Korean J. Math. **30** (2022), No. 3, pp. 555–560
http://dx.doi.org/10.11568/kjm.2022.30.3.555

RESTRICTION OF SCALARS WITH SIMPLE ENDOMORPHISM ALGEBRA

Hoseog Yu

Abstract. Suppose L/K be a finite abelian extension of number fields of odd degree and suppose an abelian variety A defined over L is a K-variety. If the endomorphism algebra of A/L is a field F, the followings are equivalent :
(1) The enodomorphiam algebra of the restriction of scalars from L to K is simple.
(2) There is no proper subfield of L containing L^{G_F} on which A has a K-variety descent.

1. Introduction

Let K be a number field and L be a finite abelian extension of K of odd degree with Galois group $G = Gal(L/K)$. Let A be an abelian variety defined over L whose endomorphism ring is denoted by $\mathrm{End}_L(A)$. Assume the endomorphism algebra $\mathrm{End}_L(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ is a field. Denote $\mathrm{End}_L(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ by F. We suppose that A is a K-variety, that is, for each $\sigma \in G$, $\sigma(A)$ is L-isogenous to A. Write $Res_{L/K}(A)$ together with a morphism $\phi\colon Res_{L/K}(A) \to A$ for the restriction of scalars of A from L to K. For the definitions and properties of the restriction of scalars, see [4, p.5] or [5, p.68]. We will prove the following main theorem.

Main Theorem. *The followings are equivalent.*

1. $Res_{L/K}(A)$ *is* K*-isogenous to a product* $B \times \cdots \times B$ *of a simple abelian variety* B *defined over* K.
2. *There is no proper subfield of* L *containing* L^{G_F} *on which* A *has a* K*-variety descent.*

Proof of Main Theorem will be given after Lemma 6.

In [1, §15] and [3], there are some corollaries of this theorem when A is an elliptic curve.

2. Simple algebra and descent

From the assumption that A is a K-variety, for each $\sigma \in G$, there is a L-isogeny $f_\sigma\colon \sigma(A) \to A$.

Received February 18, 2022. Revised August 23, 2022. Accepted September 19, 2022.
2010 Mathematics Subject Classification: 14K05, 14K02.
Key words and phrases: restriction of scalars, descent, isogeny.

For $b \in \mathrm{End}_L(A)$, we define $\widetilde{b} \in \mathrm{End}_K(Res_{L/K}(A))$ satisfying $\phi \circ \widetilde{b} = b \circ \phi$. From the universal mapping property of restriction of scalars, the existence and the uniqueness of $\widetilde{b}$ for $b \in \mathrm{End}_L(A)$ is obvious (see [4, p.5]). For details, see [5, Definition 4 in p.72]. For each $\sigma \in G$, define $u_\sigma \in \mathrm{End}_K(Res_{L/K}(A))$ such that $\phi \circ u_\sigma = f_\sigma \circ \sigma(\phi)$. There is a similar definition in [5, Definition 1 in p.68]. Then the morphism u_σ exists and is unique when the isogeny $f_\sigma \colon \sigma(A) \to A$ is given.

Define $\widetilde{F} = \left\{\widetilde{b} \in \mathrm{End}_K(Res_{L/K}(A)) \,|\, b \in \mathrm{End}_L(A)\right\} \otimes_{\mathbf{Z}} \mathbf{Q}$. Now we define the action of G on $\widetilde{F}$. Because f_σ is an isogeny, there is a dual isogeny morphism $f_\sigma^\vee \colon A \to \sigma(A)$ such that $f_\sigma \circ f_\sigma^\vee$ is multiplication by $\deg(f_\sigma)$. Now for $b \in F$ there are a positive integer m and $b_0 \in \mathrm{End}_L(A)$ such that $b = b_0 \otimes \frac{1}{m}$. We define ${}^\sigma\widetilde{b} = (f_\sigma \circ \sigma(b_0) \circ f_\sigma^\vee)^\sim \otimes \frac{1}{m \cdot \deg(f_\sigma)}$. It is clear that this action of G on $\widetilde{F}$ is independent of the choice of f_σ. We can check that $u_\sigma \circ \widetilde{b} = {}^\sigma\widetilde{b} \circ u_\sigma$ for $b \in F$.

We define $\alpha(\sigma, \tau) = u_\sigma \circ u_\tau \circ u_{\sigma\tau}^{-1} \in \widetilde{F}^\times$ for $\sigma, \tau \in G$. Then α is a 2-cocycle from G to $\widetilde{F}^\times$. Define

$$\widetilde{F}^\alpha G = \left\{ \sum_{\sigma \in G} \widetilde{a_\sigma} \circ u_\sigma \in \mathrm{End}_K(Res_{L/K}(A)) \otimes_{\mathbf{Z}} \mathbf{Q} \;\middle|\; a_\sigma \in F \right\}.$$

From $\tilde{a} \circ u_\sigma \circ \tilde{b} \circ u_\tau = \tilde{a} \circ {}^\sigma\tilde{b} \circ u_\sigma \circ u_\tau = \tilde{a} \circ {}^\sigma\tilde{b} \circ \alpha(\sigma,\tau) \circ u_{\sigma\tau}$ for $a, b \in F$ and for $\sigma, \tau \in G$, we can show that $\widetilde{F}^\alpha G$ is a twisted group ring.

Theorem 1. *We get* $\mathrm{End}_K(Res_{L/K}(A)) \otimes_{\mathbf{Z}} \mathbf{Q} = \widetilde{F}^\alpha G$.

Proof. Let $\iota_\tau \colon \tau(A) \to \prod_{\sigma \in G} \sigma(A)$ denote the inclusion map into the τ-th component. Define the isomorphism $\Phi \colon \prod_\sigma \sigma(A) \to Res_{L/K}(A)$ to be the the inverse morphism of $\prod_\sigma \sigma(\phi) \colon Res_{L/K}(A) \to \prod_\sigma \sigma(A)$. For $\beta \in \mathrm{End}_K(Res_{L/K}(A)) \otimes_{\mathbf{Z}} \mathbf{Q}$, define $b_\sigma \in F$ by $b_\sigma = \phi \circ \beta \circ \Phi \circ \iota_\sigma \circ f_\sigma^{-1}$. Note that

$$\phi \circ \sum_\sigma \widetilde{b_\sigma} \circ u_\sigma = \sum_\sigma b_\sigma \circ f_\sigma \circ \sigma(\phi) = \sum_\sigma (\phi \circ \beta \circ \Phi \circ \iota_\sigma \circ f_\sigma^{-1}) \circ f_\sigma \circ \sigma(\phi) = \phi \circ \beta.$$

Thus $\beta = \sum_\sigma \widetilde{b_\sigma} \circ u_\sigma$ and $\mathrm{End}_K(Res_{L/K}(A)) \otimes_{\mathbf{Z}} \mathbf{Q} \subseteq \widetilde{F}^\alpha G$. Then the theorem follows. □

Define the isotropy subgroup of G by $G_F = \{\sigma \in G \,|\, {}^\sigma\widetilde{b} = \widetilde{b} \text{ for } b \in F\}$. Define G_r by $\{\sigma \in G_F \,|\, \text{There is } a_\sigma \in \mathrm{End}_L(A)^\times \text{ such that } u_\tau \circ (\widetilde{a_\sigma} \circ u_\sigma) = (\widetilde{a_\sigma} \circ u_\sigma) \circ u_\tau \text{ for } \tau \in G\}$. Then we replace f_σ with $a_\sigma \circ f_\sigma$ for $\sigma \in G_r$ to define new u_σ's. With these newly defined u_σ's,

$$G_r = \{\sigma \in G_F \,|\, u_\tau \circ u_\sigma = u_\sigma \circ u_\tau \text{ for } \tau \in G\}.$$

Note that the endomorphism algebra $\widetilde{F}^\alpha G = \mathrm{End}_K(Res_{L/K}(A)) \otimes_{\mathbf{Z}} \mathbf{Q}$ is semisimple (see [2]) and the center of $\widetilde{F}^\alpha G$ is $(\widetilde{F}^G)^\alpha G_r$. Thus $\widetilde{F}^\alpha G$ is simple if and only if $(\widetilde{F}^G)^\alpha G_r$ is a field.

Theorem 2. *The center $(\widetilde{F}^G)^\alpha G_r$ of $\widetilde{F}^\alpha G$ is a field if and only if $(\widetilde{F}^G)^\alpha H$ is a field for any prime order subgroup H of G_r.*

Proof. It is clear from the following lemma. □

Lemma 3. *Let a finite abelian group G act on a number field M trivially. Define $\mathfrak{H} = \{H \le G \,|\, H$ is a group of prime order.$\}$. Let α be a 2-cocycle from G to $M^\times$. Assume that the twisted group ring $M^\alpha G$ is commutative and $M^\alpha H$ is a field for $H \in \mathfrak{H}$. Then $M^\alpha G$ is a field.*

Proof. With Sylow p-subgroups G_p of G, we get $G = \oplus_p G_p$. From section 3, $M^\alpha G_p$ is a field. Because $M^\alpha G \cong \otimes_p M^\alpha G_p$, $M^\alpha G$ is a field. □

Definition 4. An abelian variety A defined over L has a K-variety descent if there are a proper subfield L_0 of L containing L^{G_F} and an abelian variety A_0 defined over L_0 such that A_0 is L-isogenous to A and A_0 is a K-variety, that is, $\sigma(A_0)$ is L_0-isogenous to A_0 for $\sigma \in G$.

Theorem 5. *Let a subgroup H of G_r be of prime order p. Then $(\widetilde{F}^G)^\alpha H$ is a field if and only if A doesn't have a K-variety descent to L^H.*

Proof. Assume A has a K-variety descent to L^H. Then $(\widetilde{F}^G)^\alpha H \cong F^G[x]/\langle x^p - 1\rangle$. Therefore, $(\widetilde{F}^G)^\alpha H$ is not a field.

Suppose that $(\widetilde{F}^G)^\alpha H$ is not a field. Let $\sigma \in H$ be a generator. Define $f_{\sigma^i} = f_{\sigma^{i-1}} \circ \sigma^{i-1}(f_\sigma)$ for $2 \le i \le p$. Then $u_{\sigma^i} = u_\sigma^i$ for $1 \le i \le p$ and $u_\sigma^p \in \widetilde{F}^G$. If $x^p - u_\sigma^p$ is irreducible in $\widetilde{F}^G[x]$, $(\widetilde{F}^G)^\alpha H$ is a field. Thus $x^p - u_\sigma^p$ is reducible in $\widetilde{F}^G[x]$ and there is $a_\sigma \in F$ such that $\widetilde{a_\sigma} \in \widetilde{F}^G$ and $u_\sigma^p = \widetilde{a_\sigma}^p$. Define $g_\sigma = a_\sigma^{-1} \circ f_\sigma \colon \sigma(A) \to A$.

Let $Res_{L/L^H}(A)$ be the restriction of scalars of A from L to L^H with a morphism $\psi\colon Res_{L/L^H}(A) \to A$. Define $w_\sigma \in \mathrm{End}_{L^H}(Res_{L/L^H}(A)) \otimes_{\mathbf{Z}} \mathbf{Q}$ such that $\psi \circ w_\sigma = g_\sigma \circ \sigma(\psi)$.

Define $B = \left(\sum_{i=0}^{p-1} w_\sigma^i\right) Res_{L/L^H}(A)$. Then ψ is a morphism from B to A. By restricting the domain of ψ to B, we get $g_\sigma \circ \sigma(\psi) = \psi$ because $g_\sigma \circ \sigma(\psi) \circ \left(\sum_{i=0}^{p-1} w_\sigma^i\right) = \psi \circ w_\sigma \circ \left(\sum_{i=0}^{p-1} w_\sigma^i\right) = \psi \circ \left(\sum_{i=0}^{p-1} w_\sigma^i\right)$.

Define $\widetilde{\psi}\colon Res_{L/K}(B) \to Res_{L/K}(A)$ by $\phi \circ \widetilde{\psi} = \psi \circ \phi_B$ with the morphism $\phi_B\colon Res_{L/K}(B) \to B$. We know that $u_\tau \circ u_\sigma = u_\sigma \circ u_\tau$ for $\tau \in G$ and $\sigma \in G_r$. Thus $u_\tau \circ (\widetilde{a_\sigma}^{-1} \circ u_\sigma) = (\widetilde{a_\sigma}^{-1} \circ u_\sigma) \circ u_\tau$ for $\tau \in G$ and $\sigma \in G_r$.

Then $\widetilde{\psi}^{-1} \circ u_\tau \circ u_\sigma \circ \widetilde{\psi} = \widetilde{\psi}^{-1} \circ u_\sigma \circ u_\tau \circ \widetilde{\psi}$. Note $\phi_B \circ \widetilde{\psi}^{-1} \circ u_\tau \circ u_\sigma \circ \widetilde{\psi} = \psi^{-1} \circ f_\tau \circ x(\psi) \circ (\tau\sigma)(\phi_B)$ and $\phi_B \circ \widetilde{\psi}^{-1} \circ u_\sigma \circ u_\tau \circ \widetilde{\psi} = \sigma(\psi^{-1} \circ f_\tau \circ \tau(\psi)) \circ (\sigma\tau)(\phi_B)$. Then $\sigma(\psi^{-1} \circ f_\tau \circ \tau(\psi)) = \psi^{-1} \circ f_\tau \circ \tau(\psi)\colon \tau(B) \to B$. That is $\psi^{-1} \circ f_\tau \circ \tau(\psi)$ is defined over L^H. □

Lemma 6. *Suppose that A has a K-variety descent on L^H for a subgroup H of G_F. Then $H \le G_r$.*

Proof. We may assume that the abelian varity A is defined over L^H and for $\sigma \in G$, $\sigma(A)$ is L^H-isogenous to A. We can assume $f_\theta = id_A$ for $\theta \in H$. Pick $\theta \in H$ and $\tau \in G$. Note that $\theta(f_\tau) = f_\tau$. Now $\phi \circ u_\tau \circ u_\theta = f_\tau \circ (\tau\theta)(\phi)$ and $\phi \circ u_\theta \circ u_\tau = f_\tau \circ (\theta\tau)(\phi)$. Since G is abelian, $u_\tau \circ u_\theta = u_\theta \circ u_\tau$. Thus $\theta \in G_r$ and $H \le G_r$. □

Proof of Main Theorem. *The following equivalences prove Main Theorem. $Res_{L/K}(A)$ is K-isogenous to a product $B \times \cdots \times B$ of a simple abelian variety B defined over K.*

$\Updownarrow$

$\widetilde{F}^\alpha G$ is simple.

$\Updownarrow$ *by the statement after* THEOREM 1
$(\widetilde{F^G})^\alpha G_r$ *is a field.*
$\Updownarrow$ *by* THEOREM 2
$(\widetilde{F^G})^\alpha H$ *is a field for any prime order subgroup* H *of* G_r.
$\Updownarrow$ *by* THEOREM 5
A doesn't have a K*-variety descent to* L^H *for any prime order subgroup* H *of* G_r.
$\Updownarrow$ *by* LEMMA 6
There is no proper subfield of L *containing* L^{G_F} *on which* A *has a* K*-variety descent.*
□

COROLLARY 7. *Let* K *be finite Galois extension over* $\mathbf{Q}$ *which is a primitive totally complex. Let* L *be an abelian extension of* K *and let* A *be an abelian variety defined over* L*. We assume that* L *is the field of moduli and that* A *is a* K*-variety, that is, for each* $\sigma \in Gal(L/K)$, $\sigma(A)$ *and* A *are* L*-isogenous. Assume that there is no* K*-variety descent of* A *on* M *such that* $K \leq M \lneqq L$*. Then* $Res_{L/K}(A)$ *has only one simple factor up to isogeny over* K*, that is, the endomorphism algebra* $\mathrm{End}_K(Res_{L/K}(A)) \otimes_{\mathbf{Z}} \mathbf{Q}$ *is simple.*

THEOREM 8. [3] *Let* E *be an elliptic curve such that* $F = \mathrm{End}^0(E)$ *is a quadratic imaginary number field. Let* j *be the* j*-invariant of* E*. Assume that* E *is defined over the Hilbert class field* $F(j)$ *of* F *and* $F = \mathrm{End}^0_{F(j)}(E)$*. Assume that* E *is an* F*-curve. Then* $Res_{F(j)/F}(E)$ *has only one simple factor.*

Proof. It is well-known that there is no descent of E to a proper subfield of $F(j)$. From the above corollary, the theorem follows. □

Assume that G acts trivially on F. Define $\beta(\sigma,\tau) = \alpha(\sigma,\tau)/\alpha(\tau,\sigma)$. We can show that β is a bilinear antisymmetric pairing from $G \times G$ to μ_F, where μ_F is the set of roots of unity in F. Then it is easy to show that $\beta(G_r, G) = \beta(G, G_r) = 1$. Moreover, the induced pairing from $G/G_r \times G/G_r$ to μ_F is non-degenerate bilinear antisymmetric. In the theorem of Nakamura, we know that if the class number of F is not 1, then $\mu_F = \{\pm 1\}$. Therefore, $G/G_r \cong (\mathbf{Z}/2\mathbf{Z})^m \oplus (\mathbf{Z}/2\mathbf{Z})^m$. Then $F^\alpha G \cong (F^\alpha G_r)^\alpha (G/G_r)$. Denote by D_i central simple quaternion algebra with center $F^\alpha G_r$. Then $F^\alpha G \cong D_1 \otimes \cdots \otimes D_m$. Now $F^\alpha G \cong M_{2^m}(F^\alpha G_r)$ or $F^\alpha G \cong M_{2^{m-1}}(D)$, where D is a central simple quaternion algebra with center $F^\alpha G_r$.

THEOREM 9. *[1, §15] Let* E *be an elliptic curve such that* $F = \mathrm{End}^0(E)$ *is a quadratic imaginary number field. Let* j *be the* j*-invariant of* E*. Assume that* E *is defined over* $\mathbf{Q}(j)$ *and* $F = \mathrm{End}^0_{F(j)}(E)$*. Assume that* E *is a* $\mathbf{Q}$*-curve and* $[\mathbf{Q}(j)\colon \mathbf{Q}]$ *is odd. Then* $Res_{\mathbf{Q}(j)/\mathbf{Q}}(E)$ *is simple.*

Proof. In a similar way, we can show that $Res_{\mathbf{Q}(j)/\mathbf{Q}}(E)$ has only one simple factor. Since $[G\colon G_r]$ is odd, $G = G_r$. Therefore, $F^\alpha G$ is a field. Then $Res_{\mathbf{Q}(j)/\mathbf{Q}}(E)$ is simple. □

3. Lemmas

Assume that G is a finite abelian p-group with an odd prime p. The group G acts on a number field M trivially. With a 2-cocycle α from G to $M^\times$, we assume that the twisted group ring $M^\alpha G = \{\sum_\sigma a_\sigma u_\sigma \mid a_\sigma \in M \text{ and } \sigma \in G\}$ is commutative. Assume that for any cyclic subgroup H of G of order p, $M^\alpha H$ is a field.

Lemma 10. *Let $\gamma \in \mathbf{C}$ be a root of a polynomial $x^{p^2} - a \in M[x]$ such that $[M(\gamma)\colon M] = p$. Then $M(\gamma^p) = M$.*

Proof. We assume that $M(\gamma^p) = M(\gamma)$. Then $[M(\gamma^p, \zeta_p)\colon M(\zeta_p)] = p$ with a primitive p-th root of unity ζ_p. Now we choose a generator δ in $Gal(M(\gamma^p, \zeta_p)/M(\zeta_p))$ such that $\delta(\gamma^p) = \gamma^p\zeta_p$. Thus $\eta = \delta(\gamma)\gamma^{-1} \in M(\gamma^p, \zeta_p)$ is a primitive p^2-th root of unity. Then $\delta(\eta) = \eta^k$ with $k \equiv 1 \pmod p$. Now $\gamma = \delta^p(\gamma) = \gamma\eta^p$, which is impossible. Therefore, $M \subseteq M(\gamma^p) \subsetneq M(\gamma)$. □

Lemma 11. *Assume that $\alpha \in \mathbf{C}$ is a solution of an irreducible polynomial $x^p - d \in M[x]$. If $e^p \in M$ for $e \in M(\alpha)$, then $e = b\alpha^t$ with $b \in M$ and an integer t $(0 \le t \le p-1)$.*

Proof. Note that $[M(\alpha) : M] = p$. With a p-th root of unity ζ_p, we know $[M(\alpha, \zeta_p) : M(\zeta_p)] = p$. Write $e = \sum_{i=0}^{p-1} e_i\alpha^i$ with $e_i \in M$. Let δ be a generator of $Gal(M(\alpha, \zeta_p)/M(\zeta_p))$ such that $\delta(\alpha) = \zeta_p\alpha$. Because $e^p \in M$, $\delta(e) = e\zeta_p^t$ for an integer t $(0 \le t \le p-1)$. Thus from $\sum_{i=0}^{p-1} e_i(\alpha\zeta_p)^i = \sum_{i=0}^{p-1} e_i\alpha^i\zeta_p^t$, we get $e = e_t\alpha^t$. □

Lemma 12. *Assume that for a subgroup J of G, $M^\alpha J$ is a field. For a positive integer m and $a \in M^\alpha J$, if $a^{p^m} \in M$, then $a = cu_\sigma$ with $c \in M$ and $\sigma \in J$.*

Proof. Let $J = J_0 \oplus \mathbf{Z}/p^n\mathbf{Z}$. Assume that the lemma is true for $M^\alpha J_0$. Let $M_1 = M^\alpha J_0$.

Assume that $m = 1$ and that the lemma is true for $M_1^\alpha J_1$ where $J_1 = p\mathbf{Z}/p^n\mathbf{Z}$. With a generator τ of $\mathbf{Z}/p^n\mathbf{Z}$, $M_1^\alpha(\mathbf{Z}/p^n\mathbf{Z}) = M_1^\alpha J_1(u_\tau)$ and $[M_1^\alpha J_1(u_\tau) : M_1^\alpha J_1] = p$. From the previous lemma, we get $a = a_t u_\tau^t$ with $a_t \in M_1^\alpha J_1$ and a nonnegative integer t.

Assume $n \ge 2$. Let $J_2 = p^2\mathbf{Z}/p^n\mathbf{Z}$. Assuming $t \ne 0$, then $a_t^p \notin M_1^\alpha J_2$ but $a_t^{p^2} \in M^\alpha J_2$. Then we get $M_1^\alpha J_1 = M_1^\alpha J_2(a_t) = M_1^\alpha J_2(a_t^p)$ and $[M_1^\alpha J_2(a_t)\colon M_1^\alpha J_2] = p$. From Lemma 10, it is not possible. Therefore, $n = 1$ and $u_\tau^p \in M$. Since $a_t \in M_1$ and $a_t^p \in M$, $a_t = cu_\sigma$ with $c \in M$ and $\sigma \in J_0$. Thus for $m = 1$ the lemma is true.

Assume that the lemma is true for $m = k$, that is, if $a^{p^k} \in M_1$, then $a = a_t u_\sigma$ where $a_t \in M_1$ and $\sigma \in \mathbf{Z}/p^n\mathbf{Z}$. Assume $a^{p^{k+1}} \in M_1$. Then $a^p = bu_\sigma$ with $b \in M_1$ and $\sigma \in \mathbf{Z}/p^n\mathbf{Z}$. If σ is a generator of $\mathbf{Z}/p^n\mathbf{Z}$, then $a^p \notin M_1^\alpha(p\mathbf{Z}/p^n\mathbf{Z})$ but $a^{p^2} = b^p u_\sigma^p \in M_1^\alpha(p\mathbf{Z}/p^n\mathbf{Z})$. From Lemma 10 it is impossible. Therefore, σ is not a generator of $\mathbf{Z}/p^n\mathbf{Z}$. Thus from Lemma 11 $a = cu_\tau$ such that $c \in M_1(u_\sigma)$ and $\tau^p = \sigma$. Note that $c^p \in M_1$. Thus there are $\delta \in <\sigma>$ and $c_1 \in M_1$ such that $c = c_1u_\delta$. We know $c_1^{p^{k+1}} \in M$. Thus $a = du_\gamma u_\delta u_\tau$. We prove the lemma. □

Lemma 13. *Let a finite abelian p-group G act on a number field M trivially. Let α be a 2-cocycle in $Z^2(G, M^\times)$. Assume that $M^\alpha G$ is commutative and for any subgroup H of G of order p, $M^\alpha H$ is a field. Then $M^\alpha G$ is a field.*

Proof. We will prove this by induction. Let $J = J_0 \oplus \mathbf{Z}/p^n\mathbf{Z}$ be a subgroup of G and τ be a generator for $\mathbf{Z}/p^n\mathbf{Z}$. Let $J_1 = J_0 \oplus p\mathbf{Z}/p^n\mathbf{Z}$. Assume that $M^\alpha J_1$ is a field and $M^\alpha J$ is not a field. Since $u_\tau^p \in M^\alpha J_1$, we know that $x^p - u_\tau^p \in M^\alpha J_1[x]$ is reducible. Then there is a solution $b \in M^\alpha J_1$ of $x^p - u_\tau^p = 0$. Since $b^{p^n} = u_\tau^{p^n} \in M$, by Lemma 12, we get $b = cu_\sigma$ with $\sigma \in J_1$. Note that $(u_\tau u_\sigma^{-1})^p = u_\tau^p u_\sigma^{-p} = b^p u_\sigma^{-p} = c^p$. Then $\tau^p = \sigma^p$ and $M^\alpha \langle \tau\sigma^{-1} \rangle$ is not a field, which contradicts the assumption. □

References

[1] B. H. Gross, *Arithmetic on Elliptic Curves with Complex Multiplications*, Lecture Notes in Math. **776**, Springer, 1980.
[2] E. Kani and M. Rosen, *Idempotent relations and factors of Jacobians*, Math. Ann. **284** (1989) 307–327.
[3] T. Nakamura, *On abelian varieties associated with elliptic curves with complex multiplications*, Acta Arith. **97** (2001), no. 4, 379–385.
[4] A. Weil, *Adeles and algebraic groups*, Progr. Math. **23** (1982).
[5] H. Yu, *Idempotent relations and the conjecture of Birch and Swinnerton-Dyer*, Math. Ann. **327** (2003) 67–78.

Hoseog Yu
Department of Mathematics and Statistics, Sejong University,
Seoul 05006, Korea
E-mail: hsyu@sejong.edu