TOKYO J. MATH.
VOL. 27, NO. 2, 2004

The Hodge Conjecture for The Jacobian Varieties of Generalized Catalan Curves

Noboru AOKI

Rikkyo University

(Communicated by S. Miyoshi)

Abstract. In this paper we prove that the Hodge conjecture is true for any self-product of the jacobian variety $J(C_{p^\mu,q^\nu})$ of the curve $C_{p^\mu,q^\nu} : y^{q^\nu} = x^{p^\mu} - 1$, where p^μ and q^ν are powers of distinct prime numbers p and q. We also prove that the Hodge ring of $J(C_{p^\mu,q^\nu})$ is *not* generated by the divisor classes whenever $p^\mu q^\nu \neq 12$ and $(\mu, \nu) \neq (1, 1)$.

1. Introduction

Let A be an abelian variety over the complex number field $\mathbf{C}$. Let $\mathscr{B}^*(A)$ be the Hodge ring of A and $\mathscr{C}^*(A)$ the subring of $\mathscr{B}^*(A)$ generated by the cohomology classes of algebraic cycles on A. The Hodge conjecture for A, which we will refer to HC(A) in this paper, asserts that the equality $\mathscr{B}^*(A) = \mathscr{C}^*(A)$ holds. If we denote by $\mathscr{D}^*(A)$ the subring of $\mathscr{C}^*(A)$ generated by the divisor classes, then the equality $\mathscr{B}^*(A) = \mathscr{D}^*(A)$ implies HC(A). We say that A is *nondegenerate* (resp. *degenerate*) if $\mathscr{B}^*(A) = \mathscr{D}^*(A)$ (resp. $\mathscr{B}^*(A) \neq \mathscr{D}^*(A)$). If $\mathscr{B}^*(A^k) = \mathscr{D}^*(A^k)$ for all $k \geq 1$, then we say that A is *stably nondegenerate* ([7]). It is clear that stably nondegeneracy implies nondegeneracy, but the converse does not always hold. However, Lenstra proved that the converse does hold if A is a CM abelian variety whose CM-field is an abelian field. A special class of such abelian varieties will be the main object in this paper

For powers p^μ, q^ν (> 1) of distinct prime numbers p, q, we consider the curve

$$C_{p^\mu,q^\nu} : y^{q^\nu} = x^{p^\mu} - 1 \tag{1}$$

defined over $\mathbf{C}$. We call this curve a *generalized Catalan curve*. (The curve $C_{p,q}$ is the usual Catalan curve.) The starting point of this paper is the following theorem:

THEOREM 1.1 (Kubota-Hazama). *The jacobian variety $J(C_{p,q})$ of the Catalan curve $C_{p,q}$ is simple and stably nondegenerate. In other words, the equality $\mathscr{B}^*(J(C_{p,q})^k) = \mathscr{D}^*(J(C_{p,q})^k)$ holds for all $k \geq 1$. In particular,* HC$(J(C_{p,q})^k)$ *is true for all $k \geq 1$.*

Received January 23, 2003

This theorem was proved by Kubota ([12]) when one of p, q is 2, and the other cases were proved by Hazama ([9]). If $(\mu, \nu) \neq (1,1)$, then $J(C_{p^\mu,q^\nu})$ is no longer simple since there is a nontrivial homomorphism from $J(C_{p^\mu,q^\nu})$ to $J(C_{p,q})$. Nevertheless, we can generalize Theorem 1.1 as follows.

THEOREM 1.2 (cf. Corollary 7.2 and Theorem 8.1). *Suppose neither p^μ nor q^ν equals 4. Then every simple factor of $J(C_{p^\mu,q^\nu})$ is stably nondegenerate. If $(\mu, \nu) \neq (1,1)$, then $J(C_{p^\mu,q^\nu})$ itself is degenerate. More precisely, $\mathscr{B}^d(J(C_{p^\mu,q^\nu})) \neq \mathscr{D}^d(J(C_{p^\mu,q^\nu}))$ for $d = p+1, q+1$ and $\frac{1}{2}(p+1)(q+1)$.*

We shall prove a similar but slightly complicated result when either $p^\mu = 4$ or $q^\nu = 4$ (see Theorem 7.1).

As for the Hodge conjecture for degnerate abelian varieties, only a few cases have been studied (see [18], [24], [21] and [4]). In spite of degeneracy of $J(C_{p^\mu,q^\nu})$, however, we can prove the following theorem, which provides a new example of degenerate abelian variety for which the Hodge conjecture is true.

THEOREM 1.3 (cf. Theorem 8.2). *For all $k \geq 1$, $\mathrm{HC}(J(C_{p^\mu,q^\nu})^k)$ is true.*

It is easy to see that the jacobian variety $J(C_{p^\mu,q^\nu})$ of C_{p^μ,q^ν} is an abelian variety of CM type. More precisely, every simple factor of $J(C_{p^\mu,q^\nu})$ is a CM abelian variety whose CM-field is an abelian field contained in $\mathbf{Q}(\zeta_m)$, where $m = p^\mu q^\nu$ and ζ_m denotes a primitive m-th root of unity. For example, $\mathrm{End}(J(C_{p,q})) \otimes \mathbf{Q} = \mathbf{Q}(\zeta_{pq})$. We prove the first statemant of Theorem 1.2 essentially in the same way as Kubota and Hazama proved Theorem 1.1. They made use of an explicit description of the CM-type of $J(C_{p,q})$, while we resort to an expression of the CM-type in terms of Stickelberger elements (Proposition 6.2). This expression, which simplifies the argument in the proof, is a consequence of the fact that C_{p^μ,q^ν} is a quotient of the Fermat curve $X_m^1 : x^m + y^m + z^m = 0$ of degree $m = p^\mu q^\nu$.

Now, suppose m is an arbitrary positive integer. If C is a quotient of the Fermat curve X_m^1 of degree m, then $\mathrm{HC}(J(C)^k)$ for the jacobian variety $J(C)$ of C follows from $\mathrm{HC}((X_m^1)^{gk})$, where g denotes the genus of X_m^1. Therefore, by the theory of inductive structure due to Shioda [20], $\mathrm{HC}(J(C_{p^\mu,q^\nu})^k)$ will follow from $\mathrm{HC}(X_m^N)$, where X_m^N is the Fermat variety of degree m and of sufficiently large dimension N. In this way, Shioda [21] succeeded in proving $\mathrm{HC}(J(C)^k)$ for all $k \geq 1$ when m is a prime number or $m \leq 20$, and our previous papers [4], [5] generalized his result to some extent. However, the same proof does not work when we consider the generalized Catalan curves, since the Hodge conjecture is still remained to be proved for the Fermat varieties of degree pq if $p, q > 2$ and $pq \neq 15, 21$. To prove Theorem 1.3, we shall show that every Hodge cycle on $J(C_{p^\mu,q^\nu})$ comes (via Shioda's inductive structure) from the Hodge cyclces on a Fermat variety of degree m corresponding to “standard elements". Then the work of [20], [15] and [2] proving that such Hodge cycles are algebraic will establish Theorem 1.3.

2. Preliminaries

We start with a brief review about the Hodge conjecture. We refer the reader to [22] and [13] for more details. Let X be a non-singular projective variety over $\mathbf{C}$. For each integer d with $0 \le d \le \dim X$, let

$$\mathscr{B}^d(X) = H^{2d}(X, \mathbf{Q}) \cap H^{d,d}(X)$$

be the space of Hodge cycles of codimension d on X. Let $\mathscr{C}^d(X)$ be the subspace of $\mathscr{B}^d(X)$ generated by the classes of algebraic cycles of codimension d on X and $\mathscr{D}^d(X)$ the subspace of classes of intersections of d divisors on X. We then have inclusions

$$\mathscr{B}^d(X) \supseteq \mathscr{C}^d(X) \supseteq \mathscr{D}^d(X)\,.$$

We denote by HC(X) the Hodge conjecture for X which asserts that the equality $\mathscr{B}^d(X) = \mathscr{C}^d(X)$ holds in all codimension d. If a subspace V of $H^{2d}(X, \mathbf{Q})$ (resp. $H^{2d}(X, \mathbf{C})$) is contained in $\mathscr{C}^d(X)$ (resp. $\mathscr{C}^d(X) \otimes \mathbf{C}$), then we say that V is *algebraic*. In this terminology, HC(X) asserts that $\mathscr{B}^d(X)$ is algebraic for any d.

Let A be an abelian variety of dimension g defined over $\mathbf{C}$. Let

$$\mathscr{B}^*(A) = \bigoplus_{i=0}^{g} \mathscr{B}^i(A) \tag{2}$$

be the Hodge ring of A and $\mathscr{C}^*(A)$ (resp. $\mathscr{D}^*(A)$) the subring of the Hodge ring generated by the classes of algebraic cycles (resp. divisors) on A. Clearly we have

$$\mathscr{B}^*(A) \supseteq \mathscr{C}^*(A) \supseteq \mathscr{D}^*(A)\,. \tag{3}$$

We say that A is *nondegenerate* if the equality $\mathscr{B}^*(A) = \mathscr{D}^*(A)$ holds. Thus, if A is nondegenerate, then it is clear from (3) that HC(A) is true. We say that A is *stably nondegenerate* if $\mathscr{B}^*(A^k) = \mathscr{D}^*(A^k)$ for all $k \ge 1$ ([6], [7] and [8]).

If there exists a CM-field K of degree $2g$ and an injective ring homomorphism

$$\theta : K \to \mathrm{End}(A) \otimes \mathbf{Q}\,,$$

then we call A a *CM abelian variety of type* (K, θ). Let (K, Φ) be the CM-type of (A, θ) and (K^*, Φ^*) its reflex in the sense of Shimura-Taniyama [19]. For simplicity we consider only the case where K is a Galois extension of $\mathbf{Q}$, which is sufficient for our purpose. Let Γ be the Galois group of the extension $K/\mathbf{Q}$, and define a subgroup $W(\Phi)$ of Γ by

$$W(\Phi) = \{\sigma \in \Gamma \mid \sigma\Phi = \Phi\}\,. \tag{4}$$

PROPOSITION 2.1. *Natation being as above, A is simple if and only if* $W(\Phi) = \{1\}$. *More generally, A is isogenuous to* $B \times \cdots \times B$ *(*$|W(\Phi)|$*-times), where B is a simple CM abelian variety such that* $\mathrm{End}(B) \otimes \mathbf{Q} = K^{W(\Phi)}$, *the fixed field of* $W(\Phi)$.

PROOF. See [19] or [17]. □

For any number field F of finite degree, let $T_F = \mathrm{Res}_{F/\mathbf{Q}}(\mathbf{G}_{m/F})$ be the Weil restriction of the multiplicative group $\mathbf{G}_{m/F}$ over F. Then the CM-type Φ induces an algebraic homomorphism $f_\Phi : T_K \to T_{K^*}$ and $\dim(\mathrm{Im}\Phi) \leq g+1$. We say that the CM-type Φ is *nondegenerate* if $\dim(\mathrm{Im} f_\Phi) = g+1$ (for details see [12] and [16]).

Now, suppose K is an abelian field. For any character χ of Γ, let

$$\chi(\Phi) = \sum_{\sigma \in \Phi} \chi(\sigma) .$$

We say that χ is *odd* if $\chi(\rho) = -1$, where ρ denotes the complex conjugation. Then the following propopsition is well known:

PROPOSITION 2.2. *Let A be a simple CM abelian variety with CM type (K, Φ). Assume that K is an abelian extension of* $\mathbf{Q}$. *Then the following four conditions are equivalent*:

i) *A is stably nondegenerate.*
ii) *A is nondegenerate.*
iii) *Φ is nondegenerate.*
iv) *$\chi(\Phi) \neq 0$ for all odd character χ of Γ.*

PROOF. The implication (i) $\Rightarrow$ (ii) is clear. The converse implication (ii) $\Rightarrow$ (i) was proved by Lenstra (see [26]). Hazama [6] proved that (i) is equivalent to (iii). (Actually he proved the equaivalence in more general cases.) The equivalence of (iii) and (iv) is easy. □

3. Fermat varieties

In this section we recall some fundamental properties on the Fermat varieties from [20], [23], [15] and [2]. We begin with the definition of the Fermat variety. Let $m > 1$ be an integer and n a non-negative integer. The Fermat variety X_m^n over $\mathbf{C}$ of degree m and dimension n is a hypersurface in the $(n+1)$-dimensional projective space $\mathbf{P}^{n+1}$ over $\mathbf{C}$ defined by the equation

$$x_0^m + x_1^m + \cdots + x_{n+1}^m = 0 .$$

Let μ_m be the group of m-th roots of unity in $\mathbf{C}$ and set $G_m^n = (\mu_m)^{n+2}/\text{diagonal}$. Then $g = [\zeta_0, \cdots, \zeta_{n+1}] \in G_m^n$ acts on X_m^n by setting $g \cdot (x_0 : \cdots : x_{n+1}) = (\zeta_0 x_0 : \cdots : \zeta_{n+1} x_{n+1})$. Hence G_m^n induces an action on the cohomology group $H^n(X_m^n, \mathbf{C})$. Let

$$\mathfrak{A}_m^n = \left\{ (a_0, a_1, \cdots, a_{n+1}) \in \mathbf{Z}^{n+2} \;\middle|\; 0 < a_i < m,\ \sum_{i=0}^{n+1} a_i \equiv 0 \ (\mathrm{mod}\ m) \right\} .$$

Note that $\mathfrak{A}_m^n$ can be naturally viewd as a subset of the chracter group $(G_m^n)^*$ of G_m^n; if $\alpha = (a_0, \cdots, a_{n+1}) \in \mathfrak{A}_m^n$ and $g = [\zeta_0, \cdots, \zeta_{n+1}] \in G_m^n$, then $\alpha(g) = \zeta_0^{a_0} \cdots \zeta_{n+1}^{a_{n+1}} \in \mu_m$. For each $\alpha \in (G_m^n)^*$, let

$$V(\alpha) = \{\xi \in H^n(X_m^n, \mathbf{C}) \mid g^* \xi = \alpha(g) \xi \ (\forall g \in G_m^n)\} .$$

For any $\alpha = (a_0, \cdots, a_{n+1}) \in \mathfrak{A}_m^n$ the number

$$|\alpha| = \frac{a_0 + \cdots + a_{n+1}}{m}$$

is an integer such that $1 \leq |\alpha| \leq n+1$. We define the action of $t \in (\mathbf{Z}/m\mathbf{Z})^\times$ on $\alpha \in \mathfrak{A}_m^n$ by the rule

$$t \cdot \alpha = (\langle ta_0 \rangle_m, \cdots, \langle ta_{n+1} \rangle_m)\,,$$

where for $a \in \mathbf{Z}$ and $t \in (\mathbf{Z}/m\mathbf{Z})^\times$, $\langle ta \rangle_m$ denotes the unique integer such that $0 \leq \langle ta \rangle_m < m$ and $\langle ta \rangle_m \equiv ta \pmod{m}$. It is then easy to see that

$$|\alpha| + |(-1) \cdot \alpha| = n + 2\,. \tag{5}$$

If n is even, we define a subset $\mathfrak{B}_m^n$ of $\mathfrak{A}_m^n$ by

$$\mathfrak{B}_m^n = \left\{ \alpha \in \mathfrak{A}_m^n \;\middle|\; |t \cdot \alpha| = \frac{n}{2} + 1 \ (\forall t \in (\mathbf{Z}/m\mathbf{Z})^\times) \right\}.$$

The importance of two sets $\mathfrak{A}_m^n$ and $\mathfrak{B}_m^n$ is clear from the following theorem:

THEOREM 3.1. *Let $V(0)$ be the eigenspace of $H^n(X_m^n, \mathbf{C})$ for the trivial character $0 \in (G_m^n)^*$. Then* $\dim V(0) = 1$ *or* 0 *according as n is even or odd. Moreover the following statements hold.*

(i) *The eigenspace decomposition of $H^n(X_m^n, \mathbf{C})$ with respect to the action of G_m^n is given by*

$$H^n(X_m^n, \mathbf{C}) = V(0) \oplus \bigoplus_{\alpha \in \mathfrak{A}_m^n} V(\alpha)$$

and $\dim V(\alpha) = 1$ *for all* $\alpha \in \mathfrak{A}_m^n$.

(ii) *If $n = 2r$ is even, then the* $\mathbf{C}$*-span of Hodge cycles of codimension r on X_m^n is given by*

$$\mathscr{B}^r(X_m^n) \otimes \mathbf{C} = V(0) \oplus \bigoplus_{\alpha \in \mathfrak{B}_m^n} V(\alpha)\,.$$

PROOF. See [20, Theorem I]. □

To take a close look at the structure of the set $\mathfrak{B}_m^n$, it is convenient to consider $\mathfrak{B}_m^n$ for all n simultaneously. For this purpose, let

$$\mathfrak{R}_m = \bigcup_{r=1}^{\infty} (\mathbf{Z}/m\mathbf{Z} \setminus \{0\})^r$$

be the disjoint union of $(\mathbf{Z}/m\mathbf{Z} \setminus \{0\})^r$ for all r. For $\alpha = (a_1, \cdots, a_r)$, $\beta = (b_1, \cdots, b_s) \in \mathfrak{R}_m$, let

$$\alpha * \beta = (a_1, \cdots, a_r, b_1, \cdots, b_s) \in \mathfrak{R}_m\,.$$

Then $\mathfrak{R}_m$ becomes a monoid with respect to the operation $*$. For two elements $\alpha, \beta \in \mathfrak{R}_m$ we write $\alpha \sim \beta$ if α is equal to β up to permutation of components. If $n = 2r$ is even, we define a subset $\mathfrak{D}_m^n$ of $\mathfrak{A}_m^n$ as follows:

$$\mathfrak{D}_m^n = \{\alpha \in \mathfrak{A}_m^n \mid \alpha \sim (a_0, m - a_0, \cdots, a_r, m - a_r) \text{ for some } a_0, \cdots, a_r\}\,.$$

Using (5), one can easily see that $\mathfrak{D}_m^n \subseteq \mathfrak{B}_m^n$. Consider the following two subsets of $\mathfrak{R}_m$:

$$\mathfrak{B}_m = \bigcup \mathfrak{B}_m^n\,, \quad \mathfrak{D}_m = \bigcup \mathfrak{D}_m^n\,,$$

where the unions are taken over all positive even integers n. Then it is clear that both $\mathfrak{B}_m$ and $\mathfrak{D}_m$ are submonoid of $\mathfrak{R}_m$ and that $\mathfrak{B}_m \supseteq \mathfrak{D}_m$. (The monoid $\mathfrak{B}_m$ is nothing but M_m studied in [20].)

If m is divisible by a prime number p with $p < m$, then we define a *standard element* ([1]) by

$$\sigma_{p,a} = \begin{cases} \left(a, a + \dfrac{m}{p}, a + \dfrac{2m}{p}, \cdots, a + \dfrac{(p-1)m}{p}, m - pa\right) & \text{if } p \geq 3\,, \\ \left(a, a + \dfrac{m}{2}, m - 2a, \dfrac{m}{2}\right) & \text{if } p = 2\,, \end{cases} \tag{6}$$

where a is an integer such that $ap \not\equiv 0 \pmod m$. For each prime number p, let

$$n(p) = \begin{cases} 2 & \text{if } p = 2\,, \\ p - 1 & \text{if } p > 2\,. \end{cases} \tag{7}$$

Then it is known that $\sigma_{p,a} \in \mathfrak{B}_m^{n(p)} \setminus \mathfrak{D}_m^{n(p)}$. We denote by $\mathfrak{S}_m$ the set of elements $\alpha \in \mathfrak{R}_m$ for which there exist some $\delta, \delta' \in \mathfrak{D}_m$ and some standard elements $\sigma_1, \cdots, \sigma_k$ such that

$$\alpha * \delta \sim \sigma_1 * \cdots * \sigma_k * \delta'\,.$$

It is clear from the definition that the following inclusions hold:

$$\mathfrak{B}_m \supseteq \mathfrak{S}_m \supseteq \mathfrak{D}_m\,.$$

Let $\mathfrak{S}_m^n = \mathfrak{S}_m \cap \mathfrak{A}_m^n$. The following theorem will play a fundamental role in the proof of Theorem 1.3.

THEOREM 3.2. *If $\alpha \in \mathfrak{S}_m^n$, then $V(\alpha) \subset \mathscr{B}^{n/2}(X_m^n)$ is algebraic.*

PROOF. The assertion for $\alpha \in \mathfrak{D}_m^n$ is proved by Shioda [20] and Ran [15]. For the algebraicity of $V(\alpha)$ for $\alpha \in \mathfrak{S}_m^n \setminus \mathfrak{D}_m^n$, see [20] and [2]. □

4. Abelian varieties of Fermat type

Every element $g \in G_m^1$ induces an automorphism g^* of the jacobian variety $J(X_m^1)$ of X_m^1. Then the natural isomorphism $H^1(J(X_m^1), \mathbf{C}) \cong H^1(X_m^1, \mathbf{C})$ is G_m^1-equivariant. By

Theorem 3.1, we have the eigenspace decomposition of $H^1(J(X_m^1), \mathbf{C})$ with respect to the action of G_m^1:

$$H^1(J(X_m^1), \mathbf{C}) = \bigoplus_{\alpha \in \mathfrak{A}_m^1} U(\alpha)\,, \tag{8}$$

where $U(\alpha) \cong V(\alpha)$ (as G_m^1-modules) is one-dimensional for all $\alpha \in \mathfrak{A}_m^1$. Recall that the group $(\mathbf{Z}/m\mathbf{Z})^\times$ acts on $\mathfrak{A}_m^1$. We denote by $\Omega_m = (\mathbf{Z}/m\mathbf{Z})^\times \backslash \mathfrak{A}_m^1$ the orbit space. The following proposition is well known.

PROPOSITION 4.1. *For each $S \in \Omega_m$, let $m_S = m/\mathrm{GCD}(\alpha)$ and ζ_{m_S} a primitive m_S-th root of unity. Then there exists an abelian variety A_S of dimension $\frac{1}{2}\varphi(m_S)$ with the following properties*:

(i) *There exists an isogeny*

$$\pi : J(X_m^1) \to \prod_{S \in \Omega_m} A_S\,.$$

Moreover, if we denote by π_S the composite map of π and the projection to A_S, then

$$H^1(A_S, \mathbf{C}) = \bigoplus_{\alpha \in S} W(\alpha)\,,$$

where $W(\alpha)$ is one-dimensional subspace of $H^1(A_S, \mathbf{C})$ such that $\pi_S^* W(\alpha) = U(\alpha)$.

(ii) *If we fix an element $\alpha \in S$ with $|\alpha| = 1$, then there is an injective ring homomorphism*

$$\theta_\alpha : \mathbf{Z}[\zeta_{m_S}] \to \mathrm{End}(A_S)$$

such that $\theta_\alpha(\alpha(g)) = g^*$ for all $g \in G_m^1$. The CM-type of (A_S, θ_α) is given by

$$\Phi_\alpha = \{t \in (\mathbf{Z}/m\mathbf{Z})^\times \mid |t \cdot \alpha| = 1\}\,.$$

(*Here we have identified $(\mathbf{Z}/m\mathbf{Z})^\times$ with the Galois group* $\mathrm{Gal}(\mathbf{Q}(\zeta_{m_S})/\mathbf{Q})$ *in the usual way.*)

PROOF. See [21] and [17]. □

Following Shioda [21], we call the abelian variety A_S an *admissible factor* of $J(X_m^1)$. We will frequently write A_α for A_S if it is equipped with the embedding θ_α in Proposition 4.1 (ii). An abelian variety A is said to be *of Fermat type of degree m* if there exist (not necessarily distinct) orbits $S_1, \cdots, S_r \in \Omega_m$ such that

$$A \sim A_{S_1} \times \cdots \times A_{S_r}\,. \tag{9}$$

To state a fundamental theorem of Shioda on the Hodge cycles on A, we recall some notation. Let $S(A)$ denote the *disjoint union* of the orbits $S_1, \cdots, S_r$ appeared in (9). If $I = \{\alpha_1, \cdots, \alpha_s\}$ is a subset of $S(A)$, we define a subspace W_I of $H^s(A, \mathbf{C})$ by

$$W_I = W(\alpha_1) \wedge \cdots \wedge W(\alpha_s)\,.$$

Then for any d with $0 \le d \le \dim A$, we have

$$H^{2d}(A, \mathbf{C}) = \bigoplus_I W_I\,, \tag{10}$$

where the direct sum is taken over the subsets $I = \{\alpha_1, \cdots, \alpha_{2d}\}$ of $S(A)$ such that $\alpha_i \neq \alpha_j$ $(i \neq j)$. Then Shioda's theorem can be stated as follows:

THEOREM 4.2. *Let A be an abelian variety of Fermat type of degree m which is isogenous to the product $A_{S_1} \times \cdots \times A_{S_r}$. Then the $\mathbf{C}$-span of Hodge cycles on A of codimension d is given by*

$$\mathscr{B}^d(A) \otimes \mathbf{C} = \bigoplus_I W_I\,,$$

where the direct sum is taken over the subsets $I = \{\alpha_1, \cdots, \alpha_{2d}\}$ of $S(A)$ such that $\alpha_i \neq \alpha_j$ $(i \neq j)$ and

$$\alpha_1 * \cdots * \alpha_{2d} \in \mathfrak{B}_m^{6d-2}\,.$$

Moreover, if the corresponding subspace $V(\alpha_1 * \cdots * \alpha_{2d})$ of $\mathscr{B}^{3d-1}(X_m^{6d-2})_{\mathbf{C}}$ is algebraic, then so is W_I.

PROOF. The first assertion is Theorem 3.1 of [21], and the second assertion follows from Lemma 4.1 and Lemma 4.2 of [21]. □

COROLLARY 4.3. *Let $I = \{\alpha_1, \cdots, \alpha_{2d}\} \subset S(A)$ be as in the above theorem. If $\alpha_1 * \cdots * \alpha_{2d} \in \mathfrak{S}_m^{6d-2}$, then W_I is algebraic.*

PROOF. This follows from Theorem 3.2 and the last statement of Theorem 4.2. □

5. The jacobian varieties of quotients of Fermat curves

In the following we will fix an element $\alpha = (a, b, c) \in \mathfrak{A}_m^1$ with $\mathrm{GCD}(\alpha) = 1$. We define C_α to be the quotient $X_m^1/\mathrm{Ker}(\alpha)$ of the Fermat curve X_m^1 by the subgroup $\mathrm{Ker}(\alpha) = \{g \in G_m^1 \mid \alpha(g) = 1\}$ of G_m^1. Then C_α is birational to the curve

$$y^m = x^a(1-x)^b\,.$$

The jacobian variety J_α of C_α is a quotient of the jacobian variety $J(X_m^1)$. In particular J_α is an abelian variety of Fermat type of degree m. We say that an element x of $\mathbf{Z}/m\mathbf{Z}$ is *α-admissible* if $xa, xb, xc \not\equiv 0 \pmod m$. Let $\{d_1, \cdots, d_r\}$ be the set of α-admissible divisors of m and S_i the orbit of $(d_i)\alpha \in \mathfrak{A}_m^1$. Then the decomposition of J_α into admissible factors is given by

$$J_\alpha \sim \prod_{i=1}^r A_{S_i} = \prod_{i=1}^r A_{(d_i)\alpha} \tag{11}$$

([21, Example 2.2]). To describe the eigenspace decomposition of $H^*(J_\alpha^k, \mathbf{C})$, let $\alpha^{(1)}, \cdots, \alpha^{(k)}$ be k copies of α. Then

$$S(J_\alpha^k) = \bigcup_{i=1}^{k} \{(x)\alpha^{(i)} \mid x \in \mathbf{Z}/m\mathbf{Z}, x \text{ is } \alpha\text{-admissible}\}.$$

By the definition of $S(J_\alpha^k)$, the equality $(b)\alpha^{(i)} = (b')\alpha^{(i')}$ holds if and only if $b = b'$ and $i = i'$.

An element $\beta = (b_1, \cdots, b_s) \in \mathfrak{R}_m$ is said to be *α-admissible* (resp. *primitive*) if b_i is α-admissible (resp. $b_i \in (\mathbf{Z}/m\mathbf{Z})^\times$) for every i. Clearly if β is primitive, then it is α-admissible.

For any $\beta = (b_1, \cdots, b_s) \in \mathfrak{R}_m$ we define the product $\beta\alpha$ by

$$\beta\alpha = (a_1)\alpha * \cdots * (a_s)\alpha \ \in (\mathbf{Z}/m\mathbf{Z})^{3s}.$$

Then $\beta\alpha \in \mathfrak{A}_m^{3s-2}$ if and only if β is α-admissible. For any subset X of $\mathfrak{R}_m$ we let

$$(X : \alpha) = \{\beta \in \mathfrak{R}_m \mid \beta\alpha \in X\}.$$

If Y is a subset of $\mathfrak{R}_m$, we denote by Y^* (resp. $Y^\times$) the set of α-admissible (resp. primitive) elements in Y. Thus

$$(X : \alpha)^* = \{\beta \in (X : \alpha) \mid \beta \text{ is } \alpha\text{-admissible}\},$$
$$(X : \alpha)^\times = \{\beta \in (X : \alpha) \mid \beta \text{ is primitive}\}.$$

Let d be a positive integer. For each $\beta = (b_1, \cdots, b_{2d}) \in (\mathfrak{A}_m^{6d-2} : \alpha)^*$ and for each $\mathbf{i} = (i_1, \cdots, i_{2d}) \in \{1, \cdots, k\}^{2d}$ we define a (at most one-dimensional) subspace of $H^{2d}(J_\alpha^k, \mathbf{C})$:

$$W_{(\beta,\mathbf{i})}(\alpha) = W((b_1)\alpha^{(i_1)}) \wedge \cdots \wedge W((b_{2d})\alpha^{(i_{2d})}).$$

In the notation of the preceding section, the subspace $W_{(\beta,\mathbf{i})}(\alpha)$ is nothing but W_I with $I = \{(b_1)\alpha^{(i_1)}, \cdots, (b_{2d})\alpha^{(i_{2d})}\}$. We say that the pair $(\beta, \mathbf{i})$ is *regular* if $(b_\mu)\alpha^{(i_\mu)} \neq (b_\nu)\alpha^{(i_\nu)}$ for all $\mu \neq \nu$. If $k = 1$, then the set $\{1\}^{2d}$ consists of the unique element $\mathbf{1} = (1, \cdots, 1)$. For simplicity we write $W_\beta(\alpha)$ for $W_{(\beta,\mathbf{1})}(\alpha)$. We say that β is regular if $(\beta, \mathbf{1})$ is regular. Thus $\beta = (b_1, \cdots, b_{2d})$ is regular if and only if $b_i \neq b_j$ $(i \neq j)$. Clearly $\dim_{\mathbf{C}} W_{(\beta,\mathbf{i})}(\alpha) = 1$ if and only if $(\beta, \mathbf{i})$ is regular. We let the permutation group of $2d$ elements act on both $(\mathbf{Z}/m\mathbf{Z})^{2d}$ and $\{1, \cdots, k\}^{2d}$ in a natural manner. Then, for two regular pair $(\beta, \mathbf{i})$ and $(\beta', \mathbf{i}')$, the corresponding spaces $W_{(\beta,\mathbf{i})}(\alpha)$ and $W_{(\beta',\mathbf{i}')}(\alpha)$ coincides if and only if there exsists a permutation σ such that $\sigma(\beta) = \beta'$ and $\sigma(\mathbf{i}) = \mathbf{i}'$. If this holds, we say that $(\beta, \mathbf{i})$ and $(\beta', \mathbf{i}')$ are *equivalent*. In particular, when $k = 1$, β and β' are equivalent if and only if $\beta \sim \beta'$.

If A denotes the abelian variety J_α or A_α, then for any positive integer k it follows from (10) that

$$H^{2d}(A^k, \mathbf{C}) = \bigoplus_{(\beta,\mathbf{i})} W_{(\beta,\mathbf{i})}(\alpha),$$

where the pair $(\beta, \mathbf{i})$ runs through the equivalent classes of the regular elements in $(\mathfrak{A}_m^{6d-2} : \alpha)^* \times \{1, \cdots, k\}^{2d}$ if $A = J_\alpha$ and in $(\mathfrak{A}_m^{6d-2} : \alpha)^\times \times \{1, \cdots, k\}^{2d}$ if $A = A_\alpha$. The eigenspace decompositions of $\mathscr{B}^d(A^k)$ and $\mathscr{D}^d(A^k)$ for $A = J_\alpha$ or A_α are given by the following theorem.

THEOREM 5.1. *Let A be either J_α or A_α and k a positive integer.*

(i) *The $\mathbf{C}$-span of the Hodge cycles on A^k of codimension d is given by*

$$\mathscr{B}^d(A^k) \otimes \mathbf{C} = \bigoplus_{(\beta, \mathbf{i})} W_{(\beta, \mathbf{i})}(\alpha)\,,$$

where the pair $(\beta, \mathbf{i})$ runs through the equivalent classes of the regular elements of $(\mathfrak{B}_m^{6d-2} : \alpha)^* \times \{1, \cdots, k\}^{2d}$ if $A = J_\alpha$ and of $(\mathfrak{B}_m^{6d-2} : \alpha)^\times \times \{1, \cdots, k\}^{2d}$ if $A = A_\alpha$. Moreover, if $\beta \in (\mathfrak{S}_m^{6d-2} : \alpha)^*$, then $W_{(\beta, \mathbf{i})}(\alpha)$ is algebraic.

(ii) *If every admissible factor of A is simple, then*

$$\mathscr{D}^d(A^k) \otimes \mathbf{C} = \bigoplus_{(\beta, \mathbf{i})} W_{(\beta, \mathbf{i})}(\alpha)\,,$$

where the pair $(\beta, \mathbf{i})$ runs through the equivalent classes of the regular elements of $(\mathfrak{D}_m^{2d-2})^* \times \{1, \cdots, k\}^{2d}$ if $A = J_\alpha$ and of $(\mathfrak{D}_m^{2d-2})^\times \times \{1, \cdots, k\}^{2d}$ if $A = A_\alpha$.

PROOF. The first assertion immediately follows from Theorem 4.2, and the second assertion can be proved by a similar arguement of the proof of [21, Theorem 5.2]. □

COROLLARY 5.2. *If $(\mathfrak{B}_m : \alpha)^* = (\mathfrak{S}_m : \alpha)^*$, then $\mathrm{HC}(J_\alpha^k)$ is true for all $k \geq 1$.*

PROOF. This follows from Theorem 5.1 (i) and Corollary 4.3. □

6. Stickelberger elements

Let $\Gamma_m = \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})$. For any $t \in (\mathbf{Z}/m\mathbf{Z})^\times$ we denote by σ_t the element of Γ_m such that $\sigma_t(\zeta_m) = \zeta_m^t$. For any $a \in \mathbf{Z}/m\mathbf{Z} \setminus \{0\}$ we define a *Stickelberger element* $\theta(a) \in \mathbf{Q}[\Gamma_m]$ by

$$\theta(a) = \sum_{t \in (\mathbf{Z}/m\mathbf{Z})^\times} \left(\left\langle \frac{at}{m} \right\rangle - \frac{1}{2} \right) \sigma_t^{-1}\,,$$

where, for any $x \in \mathbf{Q}$, $\langle x \rangle$ denotes the rational number such that $0 \leqq \langle x \rangle < 1$ and $\langle x \rangle \equiv x \pmod 1$. We extend θ to a map from $\mathfrak{R}_m$ to $\mathbf{Q}[\Gamma_m]$ by the following rule: For $\alpha = (a_1, \cdots, a_s) \in \mathfrak{R}_m$ we let

$$\theta(\alpha) = \sum_{i=1}^{s} \theta(a_i)\,.$$

The importance of θ lies in the fact that the coefficients of $\theta(\alpha)$ are described by the numbers $|t\cdot\alpha|$ ($t \in (\mathbf{Z}/m\mathbf{Z})^\times$): If $\alpha = (a_0, \cdots, a_{n+1}) \in \mathfrak{A}_m^n$, then

$$\theta(\alpha) = \sum_{t\in(\mathbf{Z}/m\mathbf{Z})^\times} \left(|t\cdot\alpha| - \frac{n}{2} - 1\right)\sigma_t^{-1}\,. \tag{12}$$

Indeed, $\theta(\alpha)$ is equal to

$$\sum_{i=0}^{n+1} \sum_{t\in(\mathbf{Z}/m\mathbf{Z})^\times} \left(\left\langle\frac{a_i t}{m}\right\rangle - \frac{1}{2}\right)\sigma_t^{-1} = \sum_{t\in(\mathbf{Z}/m\mathbf{Z})^\times} \sum_{i=0}^{n+1} \left(\left\langle\frac{a_i t}{m}\right\rangle - \frac{1}{2}\right)\sigma_t^{-1}\,.$$

Hence (12) holds. This leads to a useful characterization of the set $\mathfrak{B}_m^n$ in terms of θ:

PROPOSITION 6.1. *Let $\alpha \in \mathfrak{A}_m^n$ with n even. Then α is in $\mathfrak{B}_m^n$ if and only if $\theta(\alpha) = 0$.*

PROOF. By definition, $\alpha \in \mathfrak{B}_m^n$ if and only if $|t\cdot\alpha| = \frac{n}{2} + 1$ for all $t \in (\mathbf{Z}/m\mathbf{Z})^\times$. But this is equivalent to $\theta(\alpha) = 0$ by (12). □

The following proposition also explains significance of θ:

PROPOSITION 6.2. *Let $\alpha \in \mathfrak{A}_m^1$ and Φ_α the CM-type of A_α defined in Proposition* 4.1 (ii). *Let $\rho = \sigma_{-1}$ be the complex conjugation in Γ_m. Then*

$$\frac{1}{2}(1-\rho)\sum_{\sigma\in\Phi_\alpha}\sigma = -\theta(\alpha)^*\,,$$

where $*$ denotes the involution of $\mathbf{Q}[\Gamma_m]$ induced from the automorphism of Γ_m sending σ to σ^{-1}.

PROOF. For any $t \in (\mathbf{Z}/m\mathbf{Z})^\times$ we have $|t\cdot\alpha| = 1$ or 2 according as $\sigma_t \in \Phi_\alpha$ or $\sigma_t \in \rho\Phi_\alpha$. Therefore

$$\begin{aligned}\frac{1}{2}(1-\rho)\sum_{\sigma\in\Phi_\alpha}\sigma &= \frac{1}{2}\left(\sum_{\sigma\in\Phi_\alpha}\sigma - \sum_{\sigma\in\rho\Phi_\alpha}\sigma\right)\\ &= -\sum_{t\in(\mathbf{Z}/m\mathbf{Z})^\times}\left(|t\cdot\alpha| - \frac{3}{2}\right)\sigma_t\\ &= -\theta(\alpha)^*\,.\end{aligned}$$

Thus the assertion holds. □

Let $W(\Phi_\alpha)$ denote the subgroup of Γ_m defined by

$$W(\Phi_\alpha) = \{\sigma \in \Gamma_m \mid \sigma\Phi_\alpha = \Phi_\alpha\}$$

(see (4)). By Proposition 2.1, A_α is simple if and only if $W(\Phi_\alpha) = \{1\}$.

COROLLARY 6.3. *Notation being as above, we have*

$$W(\Phi_\alpha) = \{\sigma_t \in \Gamma_m \mid (1, -t)\sigma \in \mathfrak{B}_m^4\}\,.$$

PROOF. The proof proceeds as follows. Let $t \in \Gamma_m$. Then:

$$\begin{aligned} \sigma_t \in W(\Phi_\alpha) &\Leftrightarrow \sigma_t\Phi_\alpha = \Phi_\alpha \\ &\Leftrightarrow \sigma_t\theta(\alpha) = \theta(\alpha) \\ &\Leftrightarrow \theta(\alpha + (-t)\alpha) = 0 \\ &\Leftrightarrow (1, -t)\alpha \in \mathfrak{B}_m^4\,. \end{aligned}$$

The first equivalence is just the definition of W_α, the second follows from Proposition 6.2, the third holds since $(\sigma_t + \sigma_{-t})\theta(\alpha) = 0$ for all $t \in (\mathbf{Z}/m\mathbf{Z})^\times$, and the last one follows from Propoition 6.1. □

Now, let $C^-(m)$ stand for the set of odd Dirichlet characters of $\mathbf{Z}/m\mathbf{Z}$. For any $\chi \in C^-(m)$ we denote the conductor of χ by cond(χ), that is, cond(χ) is the smallest divisor f of m for which χ comes from $C^-(f)$. As usual we set $\chi(a) = 0$ if GCD$(a, f) > 1$. Moreover, we denote by $PC^-(m)$ the set of odd characters $\chi \in C^-(m)$ with cond$(\chi) = m$. Note that $PC^-(m) = \emptyset$ if and only if either $m = 12$ or $\mathrm{ord}_2 m = 1$. For any $\chi \in C^-(m)$ and any $a \in \mathbf{Z}/m\mathbf{Z}$ with GCD$(m, a) = d$, let

$$\tau_\chi(a) = \begin{cases} \chi(a')\dfrac{\varphi(m)}{\varphi(f)} \displaystyle\prod_{p \mid \frac{m}{fd}} (1 - \bar{\chi}(p)) & \text{if } d \mid \frac{m}{f}\,, \\ 0 & \text{otherwise}\,, \end{cases}$$

where $a' = a/d$ and the product is over the prime factors p of $\frac{m}{fd}$. More generally, for any $\alpha = (a_1, \cdots, a_s) \in (\mathbf{Z}/m\mathbf{Z} \setminus \{0\})^s$, let

$$\tau_\chi(\alpha) = \sum_{i=1}^{s} \tau_\chi(a_i)\,.$$

LEMMA 6.4. *Notation being as above, we have*

$$\chi(\theta(\alpha)) = \tau_\chi(\alpha) B_{1,\bar{\chi}}\,,$$

where $B_{1,\chi} = \frac{1}{f}\sum_{t=1}^{f} t\chi(t)$ *denotes the generalized Bernoulli number.*

PROOF. See for example [11, Chapter 1]. □

PROPOSITION 6.5. *Let* $\alpha \in \mathfrak{A}_m^n$. *Then* $\alpha \in \mathfrak{B}_m^n$ *if and only if* $\tau_\chi(\alpha) = 0$ *for all* $\chi \in C^-(m)$.

PROOF. Let $\alpha = (a_0, \cdots, a_n) \in \mathfrak{A}_m^n$. Then $\alpha \in \mathfrak{B}_m^n$ if and only if $\theta(\alpha) = 0$ by Proposition 6.1. But the latter condition holds if and only if $\chi(\theta(\alpha)) = 0$ for every odd character χ of Γ_m. Hence the assertion follows from Lemma 6.4 since $B_{1,\chi} \neq 0$ for all $\chi \in C^-(m)$ ([25, Corollary 4.4]). □

PROPOSITION 6.6. *Let α be an element of $\mathfrak{A}_m^1$ with* $\mathrm{GCD}(\alpha) = 1$ *and Φ_α the CM-type of A_α ($\alpha \in \mathfrak{A}_m^1$). Then Φ_α is nondegenerate if and only if $\tau_\chi(\alpha) \neq 0$ for all $\chi \in C^-(m)$.*

PROOF. By Proposition 6.2 and Lemma 6.4 we have

$$\chi(\Phi) = -\tau_{\bar{\chi}}(\alpha) B_{1,\chi}$$

for all $\chi \in C^-(m)$. By nonvanishing of $B_{1,\chi}$, this shows that $\chi(\Phi_\alpha) \neq 0$ if and only if $\tau_\chi(\alpha) \neq 0$. This proves the assertion. □

7. Generalized Catalan curves

Throughout this section $m = p^\mu q^\nu$ will be a product of prime powers p^μ and q^ν of distinct prime numbers p, q. Let C_{p^μ, q^ν} be the generalized Catalan curve defined by (1). Then C_{p^μ, q^ν} is a quotient of the Fermat curve $X_m^1 : x^m + y^m + z^m = 0$ of degree $m = p^\mu q^\nu$. Indeed, the map sending (x, y) to $((x/z)^{q^\nu}, \varepsilon(y/z)^{p^\mu})$ gives a finite morphism $f : X_m^1 \to C_{p^\mu, q^\nu}$, where ε denotes a root of unity such that $\varepsilon^{q^\nu} = -1$. Since p and q are relatively prime, there exist integers a, b such that $p^\mu a + q^\nu b = m - 1$, $0 < a < q^\nu$, $0 < b < p^\mu$. Let

$$\alpha = (1, p^\mu a, q^\nu b) \in \mathfrak{A}_m^1 . \tag{13}$$

Then C_{p^μ, q^ν} is the quotient $X_m^1/\mathrm{Ker}(\alpha)$. If $(\mu, \nu) = (1, 1)$, then $J(C_{p,q})$ is simple by the work of Kubota and Hazama. To obtain the decomposition of $J(C_{p^\mu, q^\nu})$ into admissible factors, we note that the α-admissible divisors are in the form $m/p^i q^j$ with $1 \leq i \leq \mu$, $1 \leq j \leq \nu$. For such i, j let $\alpha_{i,j}$ be the element of $\mathfrak{A}^1_{p^i q^j}$ such that

$$\alpha_{i,j} \equiv \alpha \pmod{p^i q^j} .$$

Let $A_{\alpha_{i,j}}$ denote the admissible factor defined in Proposition 4.1. Thus $A_{\alpha_{i,j}}$ is a CM abelian variety of dimension $\frac{1}{2}\varphi(p^i q^j)$ such that $\mathrm{End}(A_{\alpha_{i,j}}) \otimes \mathbf{Q} \supset \mathbf{Q}(\zeta_{p^i q^j})$. Then there is an isogeny

$$J(C_{p^\mu, q^\nu}) \sim \prod_{i=1}^{\mu} \prod_{j=1}^{\nu} A_{\alpha_{i,j}} . \tag{14}$$

Thus if $(\mu, \nu) \neq (1, 1)$, then $J(C_{p^\mu, q^\nu})$ is not simple. Moreover, its admissible factors can be nonsimple. Indeed, if $m = 12$, then $\alpha = (1, 3, 8) \in \mathfrak{A}_{12}^1$ and we have an isogeny

$$J(C_{3,4}) \sim A_\alpha \times J(C_{3,2}) .$$

The CM type of A_α is given by $\Phi_\alpha = \{1, \sigma_5\} \subset \Gamma_{12}$, and $W(\Phi_\alpha) = \Phi_\alpha$. Therefore by Proposition 2.1 $A_\alpha \sim E \times E$, where E is an elliptic curve with $\mathrm{End}(E) \otimes \mathbf{Q} = \mathbf{Q}(\sqrt{-1})$.

Moreover $J(C_{3,2})$ is a CM elliptic curve with $\mathrm{End}(J(C_{3,2})) \otimes \mathbf{Q} = \mathbf{Q}(\sqrt{-3})$. By the work of Imai [10] (see also [14]) any product of CM elliptic curves is stably nondegenerate, hence $J(C_{3,4})$ and A_α are stably nondegenerate. The following theorem shows that an admissible factor of $J(C_{p^\mu,q^\nu})$ is simple if it is not a factor of $J(C_{3,4})$.

THEOREM 7.1. *Suppose $m \neq 12$ and let α be the element of $\mathfrak{A}_m^1$ defined by* (13). *Then A_α is simple. Moreover A_α is stably nondegenerate except for the following case*:

$$\text{Either } p^\mu = 4 \text{ or } q^\nu = 4, \text{ and the order of } -2 \text{ in } (\mathbf{Z}/\tfrac{m}{4}\mathbf{Z})^\times \text{ is odd}.$$

In this exceptional case, A_α is degenerate. More precisely, if d denotes the order of -2 in $(\mathbf{Z}/\frac{m}{4}\mathbf{Z})^\times$, then

$$\dim \mathscr{B}^d(A_\alpha)/\mathscr{D}^d(A_\alpha) \geq \frac{\varphi(m/4)}{d}.$$

COROLLARY 7.2. *Suppose neither p^μ nor q^ν equals* 4. *Then every admissible factor of $J(C_{p^\mu,q^\nu})$ is simple and stably nondegenerate.*

PROOF. This is a special case of the above theorem. □

In order to prove Theorem 7.1, we need to determine which characters $\chi \in C^-(m)$ satisfy the equality $\tau_\chi(\alpha) = 0$.

LEMMA 7.3. *Let the notation be as above.*
(i) *If $\mathrm{ord}_2(m) \neq 2$, then $\tau_\chi(\alpha) \neq 0$ for all $\chi \in C^-(m)$.*
(ii) *If $\mathrm{ord}_2(m) = 2$, then $\tau_\chi(\alpha) = 0$ if and only if $\chi \in C^-(m/4)$ and $\chi(-2) = 1$.*

PROOF. First, consider the case $\mathrm{ord}_2(m) = 1$, say $m = 2p^\mu$ with p an odd prime. Then $\alpha = (1, p^\mu, p^\mu - 1)$. Hence, for any $\chi \in C^-(p^\mu)$, we have

$$\begin{aligned}\tau_\chi(\alpha) &= 1 - \bar{\chi}(2) + \chi\left(\frac{p^\mu - 1}{2}\right) \\ &= 1 - 2\bar{\chi}(2).\end{aligned}$$

The last expression shows that $\tau_\chi(\alpha) \neq 0$ for any $\chi \in C^-(p^\mu)$.

Next, suppose $\mathrm{ord}_2(m) \neq 1$. Thus $p^\mu, q^\nu > 2$. If $\chi \in C^-(m) \setminus \{C^-(p^\mu) \cup C^-(q^\nu)\}$, then $\tau_\chi(1) = 1$ and $\tau_\chi((ap^\mu)) = \tau_\chi((bq^\nu)) = 0$, hence $\tau_\chi(\alpha) = 1$. Suppose $\tau_\chi(\alpha) = 0$ for some $\chi \in C^-(p^\mu) \cup C^-(q^\nu)$. By symmetry it suffices to consider the case $\chi \in C^-(p^\mu)$. Since $bq^\nu \equiv -1 \pmod{p^\mu}$, we have $\chi(b) = -\bar{\chi}(q)^\nu$. Therefore

$$\tau_\chi(\alpha) = 1 - \bar{\chi}(q) - \varphi(q^\nu)\bar{\chi}(q)^\nu.$$

The assumption $\tau_\chi(\alpha) = 0$ then implies that

$$\chi(q^\nu)(1 - \bar{\chi}(q)) = \varphi(q^\nu). \tag{15}$$

Since $|\chi(p^\mu)(1-\bar{\chi}(p))| \le 2$, this shows that $\varphi(q^\nu) \le 2$. Hence $q^\nu = 3$ or 4. If $q^\nu = 3$, then by (15) we have

$$\chi(3) - 1 = 2\,,$$

which is clearly impossible. Hence q^ν must be 4. It then follows from (15) that

$$\chi(2)^2(1-\bar{\chi}(2)) = 2\,.$$

But this holds if and only if $\chi(2) = -1$, or equivalently $\chi(-2) = 1$. This completes the proof. □

PROOF OF THEOREM 7.1. Recall that A_α is simple and stably nondegenerate if the CM-type Φ_a is degenerate, and the latter condition holds if and if $\tau_\chi(\alpha) \neq 0$ for all $\chi \in C^-(m)$. Therefore A_α is simple and stably nondegenerate provided that $\mathrm{ord}_2(m) \neq 2$ by Lemma 7.3 (i).

Suppose $\mathrm{ord}_2(m) = 2$. If there is no odd character $\chi \in C^-(m/4)$ such that $\chi(-2) = 1$, then Lemma 7.3 (ii) shows that A_α is simple and stably nondegenerate. Suppose there exists an odd character $\chi \in C^-(m/4)$ such that $\chi(-2) = 1$. Then the order d of -2 in $(\mathbf{Z}/\frac{m}{4}\mathbf{Z})^\times$ is odd. Moreover, we have $d > 1$ since $\frac{m}{4} > 3$. First we shall show that A_α is simple. For this we must show that $W(\Phi_\alpha) = \{1\}$ (see Proposition 2.1). Let $\sigma_t \in W_\alpha$. Then $(1, -t)\alpha \in \mathfrak{B}_m^4$ by Corollary 6.3. Hence by Proposition 6.5 we have

$$(1 - \chi(t))\tau_\chi(\alpha) = 0 \tag{16}$$

for all $\chi \in C^-(m)$. It follows from Lemma 7.3 (ii) that $\chi(t) = 1$ if either $\chi \in C^-(m) \setminus C^-(m/4)$ or $\chi \in C^-(m/4)$ and $\chi(-2) \neq 1$. If $\chi(t) = 1$ for some $\chi \in C^-(m) \setminus C^-(m/4)$, then

$$t \equiv \begin{cases} 1 & (\mathrm{mod}\ 4)\,, \\ \varepsilon & (\mathrm{mod}\ m/4) \quad (\varepsilon = \pm 1) \end{cases}$$

provided that $m \neq 20$ (see [1, Proposition 6.1]). Note that there is an odd character $\chi \in C^-(m/4)$ such that $\chi(-2) \neq 1$ since $d > 1$. For such a character χ we have $\chi(t) = \varepsilon$. Therefore $\varepsilon = 1$, hence $t = 1$. Thus A_α is simple when $m \neq 20$. If $m = 20$, then $\alpha = (1, 4, 15) \in \mathfrak{A}_{20}^1$, $\Phi_\alpha = \{1, \sigma_3, \sigma_7, \sigma_{11}\}$ and $W(\Phi_\alpha) = \{1\}$. Thus A_α is also simple. This proves the first statement.

Now, we shall prove that A_α is degenerate assuming that $\mathrm{ord}_2(m) = 2$ and the order d of -2 in $(\mathbf{Z}/\frac{m}{4}\mathbf{Z})^\times$ is odd. Let b be the element of $(\mathbf{Z}/m\mathbf{Z})^\times$ such that

$$b \equiv \begin{cases} -1 & (\mathrm{mod}\ 4)\,, \\ -2 & (\mathrm{mod}\ p^\mu)\,. \end{cases}$$

Then the order of b is $2d$. Let

$$\beta_1 = (1, b, \cdots, b^{2d-1}) \in \mathfrak{R}_m\,.$$

Let $\mathfrak{R}_m^\times$ be the set of primitive elements in $\mathfrak{R}_m$ and $\bar{\beta_1} \in \mathbf{Z}[\Gamma_m]$ the image of β_1 under the natural isomorphism from $\mathfrak{R}_m^\times$ to the integral group ring $\mathbf{Z}[\Gamma_m]$ induced from the map sending (t) to σ_t. Then

$$\bar{\beta_1} = (1 + \sigma_{\frac{m}{2}+1})(1 + \sigma_u + \cdots + \sigma_u^{d-1}) ,$$

where u is the element of $\mathbf{Z}/m\mathbf{Z}$ such that

$$u \equiv \begin{cases} 1 & (\text{mod } 4) , \\ -2 & (\text{mod } m/4) . \end{cases}$$

Since $\chi(\sigma_{\frac{m}{2}+1}) = -1$ for all $\chi \in C^-(m) \setminus C^-(m/4)$ and

$$1 + \chi(\sigma_u) + \cdots + \chi(\sigma_u)^{d-1} = 0$$

for any $\chi \in C^-(m/4)$ such that $\chi(-2) \neq 1$, we have $\chi(\beta_1)\tau_\chi(\alpha) = 0$ for all $\chi \in C^-(m)$ by Lemma 7.3 (ii). Therefore β_1 is in $(\mathfrak{B}_m^{6d-2} : \alpha)^\times$. To show that A_α is degenerate, we have only to verify that $\beta_1 \notin \mathfrak{D}_m^{2d-2}$. To see this, suppose on the contrary that $\beta \in \mathfrak{D}_m^{2d-2}$. Then $b^d = -1$ since the order of b is $2d$. But this is impossible since d is odd and $b \equiv -1$ (mod 4). Thus $\beta_1 \notin \mathfrak{D}_m^{2d-2}$.

To prove the last assertion of the theorem, note that by Theorem 5.1 (ii) the dimension of the quotient space $\mathscr{B}^d(A_\alpha)/\mathscr{D}^d(A_\alpha)$ equals the number of the equivalent classes of $(\mathfrak{B}^{6d-2} : \alpha)^\times \setminus (\mathfrak{D}^{6d-2} : \alpha)^\times$. By the arguement above, $(\mathfrak{B}_m^{6d-2} : \alpha)^\times$ contains the elements equivalent to $(c)\beta_1$ for some $c \in (\mathbf{Z}/m\mathbf{Z})^\times/\langle b\rangle$. Thus

$$\dim \mathscr{B}^d(A_\alpha)/\mathscr{D}^d(A_\alpha) \geq \frac{\varphi(m)}{2d} = \frac{\varphi(m/4)}{d} .$$

This completes the proof. □

8. The Hodge conjecture for powers of $J(C_{p^\mu,q^\nu})$

In this section we prove the following theorems.

THEOREM 8.1. *If $m \neq 12$ and $(\mu,\nu) \neq (1,1)$, then $J(C_{p^\mu,q^\nu})$ itself is degenerate. More precisely, $\mathscr{B}^d(J(C_{p^\mu,q^\nu}))$ is strictly bigger than $\mathscr{D}^d(J(C_{p^\mu,q^\nu}))$ for $d = p+1, q+1$ and $\frac{1}{2}(p+1)(q+1)$.*

THEOREM 8.2. *For any $k \geq 1$, $\mathrm{HC}(J(C_{p^\mu,q^\nu})^k)$ is true.*

To make our proof transparent, we introduce further notation. For the moment let m be an arbitrary positive integer. Let R_m be the free abelian group generated by the elements of $\mathbf{Z}/m\mathbf{Z} - \{0\}$. An element of R_m will be written as

$$\sum_{a \in \mathbf{Z}/m\mathbf{Z} - \{0\}} c_a(a) \quad (c_a \in \mathbf{Z}) .$$

There is a natural map $u : \mathfrak{R}_m \to R_m$ sending $(a_1, \cdots, a_r)$ to $\sum_{i=1}^{r}(a_i)$. Clearly we have $u(\alpha * \beta) = u(\alpha) + u(\beta)$ for any $\alpha, \beta \in \mathfrak{R}_m$. If there is no fear of confusion, we write $(a_1, \cdots, a_r)$ for the image $\sum_{i=1}^{r}(a_i)$. For any two elements $\alpha = \sum c_a(a), \beta = \sum d_b(b) \in R_m$ we define the product $\alpha\beta \in R_m$ by the rule:

$$\alpha\beta = \sum_{a,b \in \mathbf{Z}/m\mathbf{Z}\setminus\{0\}} c_a d_b (ab)\,,$$

where we understand that $(ab) = 0$ if $ab = 0$. Thus R_m is a commutative ring with the unit (1).

Let B_m, S_m and D_m be the submodule of R_m generated by the elements of $u(\mathfrak{B}_m), u(\mathfrak{S}_m)$ and $u(\mathfrak{D}_m)$ respectively. Then we have inclusions

$$R_m \supseteq B_m \supseteq S_m \supseteq D_m\,.$$

By the work of Yamamoto [27] it is known that the quotient group B_m/S_m is an elementary abelian group of exponent 2. More precisely, if r denotes the number of prime divisor of m, then

$$B_m/S_m \cong (\mathbf{Z}/2\mathbf{Z})^{\oplus 2^{r-1-\delta}-1}\,, \tag{17}$$

where $\delta = 0$ if $\mathrm{ord}_2(m) \neq 1$ and $\delta = 1$ if $\mathrm{ord}_2(m) = 1$ (see [27, Theorem 4] and [1, Theorem D]).

In the following we assume that $m = p^\mu q^\nu$ as in the previous section and that $\mathrm{ord}_2 m \neq 1$, i.e. $p^\mu, q^\nu \neq 2$. Then $B_m/S_m \cong \mathbf{Z}/2\mathbf{Z}$ by (17). This means that if both p and q are odd primes, then there exists an element $\xi \in B_{pq}$ such that B_m is generated by S_m and $(m/pq)\xi$, and if either p or q is 2, say $q = 2$, then B_m is generated by S_m and $(m/4p)\xi$ with some $\xi \in B_{4p}$. We shall need an explicit form of ξ in the proof of Theorem 7.1.

First, consider the case where both p and q are odd primes. We define g_p to be an element of $(\mathbf{Z}/m\mathbf{Z})^\times$ of order $p-1$ such that $g_p \equiv 1 \pmod q$ and define g_q similarly. Let

$$\gamma_p = (1, g_p, g_p^2, \cdots, g_p^{(p-3)/2})\,, \quad \gamma_q = (1, g_q, g_q^2, \cdots, g_q^{(q-3)/2})\,.$$

One can easily see that there exist elements $\eta_q \in R_q$ and $\eta_p \in R_p$ satisfying the condition:

$$(1, -p^{-1})\gamma_q + 2\eta_q \in D_q\,, \quad (1, -q^{-1})\gamma_p + 2\eta_p \in D_p\,. \tag{18}$$

Then we can take the following element for ξ:

$$\xi = \gamma_p\gamma_q + (p)\eta_q + (q)\eta_p\,. \tag{19}$$

Next, suppose one of p, q is 2, say $q = 2$. Let $g_p \in \mathbf{Z}/4p\mathbf{Z}$ be an element of order $p-1$ such that $g_p \equiv 1 \pmod 4$, and put

$$\gamma'_p = (1, g_p^2, g_p^4, \cdots, g_p^{p-3})\,.$$

Then we define $\xi \in R_{4p}$ by

(20)
$$\xi = \begin{cases} \gamma'_p & p \equiv 1 \pmod 8, \\ \gamma'_p + (-4)\gamma'_p + (2p) & p \equiv 3 \pmod 8, \\ \gamma'_p + (2p) & p \equiv 5 \pmod 8, \\ \gamma'_p + (-p) & p \equiv 7 \pmod 8. \end{cases}$$

For example, for $m = 12$ we have $\xi = (1, 6, 8, 9) \in B_{12}$.

REMARK 8.3. If $m = pq \equiv 3 \pmod 4$, then one can use $\gamma'_p\gamma'_q$ instead of $\gamma_p\gamma_q$ in the definition of ξ, and ξ will be in a simpler form. However, this definition does not work if $pq \equiv 1 \pmod 4$, since in this case $\gamma'_p\gamma'_q$ is an element of D_m, and so ξ does not give a generator of B_m/S_m.

Now, for any $\boldsymbol{x} = (x_1, \cdots, x_r) \in R_m \setminus (m/p)R_m$ and any $\boldsymbol{y} = (y_1, \cdots, y_s) \in R_m \setminus (m/q)R_m$, let

$$\sigma_{p,\boldsymbol{x}} = \sum_{i=1}^{r} \sigma_{p,x_i}, \quad \sigma_{q,\boldsymbol{y}} = \sum_{j=1}^{s} \sigma_{q,y_j} \in S_m.$$

Let $I_m = (p^\mu)R_m + (q^\nu)R_m$ be the ideal of R_m generated by two elements (p^μ) and (q^ν). Consider two homomorphisms

$$\pi_p : R_m \to R_{p^\mu}, \quad \pi_q : R_m \to R_{q^\nu}$$

induced from the natural surjections $\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/p^\mu\mathbf{Z}$ and $\mathbf{Z}/m\mathbf{Z} \to \mathbf{Z}/q^\nu\mathbf{Z}$, respectively. We denote by S_{p^μ,q^ν} the submodule of S_m generated by $D_m + I_m$ and the elements of the form $\sigma_{p,\boldsymbol{x}}, \sigma_{q,\boldsymbol{y}}$ such that $\pi_q(\boldsymbol{x}) \in S_{q^\nu}$ and $\pi_p(\boldsymbol{y}) \in S_{p^\mu}$, respectively.

Let $\alpha = (1, ap^\mu, bq^\nu) \in \mathfrak{A}_m^1$ be the element defined by (13). For any submodule M of R_m containig D_m, let

$$(M : \alpha) = \{\beta \in R_m \mid \beta\alpha \in M\},$$
$$(M : \alpha)^* = \{\beta \in (M : \alpha) \mid \beta \text{ is } \alpha\text{-admissible}\}.$$

Clearly, both $(M : \alpha)$ and $(M : \alpha)^*$ are submodules of R_m which enjoy the following properties:

$$(M : \alpha) = (M : \alpha)^* + I_m,$$
$$(M : \alpha)^* = (M : \alpha) \cap (R_m \setminus I_m).$$

Indeed, the first equality follows from the fact that both $(p^\mu)\alpha = (p^\mu, -p^\mu)$ and $(q^\nu)\alpha = (q^\nu, -q^\nu)$ are elements of D_m, and the second is a direct consequence of the definition. These relations show that for any submodule M, M' of R_m the equality $(M : \alpha) = (M' : a)$ holds if and only if $(M : \alpha)^* = (M' : \alpha)^*$. Moreover, if M is generated by the image $u(X)$ of a subset X of $\mathfrak{R}_m$ under the map u, then $(M : \alpha)$ (resp. $(M : a)^*$) is the submodule generated by $u((X:\alpha))$ (resp. $u((X:a)^*)$) and $u^{-1}((M:\alpha)) = (X:\alpha)$ (resp. $u^{-1}((M:\alpha)^*) = (X:\alpha)^*$).

PROPOSITION 8.4. $(B_m:\alpha) = (S_m:\alpha) = S_{p^\mu,q^\nu}$.

This proposition is the core of the proof of Theorem 8.1 and Theorem 8.2. We postpone the proof of this proposition for the moment and give the proof of Theorem 8.1 and Theorem 8.2.

PROOF OF THEOREM 8.1. The assertion follows from the second equality of Proposition 8.4. To be precise, note that S_{p^μ} (resp. S_{q^ν}) is generated by D_{p^μ} (resp. D_{q^ν}) and the elements of the form $\sigma_{p,x}$ (resp. $\sigma_{q,y}$). Therefore S_{p^μ,q^ν} is generated by D_m and the following four types of elements:

$$(21)\qquad \begin{cases} \sigma_{p,(x_1,x_2)} & (x_1+x_2\equiv 0 \pmod{q^\nu}), \\ \sigma_{q,(y_1,y_2)} & (y_1+y_2\equiv 0 \pmod{p^\mu}), \\ \sigma_{p,\boldsymbol{x}} & (\pi_q(\boldsymbol{x}) = \sigma_{q,y} \quad \text{for some } y\in \mathbf{Z}/q^\nu\mathbf{Z}), \\ \sigma_{q,\boldsymbol{y}} & (\pi_p(\boldsymbol{y}) = \sigma_{p,x} \quad \text{for some } x\in \mathbf{Z}/p^\mu\mathbf{Z}). \end{cases}$$

Thus $(B_m:\alpha)^*$ is generated by those elements with the terms in I_m omitted, and it is generated by $u((\mathfrak{B}_m^{6d-2}:\alpha)^*)$ with $d = 1, p+1, q+1$ and $\frac{1}{2}(p+1)(q+1)$. Since all the elements in (21) do not belong to D_m, $\mathscr{B}^d(J(C_{p^\mu,q^\nu}))$ is strictly bigger than $\mathscr{D}^d(J(C_{p^\mu,q^\nu}))$ for $d = p+1, q+1$ and $\frac{1}{2}(p+1)(q+1)$. This completes the proof. □

PROOF OF THEOREM 8.2. The observations before Proposition 8.4 show that if $(B_m:\alpha) = (S_m:\alpha)$, then $(\mathfrak{B}_m:\alpha)^* = (\mathfrak{S}_m:\alpha)^*$. Thus, in view of Corollary 5.2, the first equality of Proposition 8.4 establish Theorem 8.2. □

Before entering the proof of Proposition 8.4 we prove a lemma.

LEMMA 8.5. *Let* $m = p^\mu q^\nu$ *and assume that* $m \neq 12$ *and* $\mathrm{ord}_2(m) \neq 1$. *Let* $\beta \in R_m$. *If* $\chi(\beta) = 0$ *for all* $\chi \in C^-(m)$ *with* $\mathrm{cond}(\chi) \equiv 0 \pmod{pq}$, *then* $\beta \in B_m + I_m$, *that is, there exist* $\beta_0 \in B_m$, $\beta_1 \in R_{q^\nu}$ *and* $\beta_2 \in R_{p^\mu}$ *such that*

$$\beta = \beta_0 + (p^\mu)\beta_1 + (q^\nu)\beta_2 .$$

PROOF. Assuming that the lemma does not hold for some $\beta \in R_m$, we will get a contradiction. For this end we write such an element β as

$$(22)\qquad \beta \equiv \beta_0 + (p^\mu)\beta_1 + (q^\nu)\beta_2 \pmod{B_m},$$

where $\beta_1, \beta_2 \in R_m$ and $\beta_0 \in R_m \setminus I_m$. By assumption, β_0 is not an element of B_m. We write β_0 in the following form

$$\beta_0 = \sum_d (d)\gamma_d \quad (\gamma_d \in \mathbf{Z}[(\mathbf{Z}/(m/d)\mathbf{Z})^\times]),$$

where d runs through the proper divisors of m not divisible by p^μ and q^ν. Let

$$d(\beta_0) = \min\{d \mid \gamma_d \neq 0\}\,.$$

Of all the expressions of β in (22) we choose one so that $d(\beta_0)$ is as large as possible. Then $d(\beta_0) \neq p^\mu, q^\nu$. Furthermore, we have $m/d(\beta_0) \neq 12$ and $\mathrm{ord}_2(m/d(\beta_0)) \neq 1$. To see this, let $d_0 = d(\beta_0)$. If $m/d_0 = 12$, then replacing β_0 with $\beta_0' = \beta_0 - (d_0)\gamma_{d_0}\xi_{12} \equiv \beta_0 \pmod{B_m}$ in the expression (22), we obtain $d(\beta_0') > d_0$, which is a contradiction. If $\mathrm{ord}_2(m/d_0) = 1$, then replacing β_0 with $\beta_0' = \beta_0 - (d_0)\gamma_{d_0}\sigma_{2,1} \equiv \beta_0 \pmod{B_m}$ in (22), we obtain $d(\beta_0') > d_0$, which is again a contradiction. Thus $m/d_0 \neq 12$ and $\mathrm{ord}_2(m/d_0) \neq 1$. Here note that $PC^-(m/d_0)$ is not empty. Then the assumption of the proposition implies that

$$\tau_\chi(\beta) = \tau_\chi(\beta\alpha) = 0$$

for any $\chi \in PC^-(m/d_0)$ with $d_0 = d(\beta_0)$ since $p^\mu \nmid d_0$ and $q^\nu \nmid d_0$. Since $\tau_\chi(\beta) = \frac{\varphi(m)}{\varphi(m/d_0)}\chi(\gamma_{d_0})$, this implies that $\chi(\gamma_{d_0}) = 0$. Hence by [1, Proposition 4.1] there exists some $\eta \in B_{m/d_0}$ such that

$$\gamma_{d_0} = \eta + \sum_d (d)\gamma_d'\,,$$

where the sum is over the proper divisors d of m/d_0 distinct from 1 and where $\gamma_d' \in R_{m/d_0 d}$. Then we can replace β_0 with $\beta_0' = \beta_0 - (d_0)\eta \in B_m$ in (22). Since $d(\beta_0') > d_0$, we get a contradiction. This completes the proof. □

PROOF OF PROPOSITION 8.4. We prove the proposition assuming that both p and q are odd primes since the proof in the case either $p = 2$ or $q = 2$ is almost pararell.

Now, note that we have inclusions

$$(B_m : \alpha) \supseteq (S_m : \alpha) \supseteq S_{p^\mu, q^\nu}\,. \tag{23}$$

The first inclusion is clear. To prove the second, let $\beta \in S_{p^\mu,q^\nu}$. Then there exists an α-admissible element $\sigma \in S_m \cap S_{p^\mu,q^\nu}$ such that

$$\beta \equiv \sigma \pmod{I_m}\,.$$

Since $(p^\mu)\alpha, (q^\nu)\alpha \in D_m$, we have

$$\beta\alpha \equiv \sigma + (ap^\mu)\sigma + (bq^\nu)\sigma \pmod{D_m}\,. \tag{24}$$

By the definition of σ, we have $\pi_p(\sigma) \in S_{p^\mu}$, hence $(ap^\mu)\sigma \in S_m$. Similarly we have $(bq^\nu)\sigma \in S_m$. Since $\sigma \in S_m$, (24) implies that $\sigma\alpha \in S_m$ as well. Therefore $\beta \in (S_m;\alpha)$, hence $S_{p^\mu,q^\nu} \subseteq (S_m : \alpha)$, proving (23).

Thus in order to prove the proposition, it suffices to prove the inclusion

$$(B_m : \alpha) \subseteq S_{p^\mu,q^\nu}\,. \tag{25}$$

To prove this, let $\beta \in (B_m : \alpha)$. Then Proposition 6.5 implies that $\tau_\chi(\beta\alpha) = 0$ for all $\chi \in C^-(m)$. If $\mathrm{cond}(\chi) \equiv 0 \pmod{pq}$, then $\tau_\chi(\beta) = \tau_\chi(\beta\alpha) = 0$. Therefore by Lemma 8.5 there exists $\beta_0 \in B_m$ such that

$$\beta \equiv \beta_0 \pmod{I_m}.$$

Then $\beta\alpha \equiv \beta_0\alpha \pmod{D_m}$. Thus, replacing β with β_0, we may assume that $\beta \in B_m$ from the first. Write β in the form

$$\beta = \sigma_{p,\boldsymbol{x}} + \sigma_{q,\boldsymbol{y}} + c(m/pq)\xi\,, \tag{26}$$

where $\boldsymbol{x} \in R_m \setminus (m/p)R_m$, $\boldsymbol{y} \in R_m \setminus (m/q)R_m$, $\xi \in B_{pq}$ and $c = 0$ or 1. Of cource, $\beta \in S_m$ if and only if $c = 0$, and we must show that $c = 0$, $\pi_q(\boldsymbol{x}) \in S_{q^\nu}$ and $\pi_p(\boldsymbol{y}) \in S_{p^\mu}$. Since $\beta \in B_m$, we have

$$\beta\alpha \equiv (ap^\mu)\beta + (bq^\nu)\beta \pmod{B_m}.$$

Hence for any $\chi \in C^-(q^\nu)$ we have the equality

$$\tau_\chi(\beta\alpha) = \tau_\chi((ap^\mu)\beta)\,. \tag{27}$$

To compute the right-hand side of (27), we note that

$$(p^\mu)\sigma_{p,\boldsymbol{x}} = (p^\mu)\{p(1) + (-p)\}\pi_q(\boldsymbol{x})$$

and $(p^\mu)\sigma_{q,\boldsymbol{y}} \in S_m$. If $\chi \in C^-(q^\nu) \setminus C^-(q)$, then $\tau_\chi((ap^\mu)\xi) = 0$, hence by the expression (26) we have

$$\tau_\chi((ap^\mu)\beta) = \varphi(p^\mu)(p - \chi(p))\tau_\chi(\pi_q(\boldsymbol{x}))\,. \tag{28}$$

Since $\beta \in (B_m : \alpha)$, we have $\tau_\chi(\beta\alpha) = 0$, so $\tau((ap^\mu)\beta) = 0$ for all $\chi \in C^-(m)$ by (27). But since $p - \chi(p) \neq 0$ for any χ, we have $\tau_\chi(\pi_q(\boldsymbol{x})) = 0$ by (28) for any $\chi \in C^-(q^\nu) \setminus C^-(q)$. A quite similar arguement as in the proof of Lemma 8.5 show that

$$\pi_q(\boldsymbol{x}) \equiv (q^{\nu-1})\boldsymbol{x}' \pmod{S_{q^\nu}} \tag{29}$$

for some $\boldsymbol{x}' \in R_q$. Thus

$$(ap^\mu)\beta \equiv \left(\frac{m}{q}\right)\{(p(1) + (-p))(a)\boldsymbol{x}' + c(ap^{\mu-1})\xi\} \pmod{B_m}\,. \tag{30}$$

On the other hand, multiplying (19) by $2(ap^\mu)$ and using the relation (18), we obtain

$$2(ap^\mu)\xi \equiv (ap^\mu)\{p(1) + (-p)\}\gamma_q \pmod{D_m}\,.$$

Substituting this into (30), we obtain

$$2(ap^\mu)\beta \equiv \left(\frac{m}{q}\right)\{p(1) + (-p)\}\{2(a)\boldsymbol{x}' + c\gamma_q\} \pmod{B_m}\,.$$

It follows from this and (27) that the equality

$$\frac{\varphi(m)}{\varphi(q)}(p-\chi(p))\{2\chi((a)\boldsymbol{x}')+c\chi(\gamma_q)\}=2\tau_\chi(\beta\alpha)$$

holds for any $\chi\in C^-(q)$. Since $p-\chi(p)\neq 0$ and $\tau_\chi(\beta\alpha)=0$, this shows that

$$2\chi((a)\boldsymbol{x}')+c\chi(\gamma_q)=0$$

for any $\chi\in C^-(q)$. Clearly this holds if and only if $2(a)\boldsymbol{x}'+c\gamma_q\in D_q$. But this is possible only when $c=0$ and $\boldsymbol{x}'\in D_q$. Hence (29) implies that $\pi_q(\boldsymbol{x})\in S_{q^\nu}$. Quite similarly one can show that $\pi_p(\boldsymbol{y})\in S_{p^\mu}$. Thus $\beta\in S_{p^\mu,q^\nu}$, which proves the inclusion (25). This completes the proof of Proposition 8.4. □

References

[1] N. Aoki, On some arithmetic problems related to the Hodge cycles on the Fermat varieties, Math. Ann. **266** (1983), 23–54 (Erratum: Math. Ann. **267** (1984), p. 572).

[2] N. Aoki, Some new algebraic cycles on Fermat varieties, J. Math. Soc. Japan **39** (1987), 385–396.

[3] N. Aoki, Simple factors of the jacobian of a Fermat curve and the Picard number of a product of Fermat curves, Amer. J. Math. **113** (1991), 779–833.

[4] N. Aoki, Some remarks on the Hodge conjecture for abelian varieties of Fermat type, Comm. Math. Univ. Sancti Pauli **49** (2000), 177–194.

[5] N. Aoki, Hodge cycles on CM abelian varieties of Fermat type, Comm. Math. Univ. Sancti Pauli **51** (2002), 99–130.

[6] F. Hazama, Hodge cycles on Abelian varieties of CM-type, Res. Act. Fac. Eng. Tokyo Denki Univ. **5** (1983), 31–33.

[7] F. Hazama, Algebraic cycles on certain abelian varieties and powers of special surfaces, J. Fac. Sci. Univ. Tokyo **31** (1985), 487–520.

[8] F. Hazama, Algebraic cycles on nonsimple abelian varieties, Duke Math. J. **58** (1989), 31–37.

[9] F. Hazama, Hodge cycles on the jacobian variety of the Catalan curve, Compostio Math. **107** (1997), 339–353.

[10] H. Imai, On the Hodge groups of some Abelian varieties, Kodai Math. Sem. Rep. **27** (1976), 367–372.

[11] D. S. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften **244** (1981), Springer.

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

[13] J. D. Lewis, *A Survey of the Hodge Conjecture*, CRM Monograph series **10** (1991), Amer. Math. Soc.

[14] V. K. Murty, Computing the Hodge group of an abelian variety, Séminaire de Théorie des Nombres, Paris 1988–1989, Prog. Math. **91** (1990), Birlhäuser, 141–158.

[15] Z. Ran, Cycles on Fermat hypersurfaces, Compositio Math. **42** (1981), 121–142.

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

[17] C.-G. Schmidt, *Zur Arithmetik abelscher Varietäten mit komplexer Multiplikation*, Springer Lect. Notes in Math. **1082** (1984), Springer.

[18] C. Schoen, Hodge classes on self-products of a variety with an automorphism, Compositio Math. **65** (1988), 3–32.

[19] G. Shimura and Y. Taniyama, *Complex multiplication of abelian varieties and its applications to number theory*, Math. Soc. Japan 1961.

[20] T. SHIODA, The Hodge conjecture for Fermat varieties, Math. Ann. **245** (1979), 175–184.
[21] T. SHIODA, Algebraic cycles on abelian varieties of Fermat type, Math. Ann. **258** (1981), 65–80.
[22] T. SHIODA, What is known about the Hodge conjecture?, Adv. St. in Pure Math. **1** (1983), 55–68.
[23] T. SHIODA and T. KATSURA, On Fermat varieties, Tôhoku Math. J. **31** (1979), 97–115.
[24] B. VAN GEEMEN, Theta functions and cycles on some Abelian four folds, Math. Z. **221** (1996), 617–631.
[25] L. C. WASHINGTON, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83** (1982) Springer.
[26] S. P. WHITE, Sporadic cycles on CM abelian varieties, Compositio Math. **88** (1993), 123–142.
[27] K. YAMAMOTO, The gap group of multiplicative relationship of Gauss sums, Symp. Math. **XV** (1975), 427–440.

Present Address:
DEPARTMENT OF MATHEMATICS, RIKKYO UNIVERSITY,
NISHI-IKEBUKURO, TOSHIMA-KU, TOKYO, 171–8501 JAPAN.
e-mail: aoki@rkmath.rikkyo.ac.jp