T. NAKAMURA
KODAI MATH. J.
2 (1979), 123—129

A NOTE ON ENDOMORPHISM RINGS OF ABELIAN VARIETIES OVER FINITE FIELDS

BY TETSUO NAKAMURA

Let p be a prime and let A be a simple abelian variety over a finite field k with p^a elements. In this note we ask some sufficient conditions that the endomorphism ring of A over k is maximal at p. Our result includes the first part of theorem 5.3 in Waterhouse [5]. The related facts should be referred to [5].

§1. Let $\mathrm{End}_k(A)$ be the ring of k-endomorphisms of a simple abelian variety A over a finite field k with p^a elements. We shall always assume that $\mathrm{End}_k(A)$ is commutative. Then there exist a CM field E and an isomorphism $i_A: E \to \mathrm{End}_k(A)\otimes \boldsymbol{Q}$. Let $R=\imath_A^{-1}(\mathrm{End}_k(A))$ and let K be the totally real subfield of index 2 in E. Let f_A be the Frobenius endomorphism of A over k and put $\pi=\imath_A^{-1}(f_A)$. Then π is a Weil p^a-number, i.e. an algebraic integer such that $|\pi|^2=p^a$ in all embeddings of $E=\boldsymbol{Q}(\pi)$ into $\boldsymbol{C}$. Let w be a place of K above p and v be a place of E with $v|w$. Then we have the following three cases;

(1) $v(\pi)=0$ or $v(\pi)=v(p^a)$.

(2) $v(\pi)=v(p^a\pi^{-1})$.

(3) $v(\pi)\neq v(p^a\pi^{-1})$ and $0<v(\pi)<v(p^a)$.

We call that w is of type (1) (resp., (2), (3)) if v satisfies (1) (resp., (2), (3)). This is independent of the choice of v with $v|w$. Let K_w be the completion of K at w and let

$$\begin{aligned} G_w &= (G_{1,0})^{[K_w:\boldsymbol{Q}_p]}, \quad \text{if } w \text{ is of type (1)},\\ &= (G_{1,1})^{[K_w:\boldsymbol{Q}_p]}, \quad \text{if } w \text{ is of type (2)},\\ &= G_{s,t}+G_{t,s}, \quad \text{if } w \text{ is of type (3)}, \end{aligned}$$

where $s=s(w)=[K_w:\boldsymbol{Q}_p]v(\pi)/v(p^a)$ and $t=t(w)=[K_w:\boldsymbol{Q}_p]v'(\pi)/v'(p^a)$ with the other place v' of E above w. Then the formal group $\hat{A}$ of A is isogenous to $\sum_{w|p} G_w$(over the algebraic closure of k.) (cf. Manin [1], Chap. IV).

Now let T_pA be the Dieudonné module of $\hat{A}$. Let $W=W(k)$ be the ring of Witt vectors over k and σ the automorphism of W induced by the Frobenius

Received October 13, 1977.

automorphism $x \to x^p$ of k. Let $\mathcal{A}=W[F, V]$ be the (non-commutative) ring defined by the relations $FV=VF=p$, $F\lambda=\lambda^\sigma F$ and $\lambda V=V\lambda^\sigma$ for $\lambda \in W$. Then T_pA is a left $\mathcal{A}$-module, W-free of rank $2\dim(A)$. It is a well known result of Tate that

$$\mathrm{End}_k(A)\otimes \boldsymbol{Z}_p \cong \mathrm{End}_{\mathcal{A}}\, T_pA\,.$$

Assume further that

(*) R contains the maximal order O_K of K.

Then as T_pA is a module over $O_K\otimes \boldsymbol{Z}_p=\bigoplus_{w|p} O_{K_w}$, we have the corresponding decomposition $T_pA=\bigoplus_{w|p} T_w$, where O_{K_w} is the ring of integers of K_w. We see that T_w is a Dieudonné module whose corresponding formal group is isogenous to G_w.

§2. THEOREM 1. *Let the notations be as in* §1. *We assume* (*) *and the followings, for each* w *of type* (2), K_w *is an unramified extension over* $\boldsymbol{Q}_p$ *of odd degree and* $FT_w=VT_w$, *and for each* w *of type* (3), $F^{t(w)}T_w\subset V^{s(w)}T_w$(*say* $s(w)<t(w)$.). *Then* R *is maximal at* p, *i.e.* $R\otimes \boldsymbol{Z}_p$ *is the maximal order of* $E\otimes \boldsymbol{Q}_p$.

Proof. Let L be the quotient field of $W=W(k)$, i.e. L is the unramified extension over $\boldsymbol{Q}_p$, of degree a. Put $\mathcal{B}=L\otimes_W\mathcal{A}=L[F, V]=L[F, F^{-1}]$. Let $\bigoplus_{v|p} E_v$ be the decomposition of $E_p=E\otimes \boldsymbol{Q}_p$ into fields. On $L\otimes_{\boldsymbol{Q}_p}E_p=\bigoplus_{v|p}(L\otimes_{\boldsymbol{Q}_p}E_v)$ we have L acting by left multiplication and E_p by right multiplication. Let f_v be the residue degree of $E_v/\boldsymbol{Q}_p$. Put $g_v=(f_v, a)$. Then LE_v has degree a/g_v over E_v and $L\otimes E_v$ is a sum of g_v copies of the composite extension:

$$L\otimes E_v\cong LE_v\oplus \cdots \oplus LE_v\,.$$

$$\omega\otimes\beta \longrightarrow \langle \omega\beta, \omega^\sigma\beta, \cdots, \omega^{\sigma^{g-1}}\beta\rangle\,.$$

We define the action of σ on $L\otimes E_v$ by acting on the L-factor. Then for $\langle x_1, \cdots, x_{g_v}\rangle \in \bigoplus LE_v$, we have $\sigma\langle x_1, \cdots, x_{g_v}\rangle=\langle x_2, \cdots, x_{g_v}, \tau(x_1)\rangle$, where $\tau=\sigma^{g_v}$ is the Frobenius automorphism of LE_v/E_v. Now we can choose $u\in L\otimes E_v$ with $N_{L\otimes E_v/E_v}(u)=\pi$, where N is the norm map. Define $F=u\sigma$. Then $F\lambda=\lambda^\sigma F$ for all $\lambda\in L$, and $F^a=\pi$. Thus we have constructed an operation of $\mathcal{B}$ on $L\otimes E_v$ and hence on $L\otimes E_p$. Then as a $\mathcal{B}$-module

$$V_pA=T_pA\otimes_W L\cong L\otimes E_p\,.$$

(For details of the above facts, see Chap. 5, [5].) As T_pA is an $\mathcal{A}$-invariant lattice in V_pA, we may suppose that T_pA is an $\mathcal{A}$-invariant lattice in $L\otimes E_p$. Then T_w is a lattice in $L\otimes_{\boldsymbol{Q}_p}E_w\subset L\otimes E_p$, where $E_w=E\otimes_K K_w$. Let $R_w=\mathrm{End}_{\mathcal{A}}(T_w)$, then we clearly have

$$R\otimes Z_p=\bigoplus_{w|p} R_w\,.$$

Now we claim that each R_w is the maximal order of E_w.

(i) The case that w is of type (1). Then w splits in E/K. Since $\pi-p^a\pi^{-1}$

is a unit, we see that $O_{K_w}[\pi]$ is maximal. As $R_w \supset O_{K_w}[\pi]$, R_w is maximal.

(ii) The case that w is of type (3). Then w also splits in E/K into v and v'; $L\otimes_{Q_p}E_w=(L\otimes_{Q_p}E_v)\oplus(L\otimes_{Q_p}E_{v'})$. Take $\alpha, \alpha' \in LE_v$ such that $N_{LE_v}(\alpha)=\pi$ and $N_{LE_v}(\alpha')=p^a\pi^{-1}$. We can put $F=(\langle 1, \cdots, 1, \alpha\rangle+\langle 1, \cdots 1, \alpha'\rangle)\sigma$ on $(L\otimes E_v)\oplus(L\otimes E_{v'})$. Say $v(\pi)<v'(\pi)=v(p^a\pi^{-1})$, then $s=[K_w : Q_p]v(\pi)/v(p^a)$ and $t=[K_w : Q_p]v'(\pi)/v(p^a)$. Since T_w is a $W\otimes O_{K_w}$-module, we have a decomposition $T_w=\bigoplus_{i=1}^{g} T_i$, corresponding to the decomposition $W\otimes_{Z_p}O_{K_w}=\bigoplus WO_{K_w}(g=g_v)$. As $T_w\otimes_{Z_p}\boldsymbol{Q}_p=L\otimes_{Q_p}E_w$, we have $T_i\otimes_{Z_p}\boldsymbol{Q}_p\cong LK_w\otimes_k E(\cong LE_v\oplus LE_{v'})$. Thus T_i is a WO_{K_w}-free module of rank 2 and $W[F^g, V^g]$-invariant. As a WO_{K_w}-module it has a basis of the form $(\lambda^{n_i}, 0), (\mu_i, \lambda^{m_i})$ with $\mu_i=0$ or $v(\mu_i)<n_i$, where λ is a prime element of O_{K_w}. From the assumption we have that $V^{-s}F^tT_w=p^{-s}F^{s+t}T_w \subset T_w$; hence for each i, $p^{-s}F^{s+t}T_i\subset T_i$. Now $p^{-s}F^{s+t}$ operates on T_i by $(\delta, \delta')\tau^h$, where $\delta=\alpha\cdot\alpha^{\tau}\cdots\alpha^{\tau^{h-1}}/p^s$, $\delta'=\alpha'\cdot\alpha'\cdots\alpha'^{\tau^{h-1}}/p^s$ and $h=(s+t)/g$. Then $p^{-s}F^{s+t}(\mu_i, \lambda^{m_i})=(\delta\tau^h(\mu_i), \delta'\lambda^{m_i})=\xi(\lambda^{n_i}, 0)+\eta(\mu_i, \lambda^{m_i})$ for some $\xi, \eta\in WO_{K_w}$; hence $\xi\lambda^{n_i}=\delta\tau^h(\mu_i)-\delta'\mu_i$. Now $v(\alpha)=v(\pi)/(a/g)=(gsv(p))/(s+t)$, hence $v(\delta)=0$ and $v(\delta')>0$; this implies $\mu_i=0$. Thus each T_i has a basis of the form $(\lambda^{n_i}, 0), (0, \lambda^{m_i})$ over WO_{K_w}. This shows that R_w is maximal.

(iii) The case that w is of type (2). As $K_w/\boldsymbol{Q}_p$ is an unramified extension of odd degree and $\mathrm{End}_k(A)$ is commutative, w does not split in E/K. Let v be the place of E above w. Suppose first that E_v is unramified. As $2v(\pi)=a$, a is even and hence g_v is also even. Now $FT_w=VT_w$ implies that $V^{-1}FT_w=p^{-1}F^2T_w=T_w$ and so $p^{-(a/2)}F^aT_w=T_w$. This shows that $R_w\ni p^{-(a/2)}\pi$. Since $p^{-(a/2)}\pi$ is a unit in R_w, there exists a unit u_1 in $W\otimes R_w$ with $N_{W\otimes R_w/R_w}(u_1)=p^{-(a/2)}\pi$ (cf. Prop. 7.3 and the proof of theorem 7.4 in [5], p. 554.). Put $u_2=\langle 1, p, 1, p, \cdots, 1, p\rangle \in L\otimes E_v$. Then $u_2\sigma(u_2)=p$ and $N_{L\otimes E_v/E_v}(u_1u_2)=\pi$. Now we can put $F=(u_1u_2)\sigma$. Since T_w is $W\otimes R_w$-invariant, we have $u_1T_w=T_w$. As $W\otimes R_w$ is invariant under σ, we also have that $\sigma^j(u_1)T_w=T_w (j=1, 2, \cdots.)$. As $g'=g/2$ is odd, we have

$$p^{-(g'-1)/2}F^{g'}T_w=F(p^{-1}F^2)^{(g'-1)/2}T_w=FT_w\subset T_w\,.$$

It follows, by the definition of u_1, u_2 and F, that $u_2\sigma^{g'}(T_w)\subset T_w$. As in case (ii) we have a decomposition $T_w=\bigoplus_i T_i$, corresponding to $W\otimes O_{K_w}=\bigoplus WO_{K_w}$. Here T_i is invariant under $F^{g'}$; hence $u_2\sigma^{g'}(T_i)\subset T_i$. As a WO_{K_w}-module T_i has a basis of the form $(p^{n_i}, 0), (\mu_i, p^{m_i})$ with $\mu_i=0$ or $v(\mu_i)<n_i$. $u_2\sigma^{g'}$ operates on T_i by

$$u_2\sigma^{g'}(x_1, x_{g'+1})=(x_{g'+1}, p\tau(x_1))\,, \qquad \text{for} \quad (x_1, x_{g'+1})\in T_i\,.$$

Then applying the same argument as in the proof of theorem 5.3 in [5], p. 548, we see that $\mu_i=0$; hence $T_w=\bigoplus T_i$ is invariant under the maximal order of E_v.

Suppose next E_v is ramified over K_w. Choose an $\alpha\in LE_v$ with $N_{LE_v/E_v}(\alpha)=\pi$, then we can put $F=\langle 1, \cdots, 1, \alpha\rangle\sigma$. We extend v to LE_v naturally. As $g=g_v$ is odd, we have from the assumption

$$p^{-(g-1)/2}F^gT_w=F(p^{-1}F^2)^{(g-1)/2}T_w=FT_w\subset T_w\,.$$

As $F^g=\langle\alpha, \cdots, \alpha\rangle\sigma^g$ and $v(\alpha)=g$, we see that $p^{-(g-1)/2}F^g=\langle\lambda, \cdots \lambda\rangle\sigma^g$, where $\lambda=p^{-(g-1)/2}\alpha$ and $v(\lambda)=1$. Now decompose T_w into $\oplus T_i$, corresponding to $W\otimes O_{K_w}=\oplus WO_{K_w}$. T_i is invariant under F^g and has a basis of the form p^{n_i}, $\mu_i+p^{m_i}c$ with $\mu_i\in WO_{K_w}$, $\mu_i=0$ or $w(\mu_i)<n_i$, where c is a prime element of E_v. Then we can also apply the argument in the proof of theorem 5.3 in [5] and we see that T_w is invariant under the maximal order of E_v. Therefore $R\otimes \boldsymbol{Z}_p=\oplus R_w$ is maximal and the proof is completed.

REMARK. If $R_w=\mathrm{End}_{\mathcal{A}}(T_w)$ is maximal, we can write out the condition of a base of T_w (cf. p. 545 in [5]). Hence if R_w is maximal for a place w of K, of type (3), it is easy to show, by a direct calculation, that $F^{t(w)}T_w\subset V^{s(w)}T_w$.

COROLLARY. *Let $\alpha_p=\mathrm{Spec}\, k[x]/(x^p)$ be as in [2], I. 2-11. Assume that $\hat{A}$ is isogenous to $(G_{1,0})^m+(G_{1,1})^n$ for some m, n and $a(A)(=\dim_k\mathrm{Hom}(\alpha_p, A))=n$. Assume further (*) and that for each place w of K of type (2), K_w is an unramified extension of odd degree over $\boldsymbol{Q}_p$. Then R is maximal at p. (For the property of $a(A)$, cf. [2], [3], [4].)*

Proof. Put $T=\sum T_w$, where the sum is taken over all w of type (2). Since $a(A)=\dim_k T/(F, V)T$ and $n=\dim_k T/FT=\dim_k T/VT$, we have that $(F, V)T=FT=VT$. Hence our conclusion is obvious by theorem 1.

REMARK. This corollary is a result which includes the first part of theorem 5.3 in [5], p. 548 (a result due to Shimura); assume that $R(\cong\mathrm{End}_k(A))$ is commutative and contains the maximal order of K. Assume also that p splits completely in K. Then R is maximal at p.

For, in this case, it is easy to see that $\hat{A}\sim(G_{1,0})^m+(G_{1,1})^n$ for some m, n, and, for each w of type (2), $T_w=G_{1,1}$; hence $a(T_w)=1$ and therefore $a(A)=n$.

§3. LEMMA. *Let M be a finite extension of $\boldsymbol{Q}_p$ and N be a quadratic extension of M. Let O_M and O_N be the maximal orders in M and N, respectively, and λ be a prime element of O_M. Let R be an order in O_N containing O_M. Then there exists a non-negative integer n such that $R=O_M+\lambda^n O_N$.*

Proof. Let c be an element in O_N such that $O_N=O_M[c]$. Then $R\cap cO_M=c\lambda^n O_M$ for some $n\geqq 0$. We see that

$$R=O_M+c\lambda^n O_M=O_M+\lambda^n O_N .$$

Let π be a Weil p^a-number such that its corresponding abelian varieties have commutative endomorphism rings and an isogeny type $(G_{1,0})^m+(G_{1,1})^n$, $(n>0)$ for thier formal groups. Put $E=\boldsymbol{Q}(\pi)$ and let K be the totally real subfield of E of index 2. We assume that, for each place w of K of type (2), $K_w/\boldsymbol{Q}_p$ is unramified of odd degree. (cf. the corollary of theorem 1.)

THEOREM 2. *Let π be as above. Assume, for each place w of type (2), w is ramified in E. Put $f_w=[K_w : \boldsymbol{Q}_p]$ and $g_w=(a, f_w)$. Let R be an order in O_E*

containing $O_K[\pi]$. *Then* R *is an endomorphism ring of an abelian variety corresponding to* π *if and only if, for each* w *of type* (2), R_w *contains* $O_{K_w}+p^{r_w}O_{E_v}$, *where* v *is the place of* E *with* $v|w$ *and* $r_w=(g_w-1)/2$.

Proof. By Porism 4.3 in [5] we only need to consider the situation at p. We make $V=L\otimes_{Q_p}E_p$ a $\mathcal{B}$-module as in the proof of theorem 1. The condition of R being an endomorphism ring is that there exists an $\mathcal{A}$-invariant W-lattice T in V such that $\mathrm{End}_{\mathcal{A}} T=R\otimes \boldsymbol{Z}_p$. Let T be an $\mathcal{A}$-invariant W-lattice in V such that $\mathrm{End}_{\mathcal{A}} T\supset O_K$. Then T can be decomposed as $T=\bigoplus_{w|p} T_w$. (cf. § 1) By the proof of theorem 1, $\mathrm{End}_{\mathcal{A}}(T_w)$ is maximal at each place w of type (1). Next let w be of type (2). Let c be a prime element in E_v. Then $O_{E_v}=O_{K_w}[c]$. Let α be an element in LE_v such that $N_{LE_v/E_v}(\alpha)=\pi$. Write $\alpha=d+bc$ with $b, d\in WO_{K_w}$. We see that $v(\alpha)=g_w=v(b)+1$ and $v(b)<v(d)$. Put $g=g_w$ and $r=r_w$. Then $v(b)=2r$.

Put $F=\langle 1, \cdots, 1, \alpha\rangle\sigma$ on $L\otimes_{Q_p}E_w$ with $E_w=K_w\otimes_K E=E_v$. We have a decomposition $T_w=\bigoplus_{i=1}^{g} T_i$, corresponding to the decomposition $W\otimes O_{K_w}=\bigoplus WO_{K_w}$. (cf. the proof of theorem 1) T_i are F^g-invariant WO_{K_w}-lattice in LE_v. Then, for $x\in O_{E_v}$

$$x\in \mathrm{End}_{\mathcal{A}}(T_w) \Leftrightarrow xT_i\subset T_i\,, \qquad \text{for all} \quad i.$$

Now write $\mathcal{E}(T_i)=\{x\in O_{E_v}|xT_i\subset T_i\}$. We may assume that T_i has a basis $\{1, \mu+p^m c\}$, where $\mu=0$ or $v(\mu)<0$ ($\mu\in LK_w$). Write $c^2=h_1c+h_2$ with $h_1, h_2\in O_{K_w}$. Then $v(h_1)\geqq v(h_2)=2$.

We have

$$\begin{aligned} F^g(\mu+p^m c)&=(d+bc)(\mu^\tau+p^m c)\\ &=(d\mu^\tau+bp^m h_2)+(dp^m+b\mu^\tau+bp^m h_1)c\\ &=(\delta\mu+\eta)+\delta p^m c\,, \qquad (\tau=\sigma^g)\,. \end{aligned}$$

for some δ, $\eta\in WO_{K_w}$. Hence $\delta=d+b\mu^\tau p^{-m}+bh_1$ and $\delta\mu+\eta=d\mu^\tau+bp^m h_2$. If $\mu\neq 0$ and $v(\mu)\leqq 2m$, then $v(\delta)=v(b)-2m+v(\mu)\leqq v(b)$. Hence $v(\delta\mu)<\min\{v(d\mu^\tau), v(bp^m h_2)\}$. This shows that $\delta\mu$ is integral. Therefore we have $v(b)\geqq 2m-2v(\mu)$. If $v(\mu)>2m$, then $v(\delta)\geqq v(b)+2$ and $v(bp^m h_2)<\min\{v(\delta\mu), v(d\mu^\tau)\}$. Therefore we have $v(b)\geqq -2(m+1)$. If $\mu=0$, we also have $v(b)\geqq -2(m+1)$. On the other hand, we have the following; if $v(\mu)\leqq 2m$, $\mathcal{E}(T_i)=O_{K_w}+p^{m-v(\mu)}O_{E_v}$ and if $v(\mu)>2m$ or $\mu=0$, then $\mathcal{E}(T_i)=O_{K_w}+p^{-m-1}O_{E_v}$. As this will be proved by direct computation with almost the same argument as above, we omit its proof. Consequently, we have $\mathcal{E}(T_i)\supset O_{K_w}+p^r O_{E_v}$. Hence $\mathrm{End}_{\mathcal{A}}(T_w)=\bigcap_i \mathcal{E}(T_i)\supset O_{K_w}+p^r O_{E_v}$.

Now let $S=O_{K_w}+p^t O_{E_v}(t\leqq r)$ be an order in O_{E_v} containing $O_{K_w}+p^r O_{E_v}$. Then $WS=WO_{K_w}+p^t WO_{E_v}$ in LE_v. Put $T_{r+1-s}=WO_{K_w}+p^{t-s}WO_{E_v}$ and $T_{r+1+s}=p^s T_{r+1-s}$ for $0\leqq s\leqq r$. Here we consider that $T_{r+1-s}=WO_{E_v}$ if $t\leqq s$. Let $T=\bigoplus_{i=1}^{g} T_i$ in

$L\otimes E_w=\oplus LE_v$. For $\langle x_1, x_2, \cdots, x_g\rangle\in T$ with $x_i\in T_i (i=1, \cdots, g)$, we have

$$F\langle x_1, x_2, \cdots, x_g\rangle=\langle x_2, x_3, \cdots, x_g, \alpha x_1^{\tau}\rangle$$

and

$$V\langle x_1, x_2, \cdots, x_g\rangle=\langle p(\alpha^{-1}x_g)^{\tau^{-1}}, px_1, \cdots, px_{g-1}\rangle .$$

Now we have the following relations;

$$T_1\supset T_2\supset \cdots \supset T_{g-1}\supset T_g\supset\alpha T_1,\quad pT_1\subset T_2,\quad pT_2\subset T_3, \cdots,$$

$$pT_g\subset\alpha T_1,\quad T_1=WO_{E_v} \text{ and } T_i^{\tau}=T_i \text{ for all } i.$$

It is easy to see that T is $\mathcal{A}$-invariant and $\mathrm{End}_{\mathcal{A}} T=S$. Our assertion now follows immediately from these facts.

PROPOSITION 1. *Let π be as stated just before theorem 2. Let A be an abelian variety corresponding to π such that $R=\mathrm{End}_k(A)$ contains O_K. Let w be of type (2) such that w is unramified in E. Then the localization R_w of R at w contains $O_{K_w}+p^{g-1}O_{E_v}$, where $g=([K_w : Q_p], a)$.*

Proof. Let $\langle\rho\rangle=\mathrm{Gal}(E_v/K_w)$ and $T=T_pA$. Let T_w, T_i, α, $\mathcal{E}(T_i)$ be as in the proof of theorem 2. Then $R_w=\mathrm{End}_{\mathcal{A}} T_w$. T_i are $W[F^g, V^g]$-invariant, WO_{K_w}-lattice in $LK_w\otimes_K E$. Let $(p^n, 0)$, (μ, p^m) be a WO_{K_w}-basis of T_i, where $\mu=0$ or $v(\mu)<n$. $\mu=0$ implies that $\mathcal{E}(T_i)$ is maximal. Suppose $\mu\neq 0$. We have

$$F^g(\mu, p^m)=(1, \alpha)\tau(\mu, p^m)=(p^m, \mu^{\tau}\alpha)$$
$$=\delta(p^n, 0)+\eta(\mu, p^m)=(\delta p^n+\eta\mu, \eta^{\tau}p^m)$$

for some $\delta, \eta\in WO_{K_w}$. $(\tau=\sigma^g)$ Therefore $p^m=\delta p^n+p^{-m}\alpha^{\tau^{-1}}\mu^2$. If $n>m$, then $m=-m+2v(\mu)+v(\alpha)$. As $v(\alpha)=g$ is odd, we must have $n\leqq m$. Then $p^{m-n}=\delta+p^{-m-n}\alpha^{\tau^{-1}}\mu^2$ shows that $v(\alpha)\geqq m+n-2v(\mu)>n-v(\mu)$. On the other hand, for $x\in O_{E_v}$

$$xT_i\subset T_i \Leftrightarrow (x\mu, xp^m)=(\delta p^n+\eta\mu, \eta^{\tau}p^m)$$
$$\text{for some } \delta, \eta\in WO_{K_w}.$$
$$\Leftrightarrow v(x-x^{\rho})\geqq n-v(\mu)$$
$$\Leftrightarrow x\in O_{K_w}+p^{n-v(\mu)}O_{E_v}.$$

Therefore $\mathcal{E}(T_i)=O_{K_w}+p^{n-v(\mu)}O_{E_v}\supset O_{K_w}+p^{g-1}O_{E_v}$; as $R_w=\bigcap_i\mathcal{E}(T_i)$, this completes our proof.

COROLLARY. *Let π be as above. If, for each w of type (2), a and $[K_w : \boldsymbol{Q}_p]$ are relatively prime, then $R=\mathrm{End}_k(A)$ containing O_K is maximal at p.*

This follows at once from theorem 2 and proposition 1.

REMARK. This corollary also contains theorem 5.3 in [5]. For, in that case, $[K_w : \boldsymbol{Q}_p]=1$ for all w.

EXAMPLE. Let β be a root of $f(x)=4x^4+13x^3-20x-8=0$. $f(x)$ has four real roots in the interval $(-2\sqrt{2}, 2\sqrt{2})$. $4^3f(x)=(4x)^4+13(4x)^3-20\times 4^2(4x)-8\times 4^3$ shows that $f(x)$ has a root $\xi/4$ in $\boldsymbol{Q}_2$ with a unit ξ in $\boldsymbol{Q}_2$. Put $g(x)=f(x)/(4x-\xi)$. Then $g(x)\in\boldsymbol{Z}_2[x]$ and $(1/2^3)g(2x)\equiv x^3+x+1 \pmod 2$. This shows that $g(x)$ is irreducible over $\boldsymbol{Q}_2$ and has a root in the cubic unramified extension of $\boldsymbol{Q}_2$. Since $f(x)\equiv 0 \pmod 7$ has no root in $\boldsymbol{Z}/7\boldsymbol{Z}$, we see that $f(x)$ is irreducible over $\boldsymbol{Q}$. Therefore there are two places w_1, w_2 above 2 in $K=\boldsymbol{Q}(\beta)$ giving $w_1(\beta)=-2$ and $w_2(\beta)=1$. We have $K_{w_1}=\boldsymbol{Q}_2$ and K_{w_2} is the cubic unramified extension of $\boldsymbol{Q}_2$. Let π be a root of $x^2-4\beta x+2^5=0$. π is a Weil 2^5-number. w_1 splits in $E=\boldsymbol{Q}(\pi)$ and, since $(x/4)^2-\beta(x/4)+2$ is Eisenstein in K_{w_2}, w_2 is ramified in E. π has a formal structure $G_{1,0}+(G_{1,1})^3$ and a commutative endomorphism algebra. So π satisfies the condition of the above corollary. Therefore an endomorphism ring containing O_K is maximal at p.

For a supersingular abelian variety A over k (i. e. $\hat{A}\sim(G_{1,1})^m$ with $m=\dim(A)$, cf. [4]), we have the following:

PROPOSITION 2. *Let a be even and put $a'=a/2$. Let A be a simple supersingular abelian variety over k such that $R(\cong\mathrm{End}_k(A))$ is commutative. Assume that $F^{a'}T_pA=V^{a'}T_pA$. Then R is maximal at p.*

Proof. Let π be the Weil number of A over k. Then $\pi=p^{a'}\zeta$, where ζ is a n-th root of 1 for some n. Since $V^{-a'}F^{a'}=p^{-a'}F^{a}=p^{-a'}\pi=\zeta$, we have $\zeta T_pA=T_pA$. In $E\otimes\boldsymbol{Q}_p$, $\zeta\in E=Q(\pi)$ generates the maximal order over $\boldsymbol{Z}_p$. Therfore R is maximal at p.

REFERENCES

[1] MANIN, YU. I., The theory of commutative formal groups over fields of finite characteristic, Russian Math. Surv. **18** (6) (1963) 1-83.

[2] OORT, F., Commutative group schemes, Lect. N. Math. **15**, Springer-Verlag (1966).

[3] OORT, F., Isogenies of formal groups, Proc. Konin. Neder. Akad. Wet. **78** (1975) 391-400.

[4] OORT, F., Which surfaces are products of elliptic curves?, Math. Ann. **214** (1975) 35-47.

[5] WATERHOUSE, W. C., Abelian varieties over finite fields, Ann. scient. Éc. Norm. Sup. **2** (1969) 521-560.

DEPARTMENT OF MATHEMATICS,
COLLEGE OF GENERAL EDUCATION,
TÔHOKU UNIVERSITY