J. Math. Soc. Japan
Vol. 34, No. 3, 1982

Good reduction of elliptic modules

By Toyofumi TAKAHASHI

(Received Jan. 6, 1981)

In this paper we give a criterion for good reduction of elliptic modules (Theorem 1, Section 2) which is an analogue of the criterion of Néron-Ogg-Šafarevič for abelian varieties, cf. [7]. In the rest of the paper we give applications to elliptic modules of rank one over global function fields: In Section 3, the main theorem of complex multiplication of elliptic modules ([3] and [5]) is reformulated in a more relevant form to our subject (Theorem 2). Then, to each elliptic module we can associate the "Hecke character" (Theorem 3) so that the elliptic module has good reduction at a place v if and only if the Hecke character is unramified at v. In Section 4, we give a classification theorem (Theorem 4) by means of the Hecke characters. As an application, it will be shown that each rank-one elliptic module over a global function field K has a K-form which has good reduction everywhere (Theorem 5).

1. Elliptic modules.

In this section we recall briefly the basic concepts of elliptic modules. For details, see [3] and [5].

Let F be a global field of characteristic $p>0$, $\mathbf{F}_q$ the finite field of constants, ∞ a fixed prime divisor and A the ring of elements of F which are integral outside ∞. For a commutative ring K of characteristic p we let denote $K\{\phi\}$ the (non commutative) ring of polynomials in ϕ over K with the relation $\phi c = c^q\phi$ for $c \in K$. When K is an A-algebra, i.e., there is defined $i: A \to K$, the ideal $\mathrm{Ker}\, i$ of A is called the *divisorial characteristic* of K (notation: $\mathrm{div\,char}\, K$). An *elliptic A-module X over* an algebra K is a ring homomorphism $f: A \to K\{\phi\}$ satisfying the following three conditions:

(a) $D \circ f = i$, where $D: K\{\phi\} \to K$ is a homomorphism defined by $D(\sum c_j\phi^j) = c_0$.

(b) The leading coefficient of $f(a)$ is invertible in K for each nonzero element a of A.

(c) The image $f(A)$ is not contained in K.

We write $[a]_X$, or simply a_X, for the image $f(a)$ of $a \in A$ under f. If $a_X =$

This research was partially supported by Grant-in-Aid for Scientific Research (No. 554020), Ministry of Education.

$\sum c_j\phi^j$, then $a_X(T)=\sum c_jT^{q^j}$ is an $\mathbf{F}_q$-linear polynomial. When K is a field, we put

$$X_{\mathfrak{a}}=\{t\in K_s \mid a\cdot t(=a_X(t))=0 \quad \text{for all} \quad a\in\mathfrak{a}\}$$

for an ideal $\mathfrak{a}$ of A, where K_s is the separable closure of K. Hence $X_{\mathfrak{a}}$ is the A-module of $\mathfrak{a}$-division points of X. If $\mathfrak{a}$ is prime to div char K, the module $X_{\mathfrak{a}}$ is a free $(A/\mathfrak{a})$-module of finite rank r. The rank r is independent of $\mathfrak{a}$ and called the *rank* of X.

PROPOSITION 1 ([3]). $\deg a_X(T)=|a|_\infty^r$ *for* $a\in A$.

Let X and Y be two elliptic A-modules over K. A *homomorphism* (over K) from X to Y is an element $\alpha\in K\{\phi\}$ such that $\alpha a_X=a_Y\alpha$ for all $a\in A$. Hence an *isomorphism* $u: X \xrightarrow{\sim} Y$ is an invertible element u of K such that $a_Y=u a_X u^{-1}$. In this case we write $Y=u(X)$. A non zero homomorphism is called an *isogeny*.

2. Good reduction of elliptic modules.

Let K be a field, v an (additive) discrete valuation of K and O_v the valuation ring of v with a ring homomorphism i of A into O_v, that is, O_v is an A-algebra. We denote the residue field $O_v/\mathfrak{m}_v$ by $k(v)$ and the residue divisorial characteristic by $\mathfrak{p}_v$.

Let X be an elliptic A-module over K. We say that X has *integral coefficients at* v if $a_X\in O_v\{\phi\}$ for all $a\in A$ and the homomorphism $a\mapsto(a_X \bmod \mathfrak{m}_v)$ defines an elliptic A-module over $k(v)$ (the *reduction of* X *at* v, notation: $X(v)$). We say that X has *stable reduction at* v if there exists an elliptic A-module $Y\cong X$ which has integral coefficients at v, and that X has *good reduction at* v if in addition Y is an elliptic A-module over O_v. We say that X has *potential stable* (resp. *good*) *reduction at* v if there exists a finite extension (L, w) of (K, v) such that X has stable (resp. good) reduction at w.

We set

$$v(\sum c_i\phi^i)=\mathrm{Min}\left\{\frac{1}{q^i-1}v(c_i)\,\middle|\, i>0\right\}$$

for $\sum c_i\phi^i\in K\{\phi\}$. For an element u of $K^\times$, we see that the elliptic module $u(X)$ has integral coefficients at v if and only if

$$(1) \qquad v(u)=\mathrm{Min}\{v(a_X) \mid \text{nonconstant } a\in A\}\,.$$

Since A is a ring finitely generated over $\mathbf{F}_q$, the right-hand side of (1) exists always (in $\boldsymbol{Q}$). Hence:

PROPOSITION 2 ([3]). *Every elliptic A-module has potential stable reduction. More precisely, for each elliptic module X over K, there is a natural number* $e_v(X)$ *prime to* p *so that the following two properties are equivalent for a finite extension* w *of* v;

(a) *X has stable reduction at w.*

(b) *The index of ramification of w over v is divisible by $e_v(X)$.*

COROLLARY. *Every elliptic A-module of rank one has potential good reduction.*

Let $\mathfrak{l}$ be a prime ideal of A different from $\mathfrak{p}_v$.

THEOREM 1. *An elliptic A-module X over K has good reduction at v if and only if the Galois module $X_{\mathfrak{l}^\infty}=\bigcup_n X_{\mathfrak{l}^n}$ is unramified at v.*

PROOF. The "only if" part is a trivial consequence from the definition of good reduction. Assume that the Galois module $X_{\mathfrak{l}^\infty}$ is unramified. Some power of $\mathfrak{l}$ is principal——say $\mathfrak{l}^h=bA$. First, we show that X has stable reduction at v. Let $\bar{v}$ be an extension of v to K_s. Since $X_b=\{t\in K_s \mid b_X(t)=0\}$ is unramified, $\bar{v}(t)$ are integers for all non zero $t\in X_b$ and the maximum M of these values is equal to $-v(b_X)$. Indeed, let $b_X(T)=\sum b_j T^{q^j}=T\sum b_j T^{q^j-1}$. Then the maximal value M of the roots is given by the formula:

$$M=\mathrm{Max}\{(v(b_0)-v(b_j))/(q^j-1) \mid j>0\}\,.$$

Since $\mathfrak{l}\neq\mathfrak{p}_v$, $b_0=D(b_X)$ is a v-unit, hence $v(b_0)=0$. By definition of $v(b_X)$, we have $M=-v(b_X)$. Especially, $v(b_X)$ must be an integer. Let (L, w) be a finite extension of (K, v) where X has stable reduction (Proposition 2). Let u be an element of $L^\times$ such that $u(X)$ has integral coefficients at w. Since the reduction of $u(X)$ at w is an elliptic module over $k(w)$, $ua_Xu^{-1} \bmod \mathfrak{m}_w$ has a positive degree as a polynomial in ϕ with coefficients in $k(w)$ for nonconstant $a\in A$ (Proposition 1), or equivalently, $w(u)=w(a_X)$. Hence $v(a_X)$ is an integer ($=v(b_X)$) independent of a. This means that $e_v(X)=1$ and X has stable reduction at v. Thus we may assume that X has integral coefficients at v. To prove that X has good reduction at v, it suffices to show that the leading coefficient of b_X is a v-unit. Indeed, when this is the case, the reduction of X at v has the same rank of X (Proposition 1). Assume that the leading coefficient of b_X is not a v-unit. Since the constant term b_0 ($=D(b_X)$) of b_X is a v-unit, there is an element t_1 of X_b such that

(2) $$\bar{v}(t_1)<0\,.$$

Next, we can find a root t_2 of the equation

(3) $$b_X(T)=t_1$$

such that $\bar{v}(t_1)<\bar{v}(t_2)<0$. Indeed, if $\bar{v}(t)\leqq\bar{v}(t_1)$ holds for each root t of the equation (3), the coefficients of $t_1^{-1}b_Xt_1$ are $\bar{v}$-integers, hence $\bar{v}(t_1^{-1})\leqq v(b_X)=0$. This contradicts (2). It follows from (2) that none of roots of the equation (3) is a $\bar{v}$-integer, hence $\bar{v}(t_2)<0$. Similarly, we can find t_n in K_s such that

$$b_X(t_{n+1})=t_n\,,\qquad \bar{v}(t_n)<\bar{v}(t_{n+1})<0$$

for $n\geqq1$. Since t_n is contained in X_{b^n}, hence in $X_{\mathfrak{l}^\infty}$, the value $\bar{v}(t_n)$ is an integer for each n. This is impossible, and proves Theorem 1.

Let $\bar{v}$ be an extension of v to K_s. We denote the inertia group of $\bar{v}$ by $I(\bar{v})$ and the inertia field by K_v^{nr}. Let

$$\rho_{\mathfrak{l}}: \mathrm{Gal}(K_s/K) \longrightarrow \mathrm{Aut}_A(X_{\mathfrak{l}^\infty}) \cong \mathrm{Aut}_{A_{\mathfrak{l}}}(T_{\mathfrak{l}}(X))$$

denote the $\mathfrak{l}$-adic representation of degree r corresponding to the Galois module $X_{\mathfrak{l}^\infty}$ or the *Tate module* $T_{\mathfrak{l}}(X) = \mathrm{inv}\lim X_{\mathfrak{l}^n}$.

COROLLARY 1. *The elliptic A-module X has potential good reduction at v if and only if the image of the inertia group $I(\bar{v})$ by $\rho_{\mathfrak{l}}$ is finite. When this is the case, the extension $K_v^{\mathrm{nr}}(X_{\mathfrak{l}^\infty})$ of K_v^{nr} is independent of $\mathfrak{l}$ and cyclic tamely ramified of degree $e_v(X)$.*

PROOF. This follows from Theorem 1 and Proposition 2.

COROLLARY 2. *Suppose that X has potential good reduction at v. Let $\mathfrak{m} \neq A$ be an ideal of A prime to $\mathfrak{p}_v$.*

(i) *The extension $K_v^{\mathrm{nr}}(X_{\mathfrak{m}})$ of K_v^{nr} is independent of $\mathfrak{m}$ and tamely ramified of degree $e_v(X)$.*

(ii) *The Galois module $X_{\mathfrak{m}}$ is unramified if and only if X has good reduction at v.*

PROOF. Let $\mathfrak{l}$ be a prime divisor of $\mathfrak{m}$. The extension $K_v^{\mathrm{nr}}(X_{\mathfrak{l}^\infty})$ of $K_v^{\mathrm{nr}}(X_{\mathfrak{l}})$ is tamely ramified, and its Galois group is canonically isomorphic to a subgroup of the kernel of the natural homomorphism of $\mathrm{Aut}_A(X_{\mathfrak{l}^\infty})$ into $\mathrm{Aut}_A(X_{\mathfrak{l}})$ which is a pro-p-group. Therefore this extension is trivial. Since the extensions $K_v^{\mathrm{nr}}(X_{\mathfrak{l}^\infty}) = K_v^{\mathrm{nr}}(X_{\mathfrak{l}})$ are independent of $\mathfrak{l}$, we have $K_v^{\mathrm{nr}}(X_{\mathfrak{m}}) = K_v^{\mathrm{nr}}(X_{\mathfrak{l}^\infty})$. This proves Corollary 2.

REMARK. Part (i) of Corollary 2 shows that if X has potential good reduction at v, the extensions $K(X_{\mathfrak{m}})/K$ are always tamely ramified at v for all $\mathfrak{m}$ prime to $\mathfrak{p}_v$. On the contrary, for an abelian variety A, the primes v at which $K(A_m)/K$ are wildly ramified play an especially nasty role, cf. [7].

LEMMA 1. *Let X be an elliptic A-module over a field k, α an endomorphism of X, and $T_{\mathfrak{l}}(\alpha)$ the induced endomorphism of $T_{\mathfrak{l}}(X)$ ($\mathfrak{l} \neq \mathrm{div\,char}\, k$). Then the characteristic polynomial of $T_{\mathfrak{l}}(\alpha)$ has coefficients in A independent of $\mathfrak{l}$.*

PROOF. The subring $A[\alpha]$ generated by α in $\mathrm{End}(X)$ is a commutative ring without zero divisor, and let E be its quotient field. Since $\mathrm{End}(X) \otimes_A F_\infty$ is a division ring ([3]), the prime ∞ does not split in E. Let B be the integral closure of A in E, then $A[\alpha]$ is an order of B. Hence X can be regarded as an elliptic $A[\alpha]$-module over k. Since there exist an elliptic B-module which is isogenous to X [5, Proposition 3.2], we may assume that X is an elliptic B-module over k. Then the Tate module $T_{\mathfrak{l}}(X)$ is a free $(B \otimes_A A_{\mathfrak{l}})$-module of finite type. Therefore the $\mathfrak{l}$-adic representation $T_{\mathfrak{l}}(\alpha)$ of α is induced by the representation of $\alpha: \beta \mapsto \alpha\beta$ on B. This proves Lemma 1.

LEMMA 2. *Let X be an elliptic A-module of rank r over a finite field with q^f elements. Then the characteristic polynomial of the $\mathfrak{l}$-adic representation $T_{\mathfrak{l}}(\phi^f)$*

of the Frobenius endomorphism ϕ^f *of* X *has coefficients in* A *independent of* $\mathfrak{l}$. *The absolute values at* ∞ *of its roots are equal to* $q^{f/r}$.

PROOF. This follows from Lemma 1 and [4, Proposition 2.1].

PROPOSITION 3. *Let* X *be an elliptic* A*-module over* K *of rank* r *which has potential good reduction at* v, *and* $\mathfrak{l}$ *a prime ideal of* A *different from* $\mathfrak{p}_v$.

(i) *For* $\sigma\in I(\bar{v})$, *the characteristic polynomial of* $\rho_{\mathfrak{l}}(\sigma)$ *has coefficients in* $\mathbf{F}_q$ *independent of* $\mathfrak{l}$.

(ii) *Suppose that the residue field* $k(v)$ *is finite,* $q_v=\mathrm{Card}(k(v))$. *Let* σ_v *be a Frobenius element in the decomposition group of* $\bar{v}$. *Then the characteristic polynomial of* $\rho_{\mathfrak{l}}(\sigma_v)$ *has coefficients in* A *independent of* $\mathfrak{l}$. *The absolute values at* ∞ *of its roots are equal to* $q_v^{1/r}$.

PROOF. Let w be the restriction of $\bar{v}$ to a Galois extension L of K of finite degree where X has good reduction. Let u be an element of $L^\times$ such that $Y=u(X)$ is an elliptic A-module over O_w. Let $\mathrm{rd}: Y\to Y(w)$ be the reduction mapping. Since $\sigma\in I(\bar{v})$, $u^{1-\sigma}$ is a w-unit and $(ux)^\sigma\equiv ux \bmod \mathfrak{m}_{\bar{v}}$ for all $x\in X_{\mathrm{tors}}$. This shows that the following diagram is commutative:

$$\begin{array}{ccccc} X_{\mathfrak{l}^\infty} & \xrightarrow[\sim]{u} & Y_{\mathfrak{l}^\infty} & \xrightarrow[\sim]{\mathrm{rd}} & Y(w)_{\mathfrak{l}^\infty} \\ {\scriptstyle\sigma}\downarrow & & & & \downarrow{\scriptstyle\zeta} \\ X_{\mathfrak{l}^\infty} & \xrightarrow[\sim]{u} & Y_{\mathfrak{l}^\infty} & \xrightarrow[\sim]{\mathrm{rd}} & Y(w)_{\mathfrak{l}^\infty} \end{array}$$

where $\zeta=(u^{1-\sigma} \bmod \mathfrak{m}_w)\in k(w)$. Since $\zeta: t\mapsto\zeta t$ induces an automorphism of the A-module $Y(w)_{\mathfrak{l}^\infty}$, ζ is an automorphism of the elliptic A-module $Y(w)$. Assertion (i) follows from Lemma 1 and the fact that ζ is a root of unity. Since (ii) is concerned with the Frobenius automorphism, we may assume that X has good reduction at v, replacing K, if necessary, by a totally ramified extension of K of degree $e_v(X)$. Then the $\mathfrak{l}$-adic representation of the Frobenius automorphism σ_v is equivalent to the $\mathfrak{l}$-adic representation of the Frobenius endomorphism of the reduction $X(v)$ of X at v, and the assertion follows from Lemma 2.

3. Complex multiplication.

Let C be the completion of the algebraic closure of the local field F_∞ at ∞. Let X be an elliptic A-module over C of rank one. We know that there is a holomorphic isomorphism $X\cong C/\Gamma$ where Γ is an *A-lattice* in F (= a fractional A-ideal of F). Then we notice that the torsion part $X_{\mathrm{tors}}\cong F/\Gamma$. Conversely, given Γ, there are corresponding elliptic A-modules over C. For details, see [3] and [5].

We denote by J_F the idèle group of F and by $[s, F]\in \mathrm{Gal}(F^{\mathrm{ab}}/F)$ the Artin symbol for $s\in J_F$, where F^{ab} is the maximal abelian extension of F.

LEMMA 3. *Let X be an elliptic A-module over a field k of rank one. Then* $\mathrm{End}(X)\cong A$, *hence* $\mathrm{Aut}(X)\cong \mathbf{F}_q^{\times}$.

PROOF. This follows from the facts that A is integrally closed and that $\mathrm{End}(X)$ is a projective A-module whose rank is not greater than $(\mathrm{rank}\, X)^2$ [3, Proposition 2.4, Corollary].

LEMMA 4. *Let X and Y be two elliptic A-modules over a Dedekind ring O and L be a field containing O. Then*

$$\mathrm{Hom}_L(X, Y)\subset \mathrm{Hom}_{O_s}(X, Y)$$

where O_s denotes the separable closure of O.

PROOF. Let $\alpha\in\mathrm{Hom}_L(X, Y)$ and $\alpha\neq 0$. For a nonconstant $a\in A$, let

$$a_X=\sum_{i=0}^{n} a_i\phi^i\,, \qquad a_Y=\sum_{i=0}^{n} b_i\phi^i \qquad (a_i,\, b_i\in O)$$

and

$$\alpha=\sum_{j=0}^{m} x_j\phi^j \qquad\qquad (x_j\in L)$$

where a_n and b_n are units of O and $x_m\neq 0$. It is easily seen from $\alpha a_X=a_Y\alpha$ that

$$b_n x_m^{q^n-1}=a_n^{q^m}\,, \qquad \text{hence} \quad x_m\in O_s^{\times}\,,$$

and

$$b_n x_j^{q^n}-a_n^{q^j}x_j\in O[x_{j+1},\, x_{j+2},\, \cdots,\, x_m]$$

for each $j=m-1,\, m-2,\, \cdots,\, 0$. This shows $x_j\in O_s$ for each j, and proves Lemma 4.

THEOREM 2. *Let X be an elliptic A-module over C of rank one with an isomorphism $\xi\colon C/\Gamma \xrightarrow{\sim} X$. Let σ be an automorphism of C over F and s an idèle of F such that*

$$(4)\qquad\qquad \sigma\,|\,F^{\mathrm{ab}}=[s, F]\,.$$

Then there is an isomorphism $\xi'\colon C/s^{-1}\Gamma \xrightarrow{\sim} X^{\sigma}$ such that

$$(5)\qquad\qquad \xi(z)^{\sigma}=\xi'(s^{-1}z)$$

for every $z\in F/\Gamma$, i.e., the following diagram is commutative:

$$\begin{array}{ccc}
F/\Gamma & \xrightarrow[\sim]{\ \xi\ } & X_{\mathrm{tors}} \\
{\scriptstyle s^{-1}}\big\downarrow & & \big\downarrow{\scriptstyle \sigma} \\
F/s^{-1}\Gamma & \xrightarrow[\sim]{\ \xi'\ } & X_{\mathrm{tors}}^{\sigma}\,.
\end{array}$$

Moreover, ξ' is uniquely determined by the above property.

PROOF (cf. [8, p. 117]). 1) We may assume that X is an elliptic A-module over a finite Galois extension of F.

Indeed, every elliptic module of rank one over C is defined over a finite Galois extension of F [5, Proposition 8.7], and it is sufficient to prove the theorem for an elliptic module in a given C-isomorphism class of elliptic modules.

2) For each ideal $\mathfrak{m}(\neq\{0\}, A)$ of A there exists an isomorphism $\xi': C/s^{-1}\Gamma \xrightarrow{\sim} X^{\sigma}$ such that (5) holds for every $z \in \mathfrak{m}^{-1}\Gamma/\Gamma$.

Indeed, let K be a finite Galois extension of F satisfying the following conditions:

(a) X and X^{σ} are elliptic modules over K and

$$\mathrm{Hom}_{K_s}(X, X^{\sigma}) = \mathrm{Hom}_K(X, X^{\sigma}).$$

(b) K contains both $X_{\mathfrak{m}}$ and the ray class field of F modulo $\mathfrak{m}$.

Then we can find a prime v of K lying above a prime ideal $\mathfrak{p}$ of A so that the following conditions are satisfied:

(c) v is unramified over $\mathfrak{p}$ and $\sigma|K$ is the Frobenius element σ_v of $\mathrm{Gal}(K/F)$ for v, so $\mathfrak{m}$ is prime to $\mathfrak{p}$.

(d) X and X^{σ} are elliptic modules over O_v.

Consider a commutative diagram:

(6)
$$\begin{array}{ccc} C/\Gamma & \xrightarrow[\sim]{\ \xi\ } & X \\ {\scriptstyle \text{can.}}\downarrow & & \downarrow{\scriptstyle \alpha} \\ C/\mathfrak{p}^{-1}\Gamma & \xrightarrow[\sim]{\ \eta\ } & Y \end{array}$$

where $\alpha: X \to Y = X/X_{\mathfrak{p}}$ ($=\mathfrak{p}*X$, cf. [5]) is the canonical O_v-isogeny whose reduction at v is the Frobenius morphism $\phi^{\deg \mathfrak{p}}$. Then we have an isomorphism $u: Y \xrightarrow{\sim} X^{\sigma}$ [5, Theorem 8.5]. Since Y and X^{σ} have the same reduction $Y(v) = X^{\sigma}(v)$ at v, u induces an automorphism c ($\in \mathbf{F}_q^{\times}$) of $X^{\sigma}(v)$. Put $\kappa = c^{-1}u \circ \alpha$ and $\xi^* = c^{-1}u \circ \eta$. Since $\mathfrak{m}$ is prime to $\mathfrak{p}$ and the reduction of κ at v is the Frobenius morphism, we obtain from (6) a commutative diagram:

$$(7)\qquad \begin{array}{ccc} \mathfrak{m}^{-1}\Gamma/\Gamma & \xrightarrow[\sim]{\ \ \xi\ \ } & X_{\mathfrak{m}} \\ \Big\downarrow{\scriptstyle \text{can.}} & & \Big\downarrow{\scriptstyle \sigma} \\ \mathfrak{m}^{-1}\mathfrak{p}^{-1}\Gamma/\mathfrak{p}^{-1}\Gamma & \xrightarrow[\sim]{\ \ \xi^*\ \ } & X^{\sigma}_{\mathfrak{m}}\,. \end{array}$$

It follows from the assumption (4) and the condition (b) that there is an element a of $F^\times$ such that $\mathfrak{p}=asA$ and $az\equiv s^{-1}z \bmod s^{-1}\Gamma$ for all $z\in\mathfrak{m}^{-1}\Gamma$. Let $\xi': C/s^{-1}\Gamma \xrightarrow{\sim} X^{\sigma}$ be the isomorphism defined by

$$\xi'(z)=\xi^*(a^{-1}z)\,.$$

Then we see from (7) that (5) holds for every $z\in\mathfrak{m}^{-1}\Gamma/\Gamma$.

3) ξ' (in 2)) is uniquely determined by $\mathfrak{m}$, and consequently, independent of $\mathfrak{m}$, this proves Theorem 2. Indeed, if ξ'_1 and ξ'_2 satisfy (5) for every $z\in\mathfrak{m}^{-1}\Gamma/\Gamma$, then $c=\xi'_2\circ\xi_1'^{-1}$ is an automorphism of X^{σ}, hence $c\in\mathbf{F}_q^{\times}$ (Lemma 3). Since $c\,|\,X^{\sigma}_{\mathfrak{m}}=\text{id.}$, we have $c\equiv 1 \bmod \mathfrak{m}$, hence $c=1$ and $\xi'_1=\xi'_2$, q. e. d.

Let K be a finite separable extension of F, and X an elliptic A-module over K of rank one. For a prime ideal $\mathfrak{l}$ of A, since $\mathrm{Aut}_{A_{\mathfrak{l}}}(T_{\mathfrak{l}}(X))\cong A_{\mathfrak{l}}^{\times}$ (the $\mathfrak{l}$-adic units) is abelian, class field theory allows us to identify the $\mathfrak{l}$-adic representation $\rho_{\mathfrak{l}}$ with a continuous homomorphism

$$\rho_{\mathfrak{l}}: J_K \longrightarrow A_{\mathfrak{l}}^{\times}\subset F_{\mathfrak{l}}^{\times}$$

which is trivial on $K^\times$.

THEOREM 3. *Notations being above, there exist two continuous homomorphisms* ρ_∞ *and* χ;

$$\textit{the “Grössencharakter”}\quad \rho_\infty: J_K \longrightarrow F_\infty^{\times}$$

which is trivial on $K^\times$, *and*

$$\textit{the “Hecke character”}\quad \chi: J_K \longrightarrow F^{\times}$$

satisfying the following conditions:

$$(\mathrm{R})_{\mathfrak{l}} \qquad \rho_{\mathfrak{l}}(x)\cdot N_{K/F}(x)_{\mathfrak{l}}=\chi(x) \quad \textit{in} \quad F_{\mathfrak{l}}^{\times}$$

for all $x\in J_K$, *and*

$$(\mathrm{R})_{\infty} \qquad \rho_{\infty}(x)\cdot N_{K/F}(x)_{\infty}=\chi(x) \quad \textit{in} \quad F_{\infty}^{\times}$$

for all $x\in J_K$. *Hence the homomorphism*

$$\rho=\rho_\infty\times\prod_{\mathfrak{l}}\rho_{\mathfrak{l}}: J_K \longrightarrow F_\infty^{\times}\times\prod_{\mathfrak{l}} A_{\mathfrak{l}}^{\times}\subset J_F$$

has the property:

$$\text{(R)} \qquad \rho(x)\cdot N_{K/F}(x)=\chi(x) \quad \text{in } J_F$$

for all $x\in J_K$.

PROOF. For $x\in J_K$, put $\tau=[x, K]$, $y=N_{K/F}x$ and $\chi_{\mathfrak{l}}(y)=\rho_{\mathfrak{l}}(x)y_{\mathfrak{l}}$. Since $\tau|F^{\mathrm{ab}}=[y, F]$, for a given isomorphism ξ of C/Γ onto X, there exists by Theorem 2 an isomorphism ξ' of $C/y^{-1}\Gamma$ onto X^τ such that $\xi(z)^\tau=\xi'(y^{-1}z)$ for all $z\in F/\Gamma$. Since $X=X^\tau$, $w=\xi^{-1}\circ\xi'$ is an isomorphism of $C/y^{-1}\Gamma$ onto C/Γ. Hence $w\in F^\times$ and we obtain a commutative diagram:

$$\begin{array}{ccc} F/\Gamma & \xrightarrow{\ \xi\ } & X_{\mathrm{tors}} \\ {\scriptstyle wy^{-1}}\downarrow & & \downarrow{\scriptstyle \tau} \\ F/\Gamma & \xrightarrow{\ \xi\ } & X_{\mathrm{tors}}. \end{array}$$

This shows that $\rho_{\mathfrak{l}}(x)=wy_{\mathfrak{l}}^{-1}$ for all $\mathfrak{l}$, and consequently $\chi_{\mathfrak{l}}(x)=w\in F^\times$ is independent of $\mathfrak{l}$. This proves $(\mathrm{R})_{\mathfrak{l}}$. Put $\rho_\infty(x)=\chi(x)\cdot N_{K/F}(x)_\infty^{-1}$. If $x\in K^\times$, we obtain by $(\mathrm{R})_{\mathfrak{l}}$ that $\chi(x)=N_{K/F}(x)$, hence $\rho_\infty(x)=1$, q. e. d.

REMARK. From (R) we have

$$N_{K/F}(J_K)\subset F^\times\cdot(F_\infty^\times\times\prod_{\mathfrak{l}} A_{\mathfrak{l}}^\times).$$

This means that K contains the *Hilbert class field* H_A of A (=the maximal abelian unramified extension of F completely split at ∞). Actually, it is well known (cf. [5]) that the smallest field of definition is H_A for any rank-one elliptic A-module over C.

Let $K_\infty^\times=(K\otimes_F F_\infty)^\times$ denote the group of idèles x of K such that $x_v=1$ for all *finite* places v (i. e., not lying above ∞) of K.

COROLLARY 1. (i) $\rho_{\mathfrak{l}}|K_\infty^\times=\chi|K_\infty^\times$, *and these have values in* $\mathbf{F}_q^\times$.

(ii) *Let v be a finite place of K lying above a prime ideal $\mathfrak{p}$ of A and $\mathfrak{l}$ a prime ideal of A different from $\mathfrak{p}$. Then*

$$\rho_{\mathfrak{l}}|K_v^\times=\rho_\infty|K_v^\times=\chi|K_v^\times.$$

Hence $\rho_{\mathfrak{l}}|K_v^\times$ has values in $F^\times$ independent of $\mathfrak{l}$.

COROLLARY 2. *Let v be a finite place of K. Then the following properties are equivalent:*

(a) *X has good reduction at v.*

(b) *χ is unramified at v, i. e.,* $\chi(O_v^\times)=1$.

(c) *ρ_∞ is unramified at v, i. e.,* $\rho_\infty(O_v^\times)=1$

Let v be a finite place of K where X has good reduction, ϕ_v the Frobenius endomorphism of the reduction $X(v)$ of X at v and a_v the element of A such that $[a_v]_{X(v)}=\phi_v$. Then

COROLLARY 3. *The Hecke character χ associated to X is characterized by the following three properties:*

(a) *If x is principal idèle of K, $\chi(x)=N_{K/F}(x)$.*

(b) *The kernel of χ is open in J_K.*

(c) *If X has good reduction at v, $\chi(x_v)=a_v^{v(x_v)}$ for all $x_v \in K_v^\times$.*

4. Classification of rank-one elliptic modules.

Let K be a finite separable extension of F including the Hilbert class field H_A of A. We know that every elliptic A-module of rank one over an extension of F is isomorphic to an elliptic A-module over H_A, hence over K. In this section, by X, Y and Z we shall always understand elliptic A-modules over K of rank one, hence, by Lemma 4, all homomorphisms are K_s-homomorphisms. By a *K-form* of X we mean an elliptic A-module over K which is K_s-isomorphic to X. When $X \cong C/\Gamma$, we denote by $\mathrm{cl}(X)$ the class of Γ in $\mathrm{Pic}(A)$. Then the correspondence $X \mapsto \mathrm{cl}(X)$ gives a bijection:

$$\{K_s\text{-isomorphism classes of rank-one elliptic modules}\} \longleftrightarrow \mathrm{Pic}(A).$$

A homomorphism $\chi: J_K \to F^\times$ is called a *Hecke character* if it satisfies the following conditions H1)-3):

H1) $\chi | K^\times = N_{K/F}$.

H2) $\mathrm{Ker}\, \chi$ is open in J_K.

H3) $\chi(K_\infty^\times) \subset \mathbf{F}_q^\times$.

The Hecke character χ_X associated to a rank-one elliptic module X over K is a Hecke character in this sense.

THEOREM 4. (i) *Let c be an element of* $\mathrm{Pic}(A)$ (*the ideal class group of* A) *and let χ be a Hecke character of J_K into $F^\times$. Then there exists an elliptic module X over K of rank one with* $\mathrm{cl}(X)=c$ *and* $\chi_X=\chi$.

(ii) *The Hecke character χ_X determines the K-isogeny class of X, and the pair* $(\mathrm{cl}(X), \chi_X)$ *determines the K-isomorphism class of X.*

Before proving this theorem, we remark that one can apply the well known "theory of K-forms" (cf. [2], [6]) to elliptic modules: First, notice that

$$H^1(G, \mathrm{Aut}(X)) = H^1(G, \mathbf{F}_q^\times) = H^1(G, F^\times)$$

where $G=\mathrm{Gal}(K_s/K)$, and that

$$H^1(G, \mathbf{F}_q^\times) = \mathrm{Hom}(G, \mathbf{F}_q^\times)$$

where "Hom" means continuous homomorphisms. To each pair (X, Y) of elliptic modules, we associate $\omega_{Y/X} \in \mathrm{Hom}(G, \mathbf{F}_q^\times)$ as follows: Since Y is isogenous to

X over C, hence over K_s, there are K_s-isogenies $\alpha: X \to Y$ and $\beta: Y \to X$. For $\sigma \in G$ let a_σ be the element of A such that $[a_\sigma]_X = \beta \cdot \alpha^\sigma$. Then

$$\omega_{Y/X}: G \longrightarrow F^\times, \qquad \sigma \longmapsto a_1^{-1} a_\sigma$$

defines a 1-cocycle. Hence $\omega_{Y/X}(\sigma) \in \mathbf{F}_q^\times$. We see that $\omega_{Y/X}$ is characterized by the following property:

$$(8) \qquad \gamma \cdot \omega_{Y/X}(\sigma) = \gamma^\sigma \qquad \text{for all} \quad \gamma \in \mathrm{Hom}_{K_s}(X, Y).$$

Thus, $\omega_{Y/X}$ is independent of α and β. It is clear that the transitivity formula

$$(9) \qquad \omega_{Z/X} = \omega_{Z/Y} \cdot \omega_{Y/X}$$

holds.

LEMMA 5. (i) *Y and Z are K-isogenous if and only if $\omega_{Y/X} = \omega_{Z/X}$. When this is the case,*

$$\mathrm{Hom}_{K_s}(Y, Z) = \mathrm{Hom}_K(Y, Z).$$

(ii) *Y and Z are K-isomorphic if and only if they are K-isogenous and K_s-isomorphic.*

(iii) *For given X and $\omega \in \mathrm{Hom}(G, \mathbf{F}_q^\times)$, there exists a unique* (*up to K-isomorphism*) *K-form Y* (notation: $X^{(\omega)}$) *of X with $\omega_{Y/X} = \omega$.*

PROOF. Assertions (i) and (ii) follow immediately from (8) and (9). (iii): By "Hilbert 90" there is an element u of $K_s^\times$ such that $\omega(\sigma) = u^{-1} u^\sigma$ for all $\sigma \in G$. Then $Y = u(X)$ has the required property, and the uniqueness follows from (ii).

Now we prove Theorem 4. Class field theory allows us to identify the character $\omega_{Y/X}$ with a continuous homomorphism

$$\omega_{Y/X}: J_K \longrightarrow \mathbf{F}_q^\times$$

which is trivial on $K^\times$. Assertion (ii) of Theorem 4 follows from Lemma 5 and

LEMMA 6. $\chi_Y = \omega_{Y/X} \cdot \chi_X$.

PROOF. Let $V_\mathfrak{l}(X) = T_\mathfrak{l}(X) \otimes_{A_\mathfrak{l}} F_\mathfrak{l}$. A K_s-isogeny $\alpha: X \to Y$ induces an isomorphism $V_\mathfrak{l}(\alpha): V_\mathfrak{l}(X) \xrightarrow{\sim} V_\mathfrak{l}(Y)$. We obtain from (8) a commutative diagram:

$$\begin{array}{ccc}
V_\mathfrak{l}(X) & \xrightarrow[\sim]{V_\mathfrak{l}(\alpha)} & V_\mathfrak{l}(Y) \\
\Big\downarrow{\scriptstyle \omega_{Y/X}(\sigma)\cdot\sigma} & & \Big\downarrow{\scriptstyle \sigma} \\
V_\mathfrak{l}(X) & \xrightarrow[\sim]{V_\mathfrak{l}(\alpha)} & V_\mathfrak{l}(Y).
\end{array}$$

This diagram implies that $\omega_{Y/X}\cdot\rho_{X,\mathfrak{l}}=\rho_{Y,\mathfrak{l}}$ where $\rho_{X,\mathfrak{l}}$ and $\rho_{Y,\mathfrak{l}}$ are $\mathfrak{l}$-adic representation of the Galois group associated to X and Y, respectively. This proves Lemma 6.

PROOF OF THEOREM 4, (i). Given c and χ, let X be any elliptic module with $\mathrm{cl}(X)=c$. Put $\omega=\chi/\chi_X : J_K\to F^\times$. The homomorphism ω is continuous and trivial on $K^\times$. Since the idèle class group $J_K^0/K^\times$ of degree zero is compact, we obtain from H3) that $\omega(K_\infty^\times J_K^0)\subset\mathbf{F}_q^\times$. Since $K_\infty^\times J_K^0$ has a finite index in J_K, the image $\omega(J_K)$ lies in $\mathbf{F}_q^\times$. By Lemmas 5 and 6, χ is the Hecke character associated to the elliptic module X^ω.

COROLLARY. *For given X there exists a K-form Y of X so that all infinite places of K completely split in $K(Y_{\mathrm{tors}})$.*

PROOF. It follows from the theorem of Grunwald-Hasse-Wang (cf. [**1**, Chapter 10]) that there exists a continuous homomorphism $\omega: J_K\to\mathbf{F}_q^\times$ trivial on $K^\times$ such that $\omega|K_\infty^\times=\chi_X^{-1}|K_\infty^\times$. Let $Y=X^\omega$. Then we see that χ_Y is trivial on $K_\infty^\times$. Hence $\rho_{Y,\mathfrak{l}}$ are trivial on $K_\infty^\times$ for all $\mathfrak{l}$. This proves Corollary.

THEOREM 5. *Let X be an elliptic A-module of rank one over K. Then there exists a K-form of X which has good reduction everywhere (i.e., at every finite place of K).*

PROOF. Let U_f be the group of idèles $x=(x_v)$ of K such that $x_v\in O_v^\times$ for finite v and $x_v=1$ for infinite v. First, we show that the Hecke character χ_X associated to X is trivial on $U_f\cap K^\times J_K^{q-1}$. Indeed, let $u\in U_f\cap K^\times J_K^{q-1}$ and $u=zx^{q-1}$ where $z\in K^\times$ and $x\in J_K$. For $s\in J_K$ and $y\in K^\times$, let

$$[s,\ y]_K=(y^{1/(q-1)})^{[s,K]-1}$$

be the Hilbert symbol. Since the extension $K(z^{1/(q-1)})/K$ is unramified everywhere and splits completely at every infinite place, we have $[s,z]_K=1$ for all $s\in K^\times K_\infty^\times U_f$. The principal ideal theorem says that $J_F\subset K^\times K_\infty^\times U_f$, as K contains the Hilbert class field of A. Hence we have $[s, N_{K/F}z]_F=1$ for all $s\in J_F$. This implies that $N_{K/F}z$ is a $(q-1)$th power in $F^\times$, hence $N_{K/F}u$ is a $(q-1)$th power in J_F. We see from (R) that $\chi_X(u)$ is a local $(q-1)$th power everywhere, hence in global. Consequently we have $\chi_X(u)\in\mathbf{F}_q^\times\cap F^{\times q-1}=\{1\}$.

Thus χ_X induces a character of $U_f/(U_f\cap K^\times J_K^{q-1})$ valued in $\mathbf{F}_q^\times$. Since $U_f/(U_f\cap K^\times J_K^{q-1})$ is a closed subgroup of a compact abelian group $J_K/K^\times J_K^{q-1}$ of exponent $q-1$, we can extend this character $\chi_X|U_f$ to a character

$$\omega: J_K\longrightarrow\mathbf{F}_q^\times$$

which is trivial on $K^\times$. Since $\chi_X|U_f=\omega|U_f$, the Hecke character $\psi=\omega^{-1}\cdot\chi_X$ is trivial on U_f. This shows that the K-form of X with the Hecke character ψ has good reduction everywhere, q. e. d.

REMARK. Let B be the integral closure of A in K. Hayes [**5**, Theorem 10.6] proved that if F has a prime divisor of degree one, for given X, there is an elliptic module over B which is isomorphic to X over K_s.

References

[1] E. Artin and J. Tate, Class field theory, Benjamin, New York, 1968.
[2] A. Borel et J.-P. Serre, Théorèmes de finitude en cohomologie galoisienne, Comm. Math. Helv., **39** (1964), 111-164.
[3] V.G. Drinfel'd, Elliptic modules (Russian), Mat. Sb., **94** (1974) ; Math. USSR-Sb., **23** (1974), 561-592.
[4] V.G. Drinfel'd, Elliptic modules II (Russian), Mat. Sb., **102** (1977) ; Math. USSR-Sb., **31** (1977), 159-170.
[5] D.R. Hayes, Explicit class field theory in global function fields, Studies in algebra and number theory, Advances in Math., Supplementary Studies, **6** (1980), 173-217.
[6] J.-P. Serre, Cohomologie galoisienne, Lecture Notes in Math., No. **5**, Springer-Verlag, 1964.
[7] J.-P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math., **88** (1968), 492-517.
[8] G. Shimura, Introduction to arithmetic theory of automorphic functions, Iwanami Shoten and Princeton Univ. Press, 1971.

Toyofumi TAKAHASHI
Department of Mathematics
College of General Education
Tôhoku University
Kawauchi, Sendai 980
Japan