ON THE FIELD EXTENSION BY COMPLEX MULTIPLICATION

BY
TOMIO KUBOTA[1]

An abelian variety A with sufficiently many complex multiplications determines over a certain algebraic number field F an abelian extension K_c, namely, the union of all extensions corresponding to ideal sections of A in the sense of the theory of complex multiplication. If we observe K_c as a subfield of the maximal abelian extension K_a of F, there arises a problem to investigate which part of K_a is covered by K_c. In the classical case where A is an elliptic curve, it is known that $K_a = K_c$, and there is also a result obtained in [4] for the general case.

In the present paper, we shall define for any abelian extension K over F and for any prime number l the l-dimension $\dim_l(K/F)$ of K/F, and show that $\dim_l(K_c/F)$ is, for every l, equal to a very simple invariant which we shall call the rank of A and denote by rank A. The rank of A depends only on an elementary, group theoretical property of the CM-type to which A belongs, and $\operatorname{rank} A \leqq \dim A + 1$. After the proof of this main result, we shall give an example of nondegenerate abelian variety, i.e., an abelian variety with $\operatorname{rank} A = \dim A + 1$. Such an example is given by the Jacobian variety of a hyperelliptic curve of Fermat type. At the end of the paper, we shall add a remark that $\dim_l(K_a/F) = \dim_l(K_c/F)$ holds for some special cases where, among others, a condition about the unit group of F with respect to l is satisfied. This fact suggests that, in many cases, a large part of the maximal abelian extension is obtained by complex multiplication.

1. **Preliminaries.** First of all, we propose to summarize some results about infinite abelian groups. (For details, see [1].) We denote by l a prime number, and by $\boldsymbol{Q}_l$ [resp. $\boldsymbol{Z}_l$] the rational l-adic field [resp. the ring of l-adic integers]. A discrete abelian group X is called a torsion group if every element of X has a finite order, and X is called an l-group if every element of X has a finite order which is a power of l. An element x of an abelian l-group is called divisible if there exists an element $y \in X$ with $x = y^{l^m}$ for any power l^m of l. If every element of X is divisible, X is called divisible. The union X_∞ of all divisible subgroups of an abelian l-group X is also a divisible subgroup of X, which is called the maximal divisible subgroup of X. The character group $\operatorname{char} X_\infty$ of X_∞ becomes in an obvious way a torsion free $\boldsymbol{Z}_l$ module. If $\operatorname{char} X_\infty$ is finitely generated over $\boldsymbol{Z}_l$, we call the dimension

Received by the editors January 29, 1964.
(1) Supported in part by U. S. Army Research Office.

of char X_∞ over $\boldsymbol{Z}_l$ the dimension of X, and denote it by $\dim X$. Let X, X_1, X_2 be three abelian l-groups with finite dimensions. Then the exactness of

$$0 \to X_1 \to X \to X_2 \to 0$$

implies

$$\dim X = \dim X_1 + \dim X_2 \tag{1}$$

whenever one of the following two conditions is satisfied: (i) either X_1 or X_2 is a finite group; (ii) X_1 is divisible.

If X is a torsion abelian group, then there is a natural decomposition $X = \prod_l X_l$ of X, where X_l is the l-component of X, i.e., the maximal l-group contained in X. Under this situation, we can define the l-dimension $\dim_l X$ of X by setting $\dim_l X = \dim X_l$.

Let K be an abelian extension over an algebraic number field F of finite degree, and let $G = G(K/F)$ be the Galois group of K/F. Then G is a compact abelian group, and the character group char G of G is a discrete, countable, torsion abelian group. Furthermore, it follows from the class field theory that $\dim_l \operatorname{char} G$ is finite for any prime number l [2], which will be called the l-dimension of K/F and will be denoted by $\dim_l(K/F)$. We say that K/F is a divisible l-extension, if char G is a divisible l-group. If in general $\dim_l(K/F) = d$, then K/F contains a subfield K' such that $G(K'/F)$ is isomorphic to $\boldsymbol{Z}_l^d$. Namely, K' is the field corresponding to the maximal divisible subgroup of the l-component of char G. The field K' is uniquely determined. K'/F is divisible, and every divisible subfield of K/F is contained in K'. We shall call the field K' the maximal divisible l-subfield of K/F.

We now propose to recall some terminologies and results in the theory of complex multiplication of abelian varieties. For details we refer to [5]. Let F be an algebraic number field of degree $n = 2m$ which contains a totally imaginary subfield F' as a quadratic extension of a totally real field, and let $\{\phi_i\}$ be the set of m distinct isomorphisms of F into $\boldsymbol{C}$. Then the pair $(F; \{\phi_i\})$ is called a CM-type if, for any i, j, the restrictions of ϕ_i, ϕ_j to F' are not complex conjugates of each other. Let L be a normal extension over $\boldsymbol{Q}$ containing F, and let ϕ_i denote also a fixed prolongation of ϕ_i to L. Set, furthermore, $G(L/\boldsymbol{Q}) = G$, $G(L/F) = H$, and $S = H\phi_1 + \cdots + H\phi_m$. Then the CM-type $(F; \{\phi_i\})$ is called primitive if $\gamma S = S$ $(\gamma \in G)$, implies $\gamma \in H$. For a primitive CM-type, we have $F = F'$. Let now H^* be the group of all $\gamma \in G$ such that $S\gamma = S$, let F^* be the field corresponding to H^*, and let $\{\psi_i\}$ be the set of all distinct isomorphisms of F^* into $\boldsymbol{C}$ induced by the elements of S^{-1}. Then $(F^*; \{\psi_i\})$ is a primitive CM-type which is called the dual of $(F; \{\phi_i\})$. A primitive CM-type is the dual of its dual. If $(F^*; \{\psi_i\})$ is the dual of a CM-type $(F; \{\phi_i\})$, and α [resp. $\mathfrak{a}$] is a number [resp. an ideal of F], then α^{ϕ_i} [resp. $\mathfrak{a}^{\phi_i}$] is a number [resp. an ideal of F^*].

Let $(F; \{\phi_i\})$ be a CM-type, and let A be an abelian variety belonging to the dual $(F^*;(\psi_i\})$ of $(F;\{\phi_i\})$ in the sense of the theory of complex multiplication. Let $\mathfrak{b}$ be an integral ideal of F^*, let $b \neq 0$ be a natural number divisible by $\mathfrak{b}$, and let $H(\mathfrak{b})$ be the group of all ideals $\mathfrak{a}$ prime to b of F such that there exists an element $\mu \in F^*$ with

$$\prod_i \mathfrak{a}^{\phi_i} = (\mu), \qquad \mu\bar{\mu} = N\mathfrak{a}, \qquad \mu \equiv 1 \pmod{\mathfrak{b}}.$$

Then, the extension over F obtained by the $\mathfrak{b}$-section of A is the class field $K_{\mathfrak{b}}$ over F corresponding to $H(\mathfrak{b})$. This is a main theorem in the theory of complex multiplication of abelian varieties [5] (see also [4]). The union $\bigcup K_{\mathfrak{b}}$ of all $K_{\mathfrak{b}}$ will be called the maximal extension obtained by complex multiplication of A. For our purpose, it is not necessary to give a precise definition of an abelian variety belonging to a CM-type, the ideal section of an abelian variety, etc. Our starting point is simply the class field $K_{\mathfrak{b}}$ over the ideal group $H(\mathfrak{b})$.

2. **Rank of a CM-type.** Let $(F;\{\phi_i\})$ be a CM-type and $(F^*;(\psi_i\})$ be its dual. Let L, G, H, H^*, and S be as in §1. Furthermore, let ϕ_i [resp. ψ_i] denote also a prolongation to L of the original ϕ_i [resp. ψ_i], and define γ_{ij} by

$$\gamma_{ij} = \begin{cases} 1, & \text{if } \phi_i\psi_j^{-1} \in S, \\ -1, & \text{otherwise.} \end{cases}$$

Then $C = (\gamma_{ij})$ is an $m \times m^*$ matrix, where $2m = (F:Q)$, $2m^* = (F^*:Q)$, and C depends neither on the choice of prolongations of ϕ_i, ψ_i, nor on the choice of L. Now we define the rank of the CM-type $(F;\{\phi_i\})$ by

$$\operatorname{rank}(F;\{\phi_i\}) = \operatorname{rank} C + 1.$$

If we consider an abelian variety A belonging to $(F;\{\phi_i\})$, we shall call $\operatorname{rank}(F;\{\phi_i\})$ also the rank of A, and use the notation $\operatorname{rank} A$. The rank is an elementary, group theoretical invariant of a CM-type, and we have obviously $\operatorname{rank}(F;\{\phi_i\}) \leqq m+1$. We say that $(F;\{\phi_i\})$ or an abelian variety belonging to $(F;\{\phi_i\})$ is nondegenerate if $\operatorname{rank}(F;\{\phi_i\}) = m+1$. It follows easily from the definition that the rank of a CM-type is equal to the rank of its dual, and that a nondegenerate CM-type is primitive.

The following lemma explains a meaning of the rank of a CM-type.

Lemma 1. *Notations being as above, let $R(G)$ be the group ring of G over a principal ideal domain R. Let Φ be the operator which maps $x \in R(G)$ to $x^{\Phi} = \sum_{\sigma \in S} x\sigma$. Then the dimension of $R(G)^{\Phi}$ over R is equal to the rank of the* CM-*type* $(F;\{\phi_i\})$.

Proof. Consider a general element $x = \sum_{\xi \in G} x_\xi \xi$ of $R(G)$. Then,

$$x^{\Phi} = \sum_{\sigma \in S}\left(\sum_{\xi} x_\xi \xi\right)\sigma = \sum_{\tau \in G}\left(\sum_{\xi} \delta_{\xi,\tau} x_{\xi^{-1}}\right)\tau,$$

where

$$\delta_{\xi,\tau} = \begin{cases} 1, & \text{if } \xi\tau \in S, \\ 0, & \text{otherwise.} \end{cases}$$

For the proof of the lemma, it is sufficient to show $\operatorname{rank} D = \operatorname{rank}(F; \{\phi_i\})$ with $D = (\delta_{\xi,\tau})$. Let $\rho \in G$ be the complex conjugation of L. Then,

$$\begin{aligned} G &= H\phi_1 + \cdots + H\phi_m + H\rho\phi_1 + \cdots + H\rho\phi_m \\ &= H^*\psi_1 + \cdots + H^*\psi_{m^*} + H^*\rho\psi_1 + \cdots + H^*\rho\psi_{m^*} \\ &= \psi_1^{-1}H^* + \cdots + \psi_{m^*}^{-1}H^* + \psi_1^{-1}\rho H^* + \cdots + \psi_{m^*}^{-1}\rho H^* \end{aligned}$$

and

$$\begin{aligned} \delta_{h\xi,\tau h^*} &= \delta_{\xi,\tau}, \\ \delta_{\rho\xi,\tau} + \delta_{\xi,\tau} &= 1, \\ \delta_{\xi,\tau\rho} + \delta_{\xi,\tau} &= 1 \end{aligned}$$

for $\xi, \tau \in G$, $h \in H$, $h^* \in H^*$ (cf. [5]). Therefore we have a relation between D and C in the following form containing a Kronecker product of matrices:

$$D = \frac{1}{2}\begin{pmatrix} J + C & J - C \\ J - C & J + C \end{pmatrix} \times J^*,$$

where J [resp. J^*] is an $m \times m^*$ [resp. $(g/2m) \times (g/2m^*)$] matrix whose entries are all 1, g being the order of G. Denote by D' the first factor, including $\frac{1}{2}$, of the above product. Then, $\operatorname{rank} D = \operatorname{rank} D'$. To determine rank D', we may assume without any loss of generality that $\psi_1 = 1$ or ρ. If $\psi_1 = 1$, then all the entries of the first column of $\frac{1}{2}(J + C)$ are 1. If $\psi_1 = \rho$, then all the entries of the first column of $\frac{1}{2}(J - C)$ are 1.

Let now in general M, J be two matrices of the same size, and assume that the entries of M are 1 or 0, and that the enries of J are all 1. Then,

$$\operatorname{rank}\begin{pmatrix} M & J - M \\ J - M & M \end{pmatrix} = \operatorname{rank}\begin{pmatrix} M & J \\ J & 2J \end{pmatrix}.$$

If, furthermore, the entries of the first column of M are all 1, we have

$$\operatorname{rank}\begin{pmatrix} M & J \\ J & 2J \end{pmatrix} = \operatorname{rank}\begin{pmatrix} M & 0 \\ J & J \end{pmatrix}$$

and

$$\operatorname{rank}\begin{pmatrix} M & J - M \\ J - M & M \end{pmatrix} = \operatorname{rank} M + 1 = \operatorname{rank}(2M - J) + 1.$$

If we apply this result to our special case of $M = \frac{1}{2}(J + C)$ or $M = \frac{1}{2}(J - C)$, we obtain

$$\operatorname{rank} D' = \operatorname{rank} C + 1,$$

which proves the lemma.

3. **Main result.** Our main result is the following:

THEOREM 1. *Let $(F_j; \{\phi_i\})$ be a* CM*-type, and let K_c be the maximal extension over F obtained by the complex multiplication of an abelian variety A belonging to the dual $(F^*; \{\psi_i\})$ of $(F; \{\phi_i\})$. Then*

$$\dim_l (K_c/F) = \operatorname{rank} A$$

for any prime number l.

Proof. Let L be a normal field of finite degree over Q which contains the absolute class field over F. Then, for any ideal $\mathfrak{a}$ of L, there is an element $\mu_0 \in F$ such that $N_{L/F}\mathfrak{a} = (\mu_0)$. The product $\mu = \prod_i \mu_0^{\phi_i}$ lies in F^*, and we have $\mu\bar{\mu} = N\mathfrak{a}$. In other words, we find a $\mu \in F^*$ with $\prod_i (N_{L/F}\mathfrak{a})^{\phi_i} = (\mu)$, $\mu\bar{\mu} = N\mathfrak{a}$. This property determines μ up to a root of unity. Furthermore, if we denote by b a natural number, by $u(b)$ the group of residue classes mod b in F^* represented by numbers prime to b, and by $w(b)$ the subgroup of $u(b)$ consisting of residue classes represented by roots of unity in F^*, then $\mathfrak{a} \to \mu$ defines a homomorphism of the group of ideals prime to b of L into $u(b)/w(b)$. We denote the image of this homomorphism by $c'(b)$. Let $K_{(b)}$ be the extension over F obtained by the (b)-section of A. Then, by the class field theoretical characterization of $K_{(b)}$ given in §1, the Galois group of $K_{(b)}L/L$ is isomorphic to $c'(b)$.

Let $b_1, b_2, \cdots, b_k, \cdots$ be a sequence of natural numbers such that b_k divides b_{k+1}, and that there exists a $b_k \equiv 0 \pmod{N}$ for any natural number N. Then, there is a natural epimorphism $u(b_k) \leftarrow u(b_{k+1})$, and, since $K_c = \bigcup K_{(b_k)}$, the limit group $\lim c'(b_k)$ is isomorphic to the Galois group of K_cL/L. Denote by $c(b)$ the subgroup of $c'(b)$ consisting of images of all principal ideals prime to b of L. Then, there is a natural epimorphism $c(b_k) \leftarrow c(b_{k+1})$.

Now, in general, a commutative diagram of homomorphisms of additive groups

$$\begin{array}{ccccccc}
0 & & 0 & & 0 & & \\
\downarrow & & \downarrow & & \downarrow & & \\
C_1 & \leftarrow & C_2 & \leftarrow & C_3 & \leftarrow & \\
\downarrow & & \downarrow & & \downarrow & & \\
C_1' & \leftarrow & C_2' & \leftarrow & C_3' & \leftarrow & \\
\downarrow & & \downarrow & & \downarrow & & \\
C_1'' & \leftarrow & C_2'' & \leftarrow & C_3'' & \leftarrow & \\
\downarrow & & \downarrow & & \downarrow & & \\
0 & & 0 & & 0 & &
\end{array}$$

with exact columns and epimorphic horizontal mappings gives rise to an exact sequence

$$0 \to \lim C_k \to \lim C'_k \to \lim C''_k \to 0. \tag{2}$$

Apply this result to $C_k = c(b_k)$, $C'_k = c'(b_k)$, $C''_k = c'(b_k)/c(b_k)$. Then, since C''_k is a homomorphic image of the ideal class group of L, it follows from (1) that it is sufficient for our purpose to observe $\lim c(b_k)$ instead of $\lim c'(b_k)$.

Set $\alpha^{\Phi} = \prod_i (N_{L/F}\alpha)^{\varphi_i}$ for $\alpha \in L$. Then, Φ defines a homomorphism of the multiplicative group of numbers prime to b in L into $u(b)$. Let $v(b)$ be the image of this homomorphism. Then we have $c(b) = v(b)w(b)/w(b) \cong v(b)/v(b) \cap w(b)$. Apply this time (2) to $C_k = v(b_k) \cap w(b_k)$, $C'_k = v(b_k)$, $C''_k = c(b_k)$. Then, since C_k is a subgroup of the group of roots of unity in F^*, the determination of $\dim_l (K_c/F)$ is reduced to the determination of $\dim_l$ char lim $v(b_k)$.

If $b = \prod p^{a_p}$ is the prime number decomposition of b, then $v(b)$ is the direct product of $v(p^{a_p})$. This shows that

$$\lim v(b_k) \cong \prod_p \lim v(p^k),$$

where the product is extended over all prime numbers. But, for any p, $\lim v(p^k)$ is a subgroup of $\lim u(p^k)$ which is isomorphic to the unit group $(F^* \otimes \boldsymbol{Q}_p)^*$ of $F^* \otimes \boldsymbol{Q}_p$, and $(F^* \otimes \boldsymbol{Q}_p)^*$ contains no subgroup isomorphic to $\boldsymbol{Z}_l$ unless $p = l$. So, $\dim_l (K_c/F)$ is equal to the l-dimension of char lim $v(l^k)$.

The homomorphism Φ is naturally extended to $V = (L \otimes \boldsymbol{Q}_l)^*$, and the image V^{Φ} is a subgroup of $U = (F^* \otimes \boldsymbol{Q}_l)^*$. If we denote by $U(l^k)$ the group of $u \in U$ with $u \equiv 1 \pmod{l^k}$, we have the following commutative diagram with natural homomorphisms:

$$\begin{array}{ccc} V^{\Phi} U(l^k)/U(l^k) & \longleftarrow & V^{\Phi} U(l^{k+1})/U(l^{k+1}) \\ \updownarrow & & \updownarrow \\ v(l^k) & \longleftarrow & v(l^{k+1}). \end{array}$$

Since V^{Φ} is closed in U, we have $\lim v(l^k) = V^{\Phi}$. According to the theory of local fields, V contains a subgroup of finite index which is isomorphic to the additive group of the group ring $\boldsymbol{Z}_l(G)$ over $\boldsymbol{Z}_l$ of the Galois group G of $L/\boldsymbol{Q}$. Hence, by Lemma 1, the l-dimension of char V^{Φ} is equal to rank A, which proves the theorem.

REMARK. By a similar argument used in this proof, we can also show that char lim $c'(l^k)$ has the same l-dimension as char lim $v(l^k)$. This means that the maximal divisible l-subfield of K_c/F is contained in the field obtained by l-power sections of A.

4. A special case. As was already mentioned in §2, the rank of a CM-type $(F; \{\phi_i\})$ is by definition not greater than $m + 1$ if $(F:\boldsymbol{Q}) = 2m$. We call the difference $m + 1 - \operatorname{rank}(F; \{\phi_i\})$ the defect of $(F; \{\phi_i\})$. A CM-type, or an abelian variety belonging to it, is nondegenerate if the defect of the CM-type is 0. Whereas we can find many nondegenerate CM-types through simple calculations, it sometimes turns out a nontrivial problem to determine the rank of a given CM-type. The main aim of the remaining part of the present paper is to show that the Jacobian varieties of certain well-known curves of Fermat type are nondegenerate. To do this, we require two lemmas.

LEMMA 2. *Let* $(F;\{\sigma_i\})$ *be a* CM-*type such that* F/Q *is an abelian extension. Denote by* G *the Galois group of* F/Q, *and by* $\rho \in G$ *the complex conjugation of* F. *Then, the defect of* $(F;\{\sigma_i\})$ *is equal to the number of characters* ψ *of* G *satisfying* $\sum_i \psi(\sigma_i) = 0$, $\psi(\rho) = -1$.

Proof. Let $\psi_1, \cdots, \psi_m$ be all characters of G which take -1 at ρ. Set

$$\Psi = \begin{bmatrix} \psi_1(\sigma_1) \cdots & \psi_m(\sigma_1) \\ \cdots & \\ \psi_1(\sigma_m) \cdots & \psi_m(\sigma_m) \end{bmatrix}.$$

Then $\Psi^{-1} = (1/m)^t\overline{\Psi}$. Set now for $\tau \in G$

$$\varepsilon_{ij}^{\tau} = \begin{cases} 1, & \text{if } \sigma_i\tau = \sigma_j, \\ -1, & \text{if } \sigma_i\tau = \rho\sigma_j, \\ 0, & \text{otherwise,} \end{cases}$$

and put $(\varepsilon_{ij}^{\tau}) = E(\tau)$. Furthermore, set

$$D(\tau) = \begin{bmatrix} \psi_1(\tau) & & \\ & \ddots & \\ & & \psi_m(\tau) \end{bmatrix}.$$

Then we have $E(\tau)\Psi = \Psi D(\tau)$, so that $E(\tau)\overline{\Psi} = \overline{\Psi}\overline{D(\tau)}$. If on the other hand J_j is the $m \times m$ matrix whose entries of the jth column are all 1 and other entries are all 0, then the entries c_{ij} of the matrix

$$C' = E(\sigma_1)J_1 + \cdots + E(\sigma_m)J_m$$

are given by

$$c'_{ij} = \begin{cases} 1, & \text{if } \sigma_i\sigma_j \in S, \\ -1, & \text{if } \sigma_i\sigma_j \in \rho S, \end{cases}$$

where $S = \{\sigma_i\}$. Denote now by H^* the group of all $\gamma \in G$ such that $S\gamma = S$, and recall that the dual of $(F;\{\sigma_i\})$ consists of the subfield F^* of F corresponding to H^* and the set of distinct isomorphisms induced on F^* by the elements of $\{\sigma_i^{-1}\}$. Then it follows from the definition of the matrix C in §2 that C' is of the form $(C, C, \cdots, C)$.

Thus we have rank $C' = \operatorname{rank} C$. Therefore the defect of $(F; \{\sigma_i\})$ is equal to $m - \operatorname{rank} C'$. If we set here

$$D = \begin{bmatrix} \sum_i \psi_1(\sigma_i) & & \\ & \ddots & \\ & & \sum_i \psi_m(\sigma_i) \end{bmatrix}$$

then

$$\begin{aligned} C' &= \frac{1}{m}(\overline{\Psi}\,\overline{D(\sigma_1)}^t\,\Psi J_1 + \cdots + \overline{\Psi}\,\overline{D(\sigma_m)}^t\,\Psi J_m) \\ &= \frac{1}{m}\overline{\Psi}(\overline{D(\sigma_1)}\,DJ_1 + \cdots + \overline{D(\sigma_m)}\,DJ_m) \\ &= \frac{1}{m}\overline{\Psi}D(\overline{D(\sigma_1)}J_1 + \cdots + \overline{D(\sigma_m)}\,J_m) = \frac{1}{m}\overline{\Psi}D^t\overline{\Psi}\,. \end{aligned}$$

So, $C' = \overline{\Psi}D\Psi^{-1}$. This proves the lemma.

LEMMA 3 (H. W. LEOPOLDT). *Let $p = 2m + 1$ be an odd prime number, and let ψ be a character of the group of nonzero residue classes of $Z/(p)$ such that $\psi(-1) = -1$. Then, $\sum_{a=1}^m \psi(a) \neq 0$.*

Proof. Consider the sum

$$\Theta = \sum_{a=1}^{2m} \psi(a)a.$$

Then we have always $\Theta \neq 0$, because Θ is a factor contained in the class number formula for the pth cyclotomic field. Set now

$$A = \sum_{a=1}^{m} \psi(a)a, \qquad A' = \sum_{a=m+1}^{2m} \psi(a)a,$$

$$A_1 = \sum_{a=1}^{m} \psi(2a-1)(2a-1), \quad A_2 = \sum_{a=1}^{m} \psi(2a)\cdot 2a,$$

$$B = \sum_{a=1}^{m} \psi(a), \qquad B_1 = \sum_{a=1}^{m} \psi(2a-1).$$

Then $\Theta = A + A'$, and

$$A' = \sum_{a=1}^{m} \psi(p-a)(p-a) = -pB + A.$$

Hence

$$\Theta = 2A - pB. \tag{3}$$

On the other hand, since

$$\begin{aligned} B_1 &= -\sum_{a=1}^{m} \psi(p-(2a-1)) \\ &= -\psi(2)\sum_{a=1}^{m} \psi(m+1-a) = -\psi(2)B, \end{aligned}$$

we have

$$\begin{aligned} A_1 &= -B_1 + 2\sum_{a=1}^{m} \psi(2a-1)a = -B_1 - 2\sum_{a=1}^{m} \psi(p-(2a-1))a \\ &= -B_1 - 2\psi(2)\sum_{a=1}^{m} \psi(m+1-a)a \\ &= -B_1 + 2\psi(2)\sum_{a=1}^{m} \psi(m+1-a)(m+1-a) \\ &\qquad\qquad - 2\psi(2)(m+1)\sum_{a=1}^{m} \psi(m+1-a) \\ &= \psi(2)B + 2\psi(2)A - \psi(2)(p+1)B \\ &= 2\psi(2)A - p\psi(2)B. \end{aligned}$$

Therefore, it follows from $\Theta = A_1 + A_2$ and $A_2 = 2\psi(2)A$ that

$$\Theta = 4\psi(2)A - p\psi(2)B. \tag{4}$$

By (3) and (4), we have

$$2(1-2\psi(2))A = p(1-\psi(2))B.$$

So, using (3) again, one obtains finally

$$(1-2\psi(2))\Theta = p(1-\psi(2))B - p(1-2\psi(2))B = p\psi(2)B.$$

This shows $B \neq 0$, which proves the lemma.

Denote by J the Jacobian variety of a complete, nonsingular model of the curve $y^2 = 1 - x^p$, $p = 2m+1$ being an odd prime number. Let ζ be a primitive pth root of unity, and let $\sigma_1, \cdots, \sigma_m$ be automorphisms of $F = \boldsymbol{Q}(\zeta)$ determined by $\zeta^{\sigma_i} = \zeta^i$ $(i = 1, \cdots, m)$. Then, the abelian variety J belongs to the primitive CM-type $(F; \{\sigma_i\})$, (see [5]), and it follows immediatelly from Lemma 2 and Lemma 3 that $(F; \{\sigma_i\})$ is nondegenerate. Thus we have the following

THEOREM 2. *Let p be an odd prime number. Then, the Jacobian variety of a complete, nonsingular model of the curve $y^2 = 1 - x^p$ is nondegenerate.*

REMARK. Let $(F; \{\phi_i\})$ be a CM-type, let K_a be the maximal abelian extension over F, and K_c be the maximal extension over F obtained by the complex multiplication of an abelian variety A belonging to the dual $(F^*;\{\psi_i\})$ of $(F;\{\phi_i\})$. Then, Theorem 1 shows $\dim_l(K_c/F) \leqq m+1$, if $2m=(F:\boldsymbol{Q})$. The equality holds if and only if $(F;\{\phi\})$ is nondegenerate.

Now, let us consider $\dim_l(K_a/F)$. The elements in $F\otimes Q_l$ which are congruent to 1 mod l form a multiplicative group U_1, and U_1 is regarded as a vector space over $\boldsymbol{Z}_l$, because for any $u\in U_1$, $\alpha\in \boldsymbol{Z}_l$, we can define u^α. The dimension of U_1 in this sense is $2m$. Denote by μ_l the dimension of $\boldsymbol{Z}_l$-subspace of U_1 spanned by units of F contained in U_1. Then $\mu_l \leqq m-1$ by Dirichlet's unit theorem, and it is shown in [2] that $\dim_l(K_a/F)=2m-\mu_l$. Therefore $\dim_l K_a/F \geqq m+1$, and the equality holds if and only if $\mu_l=m-1$.

The equality $\mu_l=m-1$ is equivalent to the assertion that the l-adic regulator as defined in [3] is different from 0. If this is the case, the above argument shows that $\dim_l(K_a/F)=\dim_l(K_c/F)$ for a nondegenerate CM-type $(F;\{\phi_i\})$. Therefore, by (1), the maximal divisible l-subfield of K_a/F coincides with the maximal divisible l-subfield of K_c/F.

It might be of some interest to point out that an analogous situation is also found in the case of cyclotomic extensions. Let F be a totally real field, let K_a be the maximal abelian extension over F, and let K_c be the maximal cyclotomic extension over F. Then it is easily seen that $\dim_l(K_c/F)=1$ for any prime number l, and we have $\dim_l(K_a/F)=1$ if $\mu_l=(F:\boldsymbol{Q})-1$. This means that the maximal divisible l-subfield of K_a/F is the same as that of K_c/F if $\mu_l=(F:\boldsymbol{Q})-1$.

References

1. I. Kaplansky, *Infinite abelian groups*, Univ. Michigan Press, Ann Arbor, Mich., 1954.

2. T. Kubota, *Galois group of the maximal abelian extension over an algebraic number field*, Nagoya Math. J. **12** (1957), 177–189.

3. H. W. Leopoldt, *Zur Arithmetik in abelschen Zahlkörpern*, J. Reine Angew. Math. **209** (1962), 54–71.

4. G. Shimura, *On the class-fields obtained by complex multiplication of abelian varieties*, Osaka Math. J. **14** (1962), 33–44.

5. G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, The Mathematical Society of Japan, Tokyo, 1961.

Nagoya University,
Chikusa-ku, Nagoya, Japan
The Institute for Advanced study,
Princeton, New Jersey