **80** (1980), 129–165.
[18] G. Shimura, On elliptic curves with complex multiplication as factors of the jacobians of modular function fields, Nagoya Math. J., **43** (1971), 199–208.
[19] ——, On the factors of jacobian variety of a modular function field, J. Math. Soc. Japan, **25** (1973), 523–544.
[20] ——, Class fields over real quadratic fields and Hecke operators, Ann. of Math., **95** (1972), 130–190.
[21] ——, Introduction to the Arithmetic Theory of Automorphic Functions, Pub. Math. Soc. Japan, No. 11, Tokyo-Princeton, 1971.

Department of Mathematics
Faculty of Science
University of Tokyo
Hongo, Tokyo 113
Japan