J. Math. Sci. Univ. Tokyo
10 (2003), 581–598.

Hodge Cycles on Abelian Varieties with Complex Multiplication by Cyclic CM-Fields

By Fumio Hazama

Abstract. For any cyclic CM-fields of degree $2pq$ with p, q distinct odd primes, we determine which CM-types among 2^{pq} ones give rise to degenerate abelian varieties and in what codimension nondivisorial Hodge cycles exist on them.

1. Introduction

The purpose of this paper is to classify the CM-types for cyclic CM-fields of degree $2pq$ with p, q distinct odd primes according to the structures of the Hodge rings of corresponding abelian varieties. Our classification reveals in what codimension non-divisorial Hodge cycles lie, and at the same time shows that the algebraicity of these Hodge cycles implies the Hodge conjecture for any self-products of the abelian varieties. From our result follows, for example, that there are $\sum_{0\leq i\leq p}\binom{p}{i}^q - 2^p$ p-dominated CM-types, $\sum_{0\leq i\leq q}\binom{q}{i}^p - 2^q$ q-dominated CM-types, and the other primitive ones are nondegenerate. As a byproduct we obtain the result to the effect that there is always a degenerate CM-type for $\mathbf{Q}(\zeta_{2n+1})$ whenever $n = 3q$ with q a prime > 3. This gives an effective version of a result (due to Lenstra and Stark) in [5, (3.11)] stating that for sufficiently large prime $2n+1 \equiv 7 (\mathrm{mod}\, 12)$ there exists a degenerate CM-type for $\mathbf{Q}(\zeta_{2n+1})$. As another consequence of our theorem, we have a stronger version of a theorem by Lenstra in the case of cyclic CM-fields of degree $2pq$. He showed that for any degenerate abelian variety A with complex multiplication by an *abelian* CM-field, there always exists a nondivisorial Hodge cycle on A itself (see [7]). Our theorem shows, as well as this, that for our cyclic cases the whole Hodge rings $\mathcal{H}(A^k)$, $k \geq 1$ of its self-products are *generated* (up to some equivalence relation) by Hodge cycles on A itself when A is degenerate (see Section four and five for more details).

1991 *Mathematics Subject Classification.* 14C30.
Key words: Hodge cycle, abelian variety, complex multiplication.

The plan of this paper is as follows. Section two recalls some fundamental properties of Hodge cycles on abelian varieties of CM-type. In particular, the notions of *N-dominatedness* and *h-degeneracy* are explained here. In Section three, we construct a $\mathbf{Z}$-basis of the group algebra $\mathbf{Z}[\mathbf{Z}/2n\mathbf{Z}]$ which reflects the orthogonal decomposition according to the characters of $\mathbf{Z}/2n\mathbf{Z}$. The basis plays a fundamental role in the remaining sections. In Section four, we determine completely (Theorem 4.8) what and how many CM-types for $\mathbf{Z}/2n\mathbf{Z}$ are degenerate, when $n = pq$ is the product of distinct odd primes pq. Section five is devoted to show that any absolutely simple and degenerate abelian varieties with complex multiplication by a cyclic CM-field of degree $2pq$ must be p-dominated or q-dominated. Furthermore, it is shown that all of them are 1-degenerate. As an application of our theorem we show in Section six how it is simple to construct degenerate CM-types for some cyclotomic fields and to count the number of those CM-types.

2. Hodge Cycles and Characters

The purpose of this section is to recall some fundamental facts about the relationship between Hodge cycles on an abelian variety of CM-type and characters of the Galois group of the corresponding CM-field. We also recall the notions of N-dominatedness and h-degeneracy.

Let K be a CM-field with abelian Galois group G of order $2n$. Let $G = \{g_1, \dots, g_n, g_1\rho, \dots, g_n\rho\}$, where g_1 is assumed to be the identity element and ρ denotes the complex conjugation. Let $S \subset G$ be a CM-type, namely a subset of G such that $S \coprod S\rho = G$ (disjoint union), and let A_S denote the abelian variety associated with S (see [3], for example). We identify $\mathbf{Q}[G]$ with $\mathbf{Q}^{2n}$, the space of row vectors of length n, through the given ordering of the elements of G. Furthermore we identify a subset $T \subset G$ with the element $\sum_{t \in T} t \in \mathbf{Q}[G]$. For any $g \in G$, let $h_g = Sg - S\rho g \in \mathbf{Q}[G]$. We define the *Hodge matrix* H_S to be the n by $2n$ matrix whose i-th row vector is h_{g_i}, $1 \leq i \leq n$. For any abelian variety A, let $Hg(A)$ denote the Hodge group of A. It is known that $Hg(A)$ is an algebraic torus over $\mathbf{Q}$, and the inequality $\dim Hg(A) \leq \dim A$ holds. When $\dim Hg(A)$ is smaller than $\dim A$, the abelian variety is *degenerate* in the sense that there is a nondivisorial Hodge cycle on some A^k, $k \geq 1$ ([1]). The Hodge matrix is of fundamental importance for the study of the Hodge ring of A_S, since $\operatorname{rank} H_S = \dim Hg(A_S)$ and the kernel $\mathbf{K}_S = \ker H_S$ depicts the set of nondivisorial Hodge cycles on A^k, $k \geq 1$ (see [1], [3] for details). Moreover, the rank of the Hodge matrix is related to the character sums. For any character $\chi \in X(G) = \mathrm{Hom}(G, \mathbf{C}^*$ and a subset $T \subset G$, we write $\chi(T) = \sum_{g \in T} \chi(g) \in \mathbf{C}$.

Proposition 2.1 ([4], [5]). *The difference* $\dim A - \operatorname{rank} H(A)$ *is equal to the number of the odd characters of* G *such that* $\chi(S) = 0$.

Remark 2.2. A character χ is said to be *odd* (resp. even) if $\chi(\rho) = -1$ (resp. $\chi(\rho) = 1$). Note that for any nontrivial even character χ we have $\chi(S) = (\chi(S) + \chi(S))/2 = (\chi(S) + \chi(\rho S))/2 = \chi(G)/2 = 0$. Hence we can rephrase the proposition as an equality $\operatorname{rank} H(A) = \#\{\chi \in X(G); \chi(S) \neq 0\} - 1$.

A CM-type S is said to be *primitive* if the corresponding abelian variety is absolutely simple. The following criterion for primitivity will be used later frequently.

Proposition 2.3 ([5, Section 2]). *A CM-type* S *is primitive if and only if it is not stable under any elements of* $G - \{g_1\}$.

Next we recall a characterization of N-dominatedness and h-degeneracy of an abelian variety A. Originally they are defined in terms of the structure of the Hodge rings of the self-products A^k, $k \geq 1$ (see [1] for N-dominatedness and [3] for h-degeneracy). Here we explain them through their characterizations given in the papers cited above, and thereafter we describe their relevance in the theory of Hodge cycles. For any $v = \sum_{g \in G} a_g g \in \mathbf{Z}[G]$, we set

$$w(v) = \sum_{g \in G} |a_g|/2,$$
$$h(v) = \max\{|a_g|; g \in G\},$$

and call (resp. $h(v)$) the *weight* (resp. *height*) of v. Moreover for any finite subset X of $\mathbf{Z}[G]$, we put

$$w(X) = \max\{w(v) : v \in X\},$$
$$h(X) = \max\{h(v) : v \in X\}.$$

Furthermore for any $\mathbf{Z}$-submodule $\mathbf{N}$ of $\mathbf{Z}[G]$, we put

$$w(\mathbf{N}) = \min\{w(X) : X \text{ is a spanning subset of } \mathbf{N}\},$$
$$h(\mathbf{N}) = \min\{h(X) : X \text{ is a spanning subset of } \mathbf{N}\}.$$

Using this notion of weight (resp. height), we can characterize the N-dominatedness (resp. N-degeneracy) as follows.

PROPOSITION 2.4 ([1], [3]). *Notation being as above, the abelian variety A_S is*

(i) *N-dominated if and only if $w(\mathbf{K}_S) = N$.*

(ii) *h-degenerate if and only if $h(\mathbf{K}_S) = h$.*

REMARK 2.5. These two notions are related to the investigation of the Hodge conjecture in the following way. If A is N-dominated, then the Hodge conjecture for all the self-products A^k, $k \geq 1$, is implied by the truth of the conjecture for up to codimension N. On the other hand, if A is h-degenerate, then the Hodge conjecture for all the self-products A^k, $k \geq 1$, is implied by the truth of the conjecture for A^k, $k \geq h$. See [1], [3] for more details.

3. Decomposition of $\mathbf{Z}[\mathbf{Z}/2n\mathbf{Z}]$

In this section we construct a $\mathbf{Z}$-basis of $\mathbf{Z}[\mathbf{Z}/2n\mathbf{Z}]$, which reflects the decomposition $\mathbf{C}[\mathbf{Z}/2n\mathbf{Z}] \cong \bigoplus_{\chi \in X(\mathbf{Z}/2n\mathbf{Z})} \mathbf{C}[\mathbf{Z}/2n\mathbf{Z}]_\chi$. This basis will play an important role in Sections four and five.

The character group $X(\mathbf{Z}/2n\mathbf{Z})$ consists of $2n$ characters χ_i, $0 \leq i \leq 2n-1$, where χ_i is defined by $\chi_i(a) = \zeta^{ia}$ for $a \in \mathbf{Z}/2n\mathbf{Z}$ with $\zeta = \zeta_{2n}$ a fixed primitive $2n$-th root of unity. In particular, the set of odd characters $X^-(\mathbf{Z}/2n\mathbf{Z})$ consists of χ_{2i-1}, $1 \leq i \leq n$. For any commutative ring R, let $R[\mathbf{Z}/2n\mathbf{Z}]$ denote the group algebra of $\mathbf{Z}/2n\mathbf{Z}$ with coefficients in R. For any $\chi \in X(\mathbf{Z}/2n\mathbf{Z})$, let $v_\chi = \sum_{a \in \mathbf{Z}/2n\mathbf{Z}} \chi(-a)[a] \in \mathbf{C}[\mathbf{Z}/2n\mathbf{Z}]$. Then the χ-part

$$\mathbf{C}[\mathbf{Z}/2n\mathbf{Z}]_\chi = \{v \in \mathbf{C}[\mathbf{Z}/2n\mathbf{Z}]; a.v = \chi(a)v \text{ for any } a \in \mathbf{Z}/2n\mathbf{Z}\}$$

is a one-dimensional subspace spanned by v_χ, and we have an isomorphism $\mathbf{C}[\mathbf{Z}/2n\mathbf{Z}] \cong \bigoplus_{\chi \in X(\mathbf{Z}/2n\mathbf{Z})} \mathbf{C}[\mathbf{Z}/2n\mathbf{Z}]_\chi$. Let ρ denote the element

$n \in \mathbf{Z}/2n\mathbf{Z}$, which will correspond later to the complex conjugation of respective CM-field. Let

$$R[\mathbf{Z}/2n\mathbf{Z}]^- = \{v \in R[\mathbf{Z}/2n\mathbf{Z}]; \rho.v = -v\}$$

the *odd* part of $R[\mathbf{Z}/2n\mathbf{Z}]$. Then through the isomorphism above we have $\mathbf{C}[\mathbf{Z}/2n\mathbf{Z}]^- \cong \bigoplus_{\chi \in X^-(\mathbf{Z}/2n\mathbf{Z})} \mathbf{C}[\mathbf{Z}/2n\mathbf{Z}]_\chi$. For any positive divisor m of $2n$, let $X_m = \{\chi \in X(\mathbf{Z}/2n\mathbf{Z})$; is of order $m\} = \{\chi_d \in X(\mathbf{Z}/2n\mathbf{Z}); (d, 2n) = 2n/m\}$. Let $v_a^{(m)} \sum_{\chi_d \in X_m} \zeta_{2n}^{ad} v_{\chi_d}$ for $a \in (\mathbf{Z}/m\mathbf{Z})^*$. These are a priori elements of $\mathbf{C}[\mathbf{Z}/2n\mathbf{Z}]$ and linearly independent over $\mathbf{C}$. They, however, are visibly invariant under the action of the Galois group $Gal(\mathbf{Q}(\mu_m)/\mathbf{Q})$ of the m-th cyclotomic field, hence we have $v_a^{(m)} \in \mathbf{Q}[\mathbf{Z}/2n\mathbf{Z}]$ for every $a \in (\mathbf{Z}_m\mathbf{Z})^*$. Therefore they give a $\mathbf{Q}$-structure on the direct sum $\bigoplus_{\chi \in X_m} \mathbf{C}[\mathbf{Z}/2n\mathbf{Z}]_\chi$, and we have

$$Q[\mathbf{Z}/2n\mathbf{Z}] \cong \bigoplus_{m|2n} V_m, \qquad \text{where} \qquad V_m = \langle v_a^{(m)}; a \in (\mathbf{Z}/m\mathbf{Z})^* \rangle_Q.$$

When $n = pq$ with p, q distinct odd primes, they can be expressed quite explicitly.

Proposition 3.1. *Let $n = pq$ with p, q distinct odd primes. For $r = p$ (resp. q), the elements $v_d^{(2r)}$, $d \in (\mathbf{Z}/2r\mathbf{Z})^*$, are given by*

$$v_d^{(2r)} = \sum_{a \in X(\mathbf{Z}/2n\mathbf{Z})} f_d^{(2r)}(a)[a], \qquad \textit{where} \tag{3.1}$$

$$f_d^{(2r)}(a) = \begin{cases} 1, & a : \textit{even}, \not\equiv 0 (\operatorname{mod} 2r), \\ -1, & a : \textit{odd}, \not\equiv d (\operatorname{mod} 2r), \\ r-1, & a \equiv d (\operatorname{mod} 2r), \\ -(r-1), & a \equiv d + r (\operatorname{mod} 2r). \end{cases}$$

Proof. This is essentially the orthogonality relations of characters. We may assume that $r = p$. Furthermore we have only to determine the coefficients of $[a]$ for even a, since $v_d^{(2p)}$ is an odd element as a sum of odd elements v_χ. For $d \in (\mathbf{Z}/2p\mathbf{Z})^*$, we have

$$v_d^{(2p)} = \sum_{k \in (\mathbf{Z}/2p\mathbf{Z})^*} \zeta_{2n}^{d \cdot kq} v_{\chi_{kq}}$$

$$\begin{aligned} &= \sum_{k\in(\mathbf{Z}/2p\mathbf{Z})^*} \chi_{kq}(d) \sum_{a\in\mathbf{Z}/2n\mathbf{Z}} \chi_{kq}(-a)[a] \\ &= \sum_{a\in\mathbf{Z}/2n\mathbf{Z}} \left(\sum_{k\in(\mathbf{Z}/2p\mathbf{Z})^*} \chi_{kq}(d-a) \right) [a]. \end{aligned}$$

The coefficient of $[a]$ with a even is computed as follows.

$$\begin{aligned} \sum_{k\in(\mathbf{Z}/2p\mathbf{Z})^*} \chi_{kq}(d-a) &= \sum_{k\in(\mathbf{Z}/2p\mathbf{Z})^*} \zeta_{2p}^{k(d-a)} \\ &= \sum_{\substack{k\in\mathbf{Z}/2p\mathbf{Z} \\ k:odd}} \zeta_{2p}^{k(d-a)} - (-1)^{d-a} \\ &= \begin{cases} 1, & \text{if} \quad d-a \not\equiv p(\operatorname{mod} 2p), \\ -p+1, & \text{if} \quad d-a \equiv p(\operatorname{mod} 2p). \end{cases} \end{aligned}$$

This completes the proof of Proposition 3.1. □

PROPOSITION 3.2. *Let $n = pq$ with p, q distinct odd primes. For (resp. q) and $1 \leq k \leq r-1$, let*

$$w_k^{(2r)} = \sum_{a\in\mathbf{Z}/2n\mathbf{Z}} g_k^{(2r)}(a)[a] \qquad \textit{where} \tag{3.2}$$

$$g_k^{(2r)}(a) = \begin{cases} 1, & a \equiv 0(\operatorname{mod} 2r), \\ -1, & a \equiv r(\operatorname{mod} 2r), \\ (-1)^{a-1}, & a \equiv k(\operatorname{mod} r), \\ 0, & \textit{otherwise}. \end{cases}$$

Then

$$V_{2r} \cap \mathbf{Z}[\mathbf{Z}/2n\mathbf{Z}] = \langle w_k^{(2r)}; 1 \leq k \leq r-1 \rangle_{\mathbf{Z}}. \tag{3.3}$$

PROOF. We may assume that $r = p$. First we show that the equality

$$v_{\rho^{k-1}.k} + \sum_{d\in(\mathbf{Z}/2p\mathbf{Z})^*} v_d^{(2p)} = pw_k^{(2p)} \tag{3.4}$$

holds for $1 \leq k \leq p-1$. We have only to show that the coefficients of $[a]$ with a even on the both sides are equal. When $a \equiv 0(\operatorname{mod} 2p)$, the coefficient of $[a]$ in $\sum_{d\in(\mathbf{Z}/2p\mathbf{Z})^*} v_d^{(2p)}$ is equal to $p-1$ by Proposition 3.1. When $a \not\equiv 0(\operatorname{mod} 2p)$, the coefficient is $(p-2)+(-p+1)=-1$. Hence the coefficient of $[a]$ in the left hand side of (3.4) is given by

$$\begin{cases} p, & \text{if} \quad a \equiv 0(\operatorname{mod} 2p), \\ -p, & \text{if} \quad a \equiv k(\operatorname{mod} p), \\ 0, & \text{otherwise.} \end{cases}$$

This coincides with the coefficient of $[a]$ in the right hand side. This shows that the equality (3.4) holds, and hence $w_k^{(2p)}$, $1 \le k \le p-1$ constitute a $\mathbf{Q}$-basis of V_{2p}. Suppose that $w = \sum_{1\le k\le p-1} c_k w_k^{(2p)} \in \mathbf{Z}[\mathbf{Z}/2n\mathbf{Z}]$ with $c_k \in \mathbf{Q}$. Then the coefficient of $[a]$ appearing in w is equal to $\pm c_a$ by the definition of $w_a^{(2p)}$. Hence c_a, $1 \le a \le p-1$, must be integers, and our proof is completed. □

4. Degenerate CM-types

In this section we determine what and how many CM-types for $\mathbf{Z}/2n\mathbf{Z}$ are degenerate, when $n = pq$ is the product of distinct odd primes.

A CM-type of the cyclic CM-field K with Galois group $\mathbf{Z}/2n\mathbf{Z}$ is specified by an n-element subset S of $\mathbf{Z}/2n\mathbf{Z}$ such that $S \cap \rho S = \phi$. (Recall the complex conjugation ρ corresponds to $n \in \mathbf{Z}/2n\mathbf{Z}$.) Let $f_S = \chi_T - \chi_{\rho T} : \mathbf{Z}/2n\mathbf{Z} \to \{\pm 1\}$, where χ_T, $T \subset \mathbf{Z}/2n\mathbf{Z}$, denotes the characteristic function of T. Then for an odd character $\chi \in X^-(\mathbf{Z}/2n\mathbf{Z})$ and a CM-type S, the character sum $\chi(S) = \sum_{a\in S} \chi(a)$ is expressed as

$$\chi(S) = \sum_{0\le a\le n-1} f_S(a)\chi(a) \tag{4.1}$$

Furthermore we associate to any odd function $f : \mathbf{Z}/2n\mathbf{Z} \to \mathbf{C}$ a function $E(f) : \mathbf{Z}/n\mathbf{Z} \to \mathbf{C}$ by the rule $E(f)(i) = f(2i)$, $0 \le i \le n-1$. For a CM-type S, we write $E(S)$ for $E(f_S)$.

Proposition 4.1. *The correspondence $S \mapsto E(S)$ gives a bijection between the set of CM-types for $\mathbf{Z}/2n\mathbf{Z}$ and the set of $\{\pm 1\}$-valued function on $\mathbf{Z}/n\mathbf{Z}$. Moreover for an odd character χ of $\mathbf{Z}/2n\mathbf{Z}$ and a CM-type S, $\chi(S) = 0$ if and only if $\sum_{b\in\mathbf{Z}_n\mathbf{Z}} E(\chi)(b) \cdot E(S)(b) = 0$.*

Proof. Only the last assertion needs to be proved. Let $S_{even} = \{a \in \mathbf{Z}/2n\mathbf{Z}; a \text{ is divisible by two}\}$. Note that this set is a CM-type for $\mathbf{Z}/2n\mathbf{Z}$. Hence

$$\begin{aligned} \chi(S) &= \sum_{a \in S} \chi(a) \\ &= \sum_{a \in S_{even} \cap S} \chi(a) - \sum_{a \in S_{even} - S} \chi(a) \\ &= \sum_{a \in S_{even}} f_S(a)\chi(a) \\ &= \sum_{b \in \mathbf{Z}/n\mathbf{Z}} E(S)(b)E(\chi)(b) \end{aligned}$$

This completes the proof of Proposition 4.1. □

For each odd divisor d of $n = pq$, let $\mathbf{S}_d$ denote the set of CM-types S such that $\chi_d(S) = 0$. Since the order of χ_d is equal to $\bar{d} = 2n/(d, 2n)$, we see that if $S \in S_d$ then $\chi(S) = 0$ for any $\chi \in X_{\bar{d}}$. First we consider the set $\mathbf{S}_{pq}$.

Proposition 4.2. *For the unique odd character $\chi_{pq} \in X_{\widetilde{pq}} = X_2$ of degree two, there are no CM-types S such that $\chi_{pq}(S) = 0$. Namely $\mathbf{S}_{pq} = \phi$.*

Proof. Since $\chi_{pq}(a) = (-1)^a$, $0 \leq a \leq n-1$, and $\#(S)$ is odd, the character sum $\chi(S)$ cannot be equal to zero. □

Next we consider the set $\mathbf{S}_p$.

Proposition 4.3. *There exists a natural bijection between the set $\mathbf{S}_p$ and the set of $q \times p$ $(0,1)$-matrices with constant row sum. Hence there are $\sum_{0 \leq i \leq p} \binom{p}{i}^p$ such CM-types.*

Proof. By (4.1), our task is to characterize the solutions $(\varepsilon, \ldots, \varepsilon_{n-1}) \in \{\pm 1\}^n$ of the equation $\sum_{0 \leq a \leq n-1} \varepsilon_a \chi_p(a) = 0$. If this holds, then it holds for all the characters in $X_{2q} = X_p$. Hence, by Proposition 3.2, it is equivalent to the system of equations

$$(4.2) \qquad \sum_{0 \leq a \leq n-1} \varepsilon_a g_k^{(2q)}(a) = 0, \qquad 1 \leq k \leq q-1.$$

Set

$$e_a = (-1)^a \varepsilon_a, \qquad 0 \le a \le n-1. \tag{4.3}$$

Then the equations (4.2) become

$$\sum_{0 \le a \le n-1} e_a h_k^{(2q)}(a) = 0, \qquad 1 \le k \le q-1, \tag{4.4}$$

where

$$h_k^{(2q)}(a) = \begin{cases} 1, & a \equiv 0 (\operatorname{mod} q), \\ -1, & a \equiv k (\operatorname{mod} q), \\ 0, & \text{otherwise.} \end{cases}$$

Therefore (4.4) is equivalent to the condition that

$$\#\{a \in R_i ; e_a = 1\} \text{ does not depend on } i, \tag{4.5}$$

where $R_i = \{a \in \mathbf{Z}; 0 \le a \le n-1, a (\operatorname{mod} q) = i\}$. Let $\nu : \{\pm 1\} \to \{0, 1\}$ be the map defined by $\nu(1) = 1$, $\nu(-1) = 0$. Then it follows that we have a natural bijection Φ from the set

$$N = \{(\varepsilon_0, \dots, \varepsilon_{n-1}) \in \{\pm 1\}^n ; (\varepsilon_0, \dots, \varepsilon_{n-1}) \text{ satisfies (4.2)}\}$$

to the set

$$M = \{(z_{ij} \in M(q,p); z_{ij} \in \{0,1\}, \text{ and the row sums are constant}\}$$

(where $M(q,p)$ denotes the set of $p \times q$ matrices) defined by

$$\begin{aligned} &\Phi((\varepsilon_0, \dots, \varepsilon_{n-1})) = (z_{ij}), \qquad \text{with} \\ &z_{ij} = \nu((-1)^{(i-1)+(j-1)q} e_{(i-1)+(j-1)q}), \qquad 1 \le i \le q, \quad 1 \le j \le p. \end{aligned}$$

Hence we have

$$\#(\mathbf{S}_p) = \#(M) = \sum_{0 \le i \le p} \binom{p}{i}^q .$$

This completes the proof of Proposition 4.3. □

By symmetry we have the following.

Proposition 4.4. *There exists a natural bijection between the set* $\mathbf{S}_q$ *and the set of* $p \times q$ $(0,1)$*-matrices with constant row sum. Hence there are* $\sum_{0 \le i \le q} \binom{q}{i}^p$ *such CM-types.*

Combining these two propositions we have the following.

Proposition 4.5. $\mathbf{S}_p \cap \mathbf{S}_q = \{S_{even}, S_{odd}\}$*, where*

$$S_{even} = \{2b; 0 \le b \le n-1\} \subset \mathbf{Z}/2n\mathbf{Z},$$
$$S_{odd} = \{2b+1; 0 \le b \le n-1\} \subset \mathbf{Z}/2n\mathbf{Z}.$$

In particular, the CM-types in $\mathbf{S}_p \cap \mathbf{S}_q$ *are not primitive.*

Proof. Suppose that a CM-type S belongs to $\mathbf{S}_p \cap \mathbf{S}_q$. Let $(e_0, \ldots, e_{n-1})$ be the $(0,1)$-vector which is associated to S in the proof of Proposition 4.3. Then it follows from Proposition 4.3 that $\#\{a; 0 \le a \le n-1 \text{ and } e_a = 1\}$ is divisible by q. Similarly Proposition 4.4 implies that $\#\{a; 0 \le a \le n-1 \text{ and } e_a = 1\}$ is divisible by p. Hence is divisible by pq, and we have

$$e_a = 1 \text{ (resp. } = 0) \text{ for any } a.$$

This means by (4.3) that

$$\varepsilon_a = (-1)^a, \qquad 0 \le a \le n-1,$$
$$(\text{resp. } \varepsilon_a = (-1)^{a+1},\ 0 \le a \le n-1),$$

hence we have

$$\mathbf{S}_p \cap \mathbf{S}_q = \{S_{even}, S_{odd}\}.$$

These two CM-types, however, are stable under the addition of even elements in $\mathbf{Z}/2n\mathbf{Z}$. Thus they are not primitive by Proposition 2.3. This completes the proof of Proposition 4.5. □

In order to investigate the CM-types in $\mathbf{S}_1$, a theorem in [6] plays a definite role. Let $L_{pq} = \{(c_0, \ldots, c_{pq-1}) \in \mathbf{Z}^{pq}; \sum_{0 \le i \le pq-1} c_i \zeta_{pq}^i = 0\}$, which consists of $\mathbf{Z}$-linear relations among the pq-th roots of unity. For $r = p$ (resp. q), let

$$p_i^{(r)} = (a_0, \ldots, a_{pq-1}) \in \mathbf{Z}^{pq},$$

where

$$a_j = \begin{cases} 1, & \text{if} \quad j \equiv i (\operatorname{mod} r), \\ 0, & \text{otherwise.} \end{cases}$$

It is clear that $p_i^{(p)}$, $0 \leq i \leq p-1$, $p_j^{(q)}$, $0 \leq j \leq q-1$, and hence every **Z**-linear combination of them belong to the relation module L_{pq}. The theorem in [6] asserts the converse holds too, namely

(4.6) $\quad L_{pq}$ is spanned by $p_i^{(p)}$, $0 \leq i \leq p-1$, and $p_j^{(q)}$, $0 \leq j \leq q-1$.

Using this fact we can prove the following proposition.

Proposition 4.6. *The CM-types in* $\mathbf{S}/1$ *are not primitive.*

Proof. By Proposition 2.3, it suffices to show the following.

Lemma 4.6.1. *A CM-type S belongs to $\mathbf{S}_1$ if and only if S is stable under the action of either $\mathbf{Z}/2p\mathbf{Z}$ or $\mathbf{Z}/2q\mathbf{Z}$.*

Proof of Lemma 4.6.1. We use the map $E(\bullet)$ in Proposition 4.1. Note that it gives a bijection from $\mathbf{S}_1$ to the subset

$$T_{pq} = \{(c_0, \ldots, c_{pq-1}) \in \{\pm 1\}^{pq}; \sum_{0 \leq i \leq pq-1} c_i \zeta_{pq}^i = 0\}$$

of L_{pq}. One can check easily that

(4.7) $\quad S \in \mathbf{S}_1$ is stable under the action of $\mathbf{Z}/2p\mathbf{Z}$ (resp. $\mathbf{Z}/2q\mathbf{Z}$)
if and only if
$E(S)$ is stable under the action of $\mathbf{Z}/p\mathbf{Z}$ (resp. $\mathbf{Z}/q\mathbf{Z}$).

(Here $i \in \mathbf{Z}/p\mathbf{Z}$ acts on $(c_0, \ldots, c_{pq-1}) \in \mathbf{Z}^{pq}$ by the rule

$$i.(c_0, \ldots, c_{pq-1}) = (c_{iq}, c_{iq+1}, \ldots, c_{(p+i)q-1}),$$

where the indices are regarded as elements of $\mathbf{Z}/pq\mathbf{Z}$, and the action of $\mathbf{Z}/q\mathbf{Z}$ is defined similarly.) Therefore we have only to show that

(4.8) $\quad$ if $(c_0, \ldots, c_{pq-1}) \in T_{pq}$, then $(c_0, \ldots, c_{pq-1})$ is stable
under the action of either $\mathbf{Z}/p\mathbf{Z}$ or $\mathbf{Z}/q\mathbf{Z}$.

Suppose $(c_0, \ldots, c_{pq-1}) \in T_{pq}$. Then we can express it by (4.6) as

$$(c_0, \ldots, c_{pq-1}) = \sum_{0 \le i \le p-1} a_i p_i^{(p)} + \sum_{0 \le j \le q-1} b_j p_j^{(q)}.$$

By adding or subtracting the all-one vector $(1, \ldots, 1) \in T_{pq}$, which is $\mathbf{Z}/p\mathbf{Z}$- and $\mathbf{Z}/q\mathbf{Z}$-invariant, we are reduced to showing that

(4.9) if $(d_0, \ldots, d_{pq-1}) = \sum_{0 \le i \le p-1} a_i p_i^{(p)} + \sum_{0 \le j \le q^1} b_j p_j^{(q)}$, $d_0 = 0$,
$d_i \in \{0, 1\}$, $0 \le i \le pq-1$, then $(d_0, \ldots, d_{pq-1})$ is invariant
under the action of either $\mathbf{Z}/p\mathbf{Z}$ or $\mathbf{Z}/q\mathbf{Z}$.

Let $\varphi : \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z} \to \mathbf{Z}/pq\mathbf{Z}$ denote the inverse map of the bijection $\mathbf{Z}/pq\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$ defined through the two projection maps. By the definition of $p_i^{(p)}$ and $p_j^{(q)}$, we have $d_{\varphi(i,j)} = a_i + b_j$, hence (4.9) implies that

$$a_j + b_j \in \{0, 1\} \text{ for every pair } (i, j) \in \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}. \tag{4.10}$$

It follows from the equality $d_0 = 0$ that $b_0 = -a_0$. The conditions (4.10) with $i = 0$ imply

$$b_j = -a_0, \qquad -a_0 + 1 \qquad \text{for} \qquad 1 \le j \le q-1,$$

and the conditions (4.10) with $j = 0$ imply by $b_0 = -a_0$ that

$$a_i = a_0, \qquad a_0 + 1 \qquad \text{for} \qquad 1 \le i \le p-1.$$

Suppose that there exists an i with $1 \le i \le p-1$ such that $a_i = a_0 + 1$. Then it follows from (4.10) that $b_j = -a_0$ holds for any j with $1 \le j \le q-1$. This means that

$$(d_0, \ldots, d_{pq-1}) + a_0(1, \ldots, 1) = \sum_{0 \le i \le p-1} a_i p_i^{(p)},$$

hence $(d_0, \ldots, d_{pq-1})$ is $\mathbf{Z}/q\mathbf{Z}$-invariant. On the contrary, suppose that there exists no i with $1 \le i \le p-1$ such that $a_i = a_0 + 1$. Then it follows from (4.10) that

$$(d_0, \ldots, d_{pq-1}) - a_0(1, \ldots, 1) = \sum_{0 \le j \le q-1} b_j p_j^{(q)},$$

hence $(d_0, \dots, d_{pq-1})$ is $\mathbf{Z}/p\mathbf{Z}$-invariant. Thus we complete the proof of Lemma 4.6.1 and at the same time that of Proposition 4.6. □

Let **CM** denote the set of CM-types for $\mathbf{Z}/2n\mathbf{Z}$.

Proposition 4.7. *Let r denote p or q. Then we have*

$$\mathbf{S}_1 \cap \mathbf{S}_r = \left\{ S \in \mathbf{CM}; E(S) = \sum_{0 \le i \le r-1} \varepsilon_i \chi_i^{(r)} \quad \textit{for some} \quad (\varepsilon_0, \dots, \varepsilon_{r-1}) \in \{\pm 1\}^r \right\}, \tag{4.11}$$

where $\chi_i^{(p)}$ denotes the characteristic function of the residue class $R_i^{(r)}$, $0 \le i \le r-1$, of $i \bmod r$. In particular

$$\#(\mathbf{S}_1 \cap \mathbf{S}_p) = 2^p,$$
$$\#(\mathbf{S}_1 \cap \mathbf{S}_q) = 2^q.$$

Proof. We may assume that $r = p$. Suppose that a CM-type S belongs to the right hand side of (4.11), so that $E(S) = \sum_{0 \le j \le p-1} \varepsilon_j \chi_j^{(p)}$ for some $(\varepsilon_0, \dots, \varepsilon_{r-1}) \in \{\pm 1\}^r$. Then $E(S)$ is stable under the action of $\mathbf{Z}/p\mathbf{Z}$ and it follows from Lemma 4.6.1 that $S \in \mathbf{S}_1$. Moreover $\sum_{b \in R_i^{(q)}} E(S)(b) = \sum_{0 \le j \le p-1} \varepsilon_j$ for any i, since p and q are coprime, hence it follows from Proposition 4.3 that $S \in \mathbf{S}_p$. Conversely, suppose that $S \in \mathbf{S}_1 \cap \mathbf{S}_p$. By Proposition 4.3, it follows from $S \in \mathbf{S}_p$ that

$$\sum_{b \in R_i^{(q)}} E(S)(b) \text{ is constant for } 0 \le i \le q-1. \tag{4.12}$$

By Proposition 4.6, it follows from $S \in \mathbf{S}_1$ that $E(S)$ is invariant under $\mathbf{Z}/p\mathbf{Z}$- or $\mathbf{Z}/q\mathbf{Z}$-action. Suppose first that $E(S)$ is invariant under $\mathbf{Z}/p\mathbf{Z}$-action. Then (4.12) implies that

$$E(S)(b) = 1 \qquad \text{for any} \qquad b \in \mathbf{Z}/pq\mathbf{Z}$$

or

$$E(S)(b) = -1 \qquad \text{for any} \qquad b \in \mathbf{Z}/pq\mathbf{Z}.$$

Hence S belongs to the right hand side of (4.11). Suppose next that $E(S)$ is invariant under $\mathbf{Z}/q\mathbf{Z}$-action. Then it can be expressed as

$$E(S) = \sum_{0 \le i \le p-1} \varepsilon_i \chi_i^{(p)} \qquad \text{for some} \qquad (\varepsilon_0, \dots, \varepsilon_{p-1}) \in \{\pm 1\}^p,$$

hence S belongs to the right hand side of (4.11) too. This completes the proof of Proposition 4.7. □

Summing up we obtain the following theorem, of which the assertion (iv), (v), and (vi) will be proved in the next section.

Theorem 4.8. *Let p, q be distinct odd primes. Let* **CM** *denote the set of CM-types for a cyclic galois CM-field of degree $2pq$. Let* **Deg** *denote the subset of* **CM** *consisting of degenerate CM-types, and* **Prim** *(resp.* **NonPrim***) the subset of primitive (resp. nonprimitive) CM-types. Let N-***Dom** *denote the subset of* **CM** *consisting of N-dominated CM-types. Moreover for any divisor d of $2pq$, let*

$$\mathbf{S}_d = \{S \in \mathbf{CM}; \chi(S) = 0 \textit{ for one (hence every) character of degree } 2pq/(d, 2pq)\}.$$

Then

(i) $\mathbf{CM} = \mathbf{Prim} \cup \mathbf{Nonprim}$ *(disjoint sum),*

(ii) $\mathbf{Deg} = \mathbf{S}_1 \cup \mathbf{S}_p \cup \mathbf{S}_q$, *where*

$$\mathbf{S}_p \cap \mathbf{S}_q = \{\{2b; 0 \le b \le pq-1\}, \{2b+1; 0 \le b \le pq-1\}\} \subset \mathbf{S}_1,$$

(iii) $\mathbf{Nonprim} = \mathbf{S}_1$,

(iv) $\mathbf{Prim} \cap p - \mathbf{Dom} = \mathbf{S}_p - \mathbf{S}_1$,

(v) $\mathbf{Prim} \cap q - \mathbf{Dom} = \mathbf{S}_q - \mathbf{S}_1$,

(vi) *all the primitive and degenerate CM-types are 1-degenerate in the sense of Section two.*

Furthermore the numbers of elements of $\mathbf{S}_1$, $\mathbf{S}_p$, $\mathbf{S}_q$ *and their intersections are given by*

$$\begin{aligned}
&\#(\mathbf{S}_1) = 2^p + 2^q - 2,\\
&\#(\mathbf{S}_p) = \sum_{0 \le i \le p} \binom{p}{i}^q,\\
&\#(\mathbf{S}_q) = \sum_{0 \le i \le q} \binom{q}{i}^p,\\
&\#(\mathbf{S}_1 \cap \mathbf{S}_p) = 2^p,\\
&\#(\mathbf{S}_1 \cap \mathbf{S}_q) = 2^q,\\
&\#(\mathbf{S}_p \cap \mathbf{S}_q) = \#(\mathbf{S}_1 \cap \mathbf{S}_p \cap \mathbf{S}_q) = 2.
\end{aligned}$$

Remark 4.9. For sufficiently large prime $2n+1 \equiv 7 (\mathrm{mod}\, 12)$, Lenstra and Stark noticed that there is always a degenerate CM-type for $\mathbf{Q}(\zeta_{2n+1})$ (see [5, (3.11)]). But the congruence means that $n = 3$ (*an odd integer*). Hence our theorem for $p = 3$ gives a constructive version of this result to the effect that there is always a degenerate CM-type for $\mathbf{Q}(\zeta_{2n+1})$ whenever n is the product of three and an odd prime > 3.

Remark 4.10. It is shown by Lenstra that for any abelian variety A with complex multiplication by an *abelian* CM-field, there always exists a nondivisorial Hodge cycle on A itself if A is degenerate (see [7]). Our theorem, however, gives stronger results for the case of cyclic CM-fields of degree $2pq$ that the whole Hodge rings $\mathcal{H}(A^k)$, $k \ge 1$, of its self-products are generated (up to distribution-equivalence) by Hodge cycles on A, if A is degenerate. In particular, the Hodge conjecture for A^k, $k \ge 1$, is implied by the truth of the conjecture for A.

Remark 4.11. Theorem 4.8 cannot be generalized as it is to the case when n is the product of three distinct odd primes. This is due to the fact that the equality (iii) **Nonprim** $= \mathbf{S}_1$ in the theorem does not hold generally for such an n as is shown in the examples of [5, (3.14)].

5. N-dominatedness

In this section we investigate the *N-dominatedness* and *h-degeneracy* of the degenerate CM-types for the cyclic CM-fields of degree $2pq$, and complete the proof of the assertions (iv), (v), and (vi) of Theorem 4.8.

By Theorem 4.8, (ii) and (iii), if a CM-type S is degenerate and primitive, then $S \in \mathbf{S}_p - \mathbf{S}_1$ or $S \in \mathbf{S}_q - \mathbf{S}_1$. Hence it suffices to consider the case $S \in \mathbf{S}_p - \mathbf{S}_1$. A Hodge cycle on a self-product A^k of A is said to be *proper* if it does not come from the ones of lower codimension by intersecting with a divisor. As is explained in [1], there is a natural bijective map between the set of (additive) basis elements of the space of proper Hodge cycles on a self-product A^k, $k \geq 1$, and the set of nontrivial nonnegative function $h : \mathbf{Z}/2n\mathbf{Z} \to \mathbf{Z}_{\geq 0}$ such that

$$(5.1) \qquad \begin{aligned} &h(a)h(a+n) = 0 \qquad \text{and} \\ &\langle h, f_{a+S} \rangle = 0 \qquad \text{for any} \qquad a \in \mathbf{Z}/2n\mathbf{Z}. \end{aligned}$$

Here we denote by $\langle , \rangle$ the natural inner product of functions on $\mathbf{Z}/2n\mathbf{Z}$ defined by $\langle f, g \rangle = \sum_{a \in \mathbf{Z}/2n\mathbf{Z}} f(a)g(a)$. To a function $h : \mathbf{Z}/2n\mathbf{Z} \to \mathbf{Z}_{\geq 0}$ satisfying the condition (5.1), we associate an odd function $\hat{h} : \mathbf{Z}_2n\mathbf{Z} \to \mathbf{Z}$ defined by

$$(5.2) \qquad \hat{h}(a) = \begin{cases} h(a), & \text{if} \quad h(a) \neq 0, \\ -h(a+n), & \text{if} \quad h(a) = 0. \end{cases}$$

This correspondence $F : h \mapsto \hat{h}$ defines a bijective map between the set

$$\{h : \mathbf{Z}/2n\mathbf{Z} \to \mathbf{Z}_{\geq 0}; h(a)h(a+n) = 0\}$$

and the set

$$\{h : \mathbf{Z}/2n\mathbf{Z} \to \mathbf{Z}; h \text{ is off}\}.$$

Moreover for any odd function f, $\langle h, f \rangle = 0$ if and only if $\langle \hat{h}, f \rangle = 0$. Note that the space of odd $\mathbf{C}$-(resp. $\mathbf{Z}$-)valued functions on $\mathbf{Z}/2n\mathbf{Z}$ is identified naturally with the *minus* part of the group algebra $\mathbf{C}[\mathbf{Z}/2n\mathbf{Z}]^-$ (resp. $\mathbf{Z}[\mathbf{Z}/2n\mathbf{Z}]^-$). Since $S \in \mathbf{S}_p - (\mathbf{S}_1 \cup \mathbf{S}_q \cup \mathbf{S}_{pq})$ by our assumption, the condition (5.2) is equivalent to

$$(5.3) \qquad h \in V_{2q} \cap \mathbf{Z}[\mathbf{Z}/2n\mathbf{Z}].$$

But, by Proposition 3.2, we already know that a $\mathbf{Z}$-basis of $V_{2q} \cap \mathbf{Z}[\mathbf{Z}/2n\mathbf{Z}]$ is given by $w_k^{(2q)}$, $1 \leq k \leq q-1$. Moreover the weight of the inverses $F^{-1}(w_k^{(2q)})$, $q \leq k \leq q-1$, are equal to p for any k. Therefore the abelian variety A is p-dominated. Furthermore the height of them are equal to one for any k. Therefore the abelian variety A is 1-degenerate. Thus we complete the proof of the assertions (iv), (v), and (vi) of Theorem 4.8.

6. Examples

In this section we apply our theory to construct some examples of degenerate abelian varieties with complex multiplication by a cyclotomic field.

Let $K_n = \mathbf{Q}(\zeta_n)$, the n-th cyclotomic extension of $\mathbf{Q}$, and let $G_n = Gal(K_n/\mathbf{Q})$. When $n = 31$, we have $G_{31} \cong (\mathbf{Z}/31\mathbf{Z})^*$. We use the primitive root $3 \in (\mathbf{Z}/31\mathbf{Z})^*$ to specify an isomorphism $G_{31} \cong \mathbf{Z}/30\mathbf{Z}$. The matrix $(a_{ij}) \in M(5,3)$ defined by

$$\begin{cases} a_{i1} = 1, & 1 \leq i \leq 5, \\ a_{ij} = 0, & j \geq 2, \end{cases}$$

satisfies the condition specified in Proposition 4.3 when $p = 3$, $q = 5$. In the notation used in the proof of the proposition, this matrix corresponds to $(e_0, \ldots, e_{14})$ with

$$e_i = \begin{cases} 1, & 0 \leq i \leq 4, \\ -1, & 5 \leq i \leq 14. \end{cases}$$

Furthermore this vector corresponds by (4.3) to $(\varepsilon_0, \ldots, \varepsilon_{14})$ with

$$\varepsilon_i = \begin{cases} (-1)^i, & 0 \leq i \leq 4, \\ (-1)^{i+1}, & 5 \leq i \leq 14. \end{cases}$$

Hence this gives the CM-type

$$S = \{1, -9, 19, -16, 20, 25, -8, 10, , -28, 4, -5, 14, -2, 18, -7\} \subset (\mathbf{Z}/31\mathbf{Z})^*.$$

Since $S \in \mathbf{S}_3 - \mathbf{S}_1$ by Proposition 4.3 and 4.6, the abelian variety A_S associated to it is absolutely simple and 3-dominated by Theorem 4.8. This is a member of the set of $\sum_{0 \leq i \leq 3} \binom{3}{i}^5 - 2^3 = 480$ of 3-dominated absolutely simple abelian varieties with complex multiplication by K_{31}. If we define another matrix $(b_{ij}) \in M(3,5)$ by

$$\begin{cases} b_{i1} = 1, & 1 \leq i \leq 3, \\ b_{ij} = 0, & \text{otherwise.} \end{cases}$$

then it corresponds to the CM-type

$$T = \{1, -9, 19, 16, -20, 25, -8, 10, , -28, 4, -5, 14, -2, 18, -7\} \subset (\mathbf{Z}/31\mathbf{Z})^*.$$

Since $T \in \mathbf{S}_5 - \mathbf{S}_1$ by Proposition 4.3 and 4.6, the abelian variety A^T associated to it is absolutely simple and 5-dominated by Theorem 4.8. This is a member of the set of $\sum_{0 \leq i \leq 5} \binom{5}{i}^3 - 2^5 = 2220$ of 5-dominated absolutely simple abelian varieties with complex multiplication by K_{31}.

References

[1] Hazama, F., Hodge cycles on abelian varieties of -type, J. Alg. Geom. **9** (2000), 711–753.

[2] Hazama, F., On the existence of N-dominated abelian varieties of CM-type, Far East J. Math. Sci. **2** (2000), 713–730.

[3] Hazama, F., General Hodge conjecture for abelian varieties of CM-type, Proc. Japan Acad. **78** (2002), 72–75.

[4] Kubota, T., On the field extension by complex multiplication, Trans. Amer. Math. Soc. **118** (1965), 113–122.

[5] Ribet, K. A., Division fields of abelian varieties with complex multiplication, Mem. Soc. Math. France (2e serie) **2** (1980), 75–94.

[6] Schoenberg, I. J., A note on the cyclotomic polynomial, Mathematika **11** (1964), 131–136.

[7] White, S. P., Sporadic cycles on CM abelian varieties, Compositio Math. **88** (1993), 123–142.

(Received September 20, 2002)

Department of Natural Sciences
College of Science and Engineering
Tokyo Denki University
Hatoyama, Saitama 350-0394
JAPAN