J. Math. Soc. Japan
Vol. 39, No. 3, 1987

Some new algebraic cycles on Fermat varieties

By Noboru AOKI

(Received Nov. 11, 1985)

Introduction.

Let X_m^n be the Fermat variety of dimension n (n=even) and degree m defined over $\boldsymbol{C}$, that is, a hypersurface in the projective space $\boldsymbol{P}_{\boldsymbol{C}}^{n+1}$ defined by the diagonal equation:

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

Let μ_m be the group of m-th root of unity and set $G_m^n=(\mu_m)^{n+2}/\text{diagonal}$. Then G_m^n acts on X_m^n and its character group $\hat{G}_m^n$ can be identified with the following group:

$$\left\{(a_0, a_1, \cdots, a_{n+1})\in(\boldsymbol{Z}/m)^{n+2} \;\middle|\; \sum_{i=0}^{n+1} a_i=0\right\}$$

by setting $\alpha(g)=\zeta_0^{a_0}\cdots\zeta_{n+1}^{a_{n+1}}$ for any $\alpha=(a_0, \cdots, a_{n+1})\in\hat{G}_m^n$ and any $g=(\zeta_0, \cdots, \zeta_{n+1})\in G_m^n$.

As for the cohomology group of X_m^n, the following results are well known (see [3], [4]):

$$H_{\text{prim}}^n(X_m^n, \boldsymbol{C})=\bigoplus_{\alpha\in\mathfrak{A}_m^n} V(\alpha), \qquad \dim V(\alpha)=1,$$

$$(H^{r,r}(X_m^n)\cap H_{\text{prim}}^n(X_m^n, \boldsymbol{Q}))\otimes\boldsymbol{C}=\bigoplus_{\alpha\in\mathfrak{B}_m^n} V(\alpha),$$

where $V(\alpha)=\{\xi\in H^n(X_m^n, \boldsymbol{C}) \mid g^*(\xi)=\alpha(g)\xi,\ \forall g\in G_m^n\}$ and $r=n/2$. The index sets $\mathfrak{A}_m^n$ and $\mathfrak{B}_m^n$ are defined as follows:

$$\mathfrak{A}_m^n=\{(a_0, \cdots, a_{n+1})\in\hat{G}_m^n \mid a_i\neq 0 \ \text{ for every } 0\leqq i\leqq n+1\},$$

$$\mathfrak{B}_m^n=\left\{(a_0, \cdots, a_{n+1})\in\mathfrak{A}_m^n \;\middle|\; \sum_{i=0}^{n+1}\langle ta_i/m\rangle=n/2+1,\ \forall t\in(\boldsymbol{Z}/m)^\times\right\},$$

where, for $a\in\boldsymbol{Z}/m$, $\langle a/m\rangle$ expresses the unique rational number such that $0\leqq\langle a/m\rangle<1$, $m\cdot\langle a/m\rangle\equiv a \pmod m$.

The Hodge conjecture for X_m^n asserts that the following claim is true for every $\alpha\in\mathfrak{B}_m^n$.

CLAIM(α): *$V(\alpha)$ is generated by the cohomology classes of algebraic cycles on X_m^n.*

For any algebraic cycle Z of dimension $n/2$ on X_m^n, put $G_Z=\{g\in G_m^n \mid g(Z)=Z\}$, and for any $\alpha\in\mathfrak{A}_m^n$ define an element of $H^n(X_m^n, \boldsymbol{C})$ by

$$\omega_\alpha(Z)=\frac{1}{\#(G_Z)}\sum_{g\in G_m^n}\overline{\alpha(g)}g^*([Z]),$$

where $[Z]$ denotes the cohomology class of Z. Then $\omega_\alpha(Z)$, which may be zero, belongs to $V(\alpha)$. In fact, for any $\xi\in H^n(X_m^n, \boldsymbol{C})$, if we put

$$P_\alpha(\xi)=\frac{1}{\#(G_m^n)}\sum_{g\in G_m^n}\overline{\alpha(g)}g^*(\xi)$$

(i.e. P_α is the projector from $H^n(X_m^n, \boldsymbol{C})$ to $V(\alpha)$), then we have

$$\omega_\alpha(Z)=\frac{\#(G_m^n)}{\#(G_Z)}P_\alpha([Z]).$$

We note that, for any algebraic cycle Z on X_m^n, $\omega_\alpha(Z)=0$ unless $\alpha\in\mathfrak{B}_m^n\cup\{0\}$ and $\operatorname{Ker}\alpha\supset G_Z$. If there exists an algebraic cycle Z on X_m^n such that $\omega_\alpha(Z)\neq 0$, then claim(α) is true, and so we want to find such an algebraic cycle for each $\alpha\in\mathfrak{B}_m^n$. If $\omega_\alpha(Z)\neq 0$, we say that Z represents the class α (cf. [2]).

In view of the geometric results due to Ran [3] and Shioda [4] and the structure theorem of $\mathfrak{B}_m^n$ in our previous paper [1], there exist, for any fixed m, finitely many elements α of $\bigcup_{n\geq 0}\mathfrak{B}_m^n$, called "standard" or "semistandard" elements, such that, once claim(α) is verified for all such α, it will prove the Hodge conjecture for the Fermat variety X_m^n of degree m for all dimension n. See § 1 below for more details.

The purpose of this paper is to define explicitly some new algebraic cycles on Fermat varieties. Namely, for each odd prime divisor p of m, we construct an algebraic cycle on X_m^{p-1} which represents "p-standard" elements (Theorem 2-1). As a corollary we can prove the Hodge conjecture for X_m^n for all n when m is a power of a prime number (Corollary 2-3).

The author is deeply gratefull to Professor Shioda for many helpful comments on this paper.

§ 1. Structure of $\mathfrak{B}_m^n$.

First let us consider a subset $\mathfrak{D}_m^n$ of $\mathfrak{B}_m^n$ defined as follows

$$\mathfrak{D}_m^n=\{\alpha\in\mathfrak{A}_m^n \mid \alpha\sim(a_0, -a_0, \cdots, a_r, -a_r) \text{ for some } a_0, \cdots, a_r\in\boldsymbol{Z}/m-\{0\}\}$$

where $r=n/2$ and we write $\alpha\sim\beta$ if α is equal to β up to permutation. It is easy to see that $\mathfrak{D}_m^n$ is a subset of $\mathfrak{B}_m^n$. Ran and Shioda showed that any element of $\mathfrak{D}_m^n$ is represented by a certain algebraic cycle. In fact, let $\delta=(a_0, -a_0, \cdots, a_r, -a_r)\in\mathfrak{D}_m^n$ and L an r-dimensional linear space on X_m^n defined by the equations:

$$x_{2i}+\varepsilon x_{2i+1}=0 \qquad (i=0, 1, \cdots, r),$$

where $\varepsilon=\exp(\pi\sqrt{-1}/m)$. Then we have the following result. (As for the case $n=2$, see [5].)

THEOREM 1-1 (Shioda [6]). *The linear space L represents δ. More precisely we have*

$$\omega_\delta(L)\cdot\overline{\omega_\delta(L)}=(-1)^r m^{n+1}.$$

The structure of $\mathfrak{B}_m^n$ has been studied in detail in our previous work [1]. Here we recall some results. Fix m and let p be a prime divisor of m, and put $d=m/p$. Then, for each i such that $d/(i, d)>2$, let

$$\sigma_{p,i}=\begin{cases}(i, i+d, \cdots, i+(p-1), m-pi) & \text{if } p\geqq 3,\\ (i, i+d, m-2i, d) & \text{if } p=2.\end{cases}$$

These elements belong to $\mathfrak{B}_m^{p-1}$ or $\mathfrak{B}_m^2$ respectively, which are called "standard" (more precisely "p-standard") elements. Put

$$\mathfrak{A}_m=\bigcup_{n\geq 0}\mathfrak{A}_m^n, \qquad \mathfrak{B}_m=\bigcup_{n\geq 0}\mathfrak{B}_m^n \qquad \text{and} \qquad \mathfrak{D}_m=\bigcup_{n\geq 0}\mathfrak{D}_m^n,$$

then we have $\mathfrak{D}_m\subset\mathfrak{B}_m\subset\mathfrak{A}_m$. We define a subset $\mathfrak{S}_m$ of $\mathfrak{A}_m$ by

$$\mathfrak{S}_m=\{\alpha\in\mathfrak{A}_m \mid \alpha\sim\sigma_1*\sigma_2*\cdots*\sigma_k,\ \sigma_i:\text{standard}\},$$

where $*$ denotes the juxtaposition. Clearly $\mathfrak{S}_m$ is a subset of $\mathfrak{B}_m$.

When m is a power of a prime number, the standard elements form "generators" of $\mathfrak{B}_m$ modulo $\mathfrak{D}_m$ in the sense of the following theorem, which is a special case of Theorem D of [1].

THEOREM 1-2. *Suppose that m is a power of a prime number p. Then for any* $\alpha\in\mathfrak{B}_m$, *there exist* $\sigma\in\mathfrak{S}_m$, $\delta, \delta'\in\mathfrak{D}_m$ *such that* $\alpha*\delta\sim\sigma*\delta'$.

However the above theorem does not hold for general m. To state the general structure theorem for $\mathfrak{B}_m$ we need another type of elements of $\mathfrak{B}_m$, i.e. "semi-standard" elements defined in [1], §5. Put

$$\mathfrak{S}'_m=\{\alpha\in\mathfrak{A}_m \mid \alpha\sim\beta_1*\cdots*\beta_k,\ \beta_i:\text{semi-standard}\}.$$

Then Theorem D of [1] can be restated as follows.

THEOREM 1-3. *For any* $\alpha\in\mathfrak{B}_m$ *there exist* $\sigma\in\mathfrak{S}_m$, $\sigma'\in\mathfrak{S}'_m$ *and* $\delta, \delta'\in\mathfrak{S}_m$ *such that* $\alpha*\delta\sim\sigma*\sigma'*\delta'$.

On the other hand we can show the following theorem using inductive structure.

THEOREM 1-4 (Shioda [4], Ran [3]). *Let r and s be non-negative even integers such that $n=r+s+2$, and let $\alpha\in\mathfrak{B}_m^r$, $\beta\in\mathfrak{B}_m^s$. Then the following statements hold.*
(i) *If* claim(α) *and* claim(β) *are true, then* claim($\alpha*\beta$) *is also true.*
(ii) *If there exists $\delta\in\mathfrak{D}_m^s$ such that* claim($\alpha*\delta$) *is true, then* claim(α) *is also true.*

In view of the above theorems, to prove claim(α) for all $\alpha\in\mathfrak{B}_m$, we have only to prove claim(α) for α of standard type and semi-standard type. In the next section we shall define a subvariety of X_m^{p-1} which represents p-standard elements for every odd prime p. As for the case $p=2$, see [2]. As for semi-standard elements, however, we have not yet found such a subvariety except for a few cases.

§ 2. Statement of the main theorem.

Let p ($\geqq 3$) and d be as before (i.e. $m=pd$), and put $r=(p-1)/2$. Let $\alpha=\sigma_{p,a}=(a, a+d, \cdots, a+(p-1)d, -pa)$, $(a, d)=1$, and fix it throughout this paper. We shall study a subvariety $Y\subset \boldsymbol{P}_C^p$ of codimension $r+1$ defined by the following equations:

$$\text{(2.1)}\qquad \begin{cases} x_0^{kd}+x_1^{kd}+\cdots+x_{p-1}^{kd}=0 & (1\leqq k\leqq r), \\ x_p^p-\varepsilon^p\sqrt[d]{p}\,x_0x_1\cdots x_{p-1}=0, \end{cases}$$

where $\varepsilon=\exp(\pi\sqrt{-1}/m)$. The main result in this paper is the following theorem.

THEOREM 2-1. *The variety Y defined by* (2.1) *is a subvariety of X_m^{p-1} of codimension r and it represents the class* $\boldsymbol{\alpha}$. *More precisely we have*

$$\omega_\alpha(Y)\cdot\overline{\omega_\alpha(Y)}=(-1)^r p^{p-2}m^p.$$

REMARK 2-2. In case $p=2$, define a curve C on X_m^2 by the equation:

$$\begin{cases} x_0^d+x_1^d+\sqrt{-1}\,x_2^d=0, \\ x_3^2-\sqrt[d]{2}\,x_0x_1=0, \end{cases}$$

where $d=m/2$. Then we have

$$\omega_\alpha(C)\cdot\overline{\omega_\alpha(C)}=-2m^3,$$

where $\alpha=(i, i+d, m-2i, d)\in\mathfrak{B}_m^2$ (cf. [2]).

COROLLARY 2-3. *If m is a power of a prime number, then Hodge conjecture for X_m^n is true for all n.*

PROOF. This is an immediate consequence of Theorem 1-2, Theorem 1-4, Theorem 2-1 and Remark 2-2. Q.E.D.

§ 3. Some properties of Y.

Throughout this section and the next section we shall fix the following notation:

$p=$ an odd prime divisor of m
$d=m/p>1$
$r=(p-1)/2\geqq 1$
$X=X_m^{p-1}$
$G=G_m^{p-1},\quad \hat{G}=\hat{G}_m^{p-1}$
$G_0=\{g\in G \mid g^d=(1:1:\cdots:1:*)\}$
$\sigma=(1, 1, \cdots, 1, -p)\in\hat{G}$
$\alpha=(a, a+d, a+2d, \cdots, a+(p-1)d, -pa)=\sigma_{p,a}$
$\varepsilon=\exp(\pi\sqrt{-1}/m),\quad \varepsilon^m=-1$
$y_i=x_i^d\ (0\leqq i\leqq p-1)$
$f_0=x_p^p-cx_0x_1\cdots x_{p-1},\quad c=\varepsilon^p\sqrt[d]{p}$
$f_{0,\zeta}=x_p^p-\zeta c x_0x_1\cdots x_{p-1},\quad \zeta^d=1$
$f_i=$ the i-th fundamental symmetric polynomial in $y_0, \cdots, y_{p-1}$ $(1\leqq i\leqq p)$
$Y=$ the subvariety of $\boldsymbol{P}_C^p$ defined in § 2
$Y_g=g(Y),\quad g\in G$
$G_Y=\{g\in G \mid Y_g=Y\}$
$\omega_\beta=\omega_\beta(Y),\quad \beta\in G$
$L=$ a linear space section of X of codimension r

PROPOSITION 3-1. *The variety Y has the following properties:*

(i) *Y is a subvariety of X of middle dimension.*

(ii) *$G_Y=G_0\cap\operatorname{Ker}\sigma$. In particular $G_Y\subset\operatorname{Ker}\alpha$.*

(iii) $\deg Y=pr!\,d^r$.

(iv) *Let D_i be the divisor on X defined by the equation: $f_i=0$ $(1\leqq i\leqq r)$, then we have*

$$D_1\cdot D_2\cdot\cdots\cdot D_r=\sum_{g\in G_0/G_Y} Y_g.$$

(v) *The right hand side of the above equality is rationally equivalent to $r!\,d^rL$.*

PROOF. First we note that Y can be defined by the equations $f_0=f_1=\cdots=f_r=0$ since $x_0^{kd}+x_1^{kd}+\cdots+x_{p-1}^{kd}=y_0^k+\cdots+y_{p-1}^k$ $(1\leqq k\leqq r)$ are symmetric polynomials of $y_0, \cdots, y_{p-1}$, and so they can be expressed by the polynomials of f_i's. Since the converse is also true, the equations $f_0=\cdots=f_r=0$ and equations (2.1) define the same variety.

The assertions (iii), (iv) and (v) are easy consequences of the definition of Y. So we prove (i) and (ii). To show (i), we need the following

LEMMA 3-2. *For any integer $l\geqq 1$, we have*

$$y_0^l+\cdots+y_{p-1}^l=(-1)^l l \sum_{\substack{\Sigma i e_i=l \\ e_i\geq 0}}(-1)^{e_1+\cdots+e_p}\frac{(e_1+\cdots+e_p-1)!}{e_1!\cdots e_p!}f_1^{e_1}\cdots f_p^{e_p}$$

where the summation runs over p-tuples $(e_1, e_2, \cdots, e_p)$ *of non-negative integers* e_i *satisfying* $\sum_{i=1}^p ie_i=l$.

If we put $l=p$ in the above lemma, we have

$$(3.1)\qquad x_0^m+\cdots+x_{p-1}^m=-p\sum_{\substack{\Sigma i e_i=p \\ e_i\geq 0}}(-1)^{e_1+\cdots+e_p}\frac{(e_1+\cdots+e_p-1)!}{e_1!\cdots e_p!}f_1^{e_1}\cdots f_p^{e_p}$$

since $y_i^p=x_i^m$ $(0\leqq i\leqq p-1)$. It is easily shown that the right hand side of (3.1) can be written as follows:

$$f_1g_1+\cdots+f_rg_r+pf_p,$$

where

$$(3.2)\qquad g_i=-pf_{p-i}+(\text{polynomials in } f_1, \cdots, f_{p-i-1}).$$

Note that

$$x_p^m+pf_p=x_p^m+p(x_0x_1\cdots x_{p-1})^d=\prod_{\zeta^d=1}f_{0,\zeta},$$

where the product runs over the d-th roots of unity. Therefore we have

$$(3.3)\qquad x_0^m+\cdots+x_p^m=f_1g_1+\cdots+f_rg_r+\prod f_{0,\zeta}.$$

Since Y is defined by the equations $f_0=\cdots=f_r=0$, (3.3) shows that Y is a subvariety of X. This proves (i).

Next note that Y_g $(g\in G)$ is defined by the following equations:

$$\begin{cases} \bar{\zeta}_0^{kd}x_0^{kd}+\cdots+\bar{\zeta}_{p-1}^{kd}x_{p-1}^{kd}=0 & (1\leqq k\leqq r), \\ x_p^p-\overline{\sigma(g)}cx_0x_1\cdots x_{p-1}=0. \end{cases}$$

It follows that $G_0\cap\operatorname{Ker}\sigma\subset G_Y$. To show the converse it is sufficient to show the existence of a point $P\in Y$ such that $P\notin Y_g$ for each $g\in G-(G_0\cap\operatorname{Ker}\sigma)$. For that purpose let ζ be a primitive m-th root of unity. Then ζ^d is a primitive p-th root of unity. Put $P_t=(1:\zeta^t:\zeta^{2t}:\cdots:\zeta^{(p-1)t}:\sqrt[m]{p})$, $1\leqq t\leqq p-1$. Then $P_t\in Y$, but for any $g\in G-(G_0\cap\operatorname{Ker}\sigma)$ there exists some t such that $P_t\notin Y_g$. This proves (ii) and completes the proof of Proposition 3-1. Q.E.D.

For $i=0, 1, \cdots, r$, let $Y^{(i)}$ be the variety defined by the equations:

$$f_0=f_1=\cdots=f_{r-i}=g_{r-i+1}=\cdots=g_r=0.$$

By (3.3), $Y^{(i)}$ is contained in X_m^{p-1} for every i.

LEMMA 3-3. *For each* $i=1, 2, \cdots, r$, *there exists an integer* s_i *such that*

$$Y \sim (-1)^i Y^{(i)} + s_i L,$$

where $\sim$ *denotes rational equivalence.*

PROOF. By the definition of $Y^{(i)}$'s, we have

$$Y^{(j)} + Y^{(j+1)} \sim a_j L \qquad (j=0, 1, \cdots, r-1), \tag{3.4}$$

where $a_j = p(r-j-1)!(r+j)!/r!$. Taking the alternating sum of (3.4) from $j=0$ to $j=i-1$, we have

$$Y + (-1)^i Y^{(i)} \sim s_i L, \qquad s_i = \sum_{j=0}^{i-1} (-1)^j a_j.$$

This proves the assertion. Q. E. D.

For i, j $(0 \leqq i \neq j \leqq p-1)$, put

$$G_{ij} = \{(\zeta_0 : \cdots : \zeta_p) \in G \mid \zeta_k^d = 1, \ k \neq i, j, p, \ (\zeta_i \zeta_j)^d = 1\}.$$

Then obviously $G_{ij} \supset G_0$.

PROPOSITION 3-4. *For any* $g \in G_{ij} - \mathrm{Ker}\, \sigma$,
(i) *if* $g \in G_0$, *then* $Y^{(r)} \cdot Y_g = 0$,
(ii) *if* $g \in G_{ij} - G_0$, *then* $Y^{(r-1)} \cdot Y_g = 0$.

PROOF. (i) If $g \in G_0 - \mathrm{Ker}\, \sigma$, then $Y^{(r)} \cap Y_g$ is defined by the equations:

$$f_0 = f_{0,\zeta} = f_1 = \cdots = f_r = g_1 = \cdots = g_r = 0,$$

where $\zeta = \sigma(g) \neq 1$. It follows from the first two equations that $x_p = x_0 x_1 \cdots x_{p-1} = 0$. Furthermore from the other equations we have $f_i = 0$ $(1 \leqq i \leqq p-1)$. Since $x_0 x_1 \cdots x_{p-1} = 0$, f_p is also zero. This implies that $y_0 = y_1 = \cdots = y_{p-1} = 0$ or equivalently $x_0 = x_1 = \cdots = x_{p-1} = 0$. Since x_p is also zero, this shows that $Y^{(r)} \cap Y_g = \emptyset$, and so $Y^{(r)} \cdot Y_g = 0$.

(ii) We may assume $i=0$, $j=1$ without loss of generality. If $g = (\zeta_0 : \cdots : \zeta_p) \in G_{01} - (G_0 \cup \mathrm{Ker}\, \sigma)$, then $Y^{(r-1)} \cap Y_g$ is defined by the equations:

$$f_0 = f_{0,\zeta} = f'_1 = \cdots = f'_r = f_1 = g_2 = \cdots = g_r = 0,$$

where $\zeta = \sigma(g) \neq 1$ as before, and where $f'_i = f_i(\bar{\eta} y_0, \eta y_1, y_2, \cdots, y_{p-1})$, $\eta = \zeta_0^d \neq 1$. As before we have $x_p = x_0 x_1 \cdots x_{p-1} = 0$. The equations $f'_1 = f_1 = 0$ implies

$$\bar{\eta} y_0 + \eta y_1 + y_2 + \cdots + y_{p-1} = 0,$$

$$y_0 + y_1 + y_2 + \cdots + y_{p-1} = 0.$$

Therefore y_1 and $y_2 + \cdots + y_{p-1}$ are of the form (const.)$\times y_0$. From this and the other equations, it follows that the k-th fundamental symmetric polynomials in $y_2, \cdots, y_{p-1}$ must be of the form (const.)$\times y_0^k$ for $k=1, 2, \cdots, p-2$. In particular, $y_2\cdots y_{p-1}=(\text{const.})\times y_0^{p-2}$, and so $0=(x_0\cdots x_{p-1})^d=y_0\cdots y_{p-1}=(\text{const.})\times y_0^p$. Hence $y_0=0$ and this implies that $y_1=y_2=\cdots=y_{p-1}=0$. Therefore we have $x_0=x_1=\cdots=x_{p-1}=0$. Since x_p is also zero, this shows that $Y^{(r-1)}\cap Y_g=\emptyset$, and so $Y^{(r-1)}\cdot Y_g=0$. Q.E.D.

COROLLARY 3-5. (i) *If $g\in G_0$, then*

$$Y\cdot Y_g=\begin{cases}(-1)^r p!\,d^{p-1}+s_r\deg(Y) & g\in G_Y,\\ s_r\deg(Y) & g\in G_0-G_Y.\end{cases}$$

(ii) *If $g\in G_{ij}-G_0$, then*

$$Y\cdot Y_g=\begin{cases}(-1)^{r-1}p(p-2)!\,d^{p-1}+s_{r-1}\deg(Y) & g\in(G_{ij}-G_0)\cap\operatorname{Ker}\sigma,\\ s_{r-1}\deg(Y) & g\in G_{ij}-(G_0\cup\operatorname{Ker}\sigma).\end{cases}$$

PROOF. Put $k=r$ or $r-1$ according to (i) or (ii). Then, from Lemma 3-3, we have

$$Y\cdot Y_g=(-1)^k Y^{(k)}\cdot Y_g+s_k\deg(Y), \tag{3.5}$$

since $\deg(Y_g)=\deg(Y)$. If $g\notin\operatorname{Ker}\sigma$, then, by Proposition 3-4, we have $Y^{(k)}\cdot Y_g=0$. This implies $Y\cdot Y_g=s_k\deg(Y)$. If $g\in\operatorname{Ker}\sigma$, then by Proposition 3-1 (iii), (iv), we have

$$Y_g\sim-\sum_{h\in(G_0-G_Y)/G_Y}Y_{gh}+r!\,d^rL.$$

Therefore

$$\begin{aligned}Y^{(k)}\cdot Y_g&=-\sum_{h\in(G_0-G_Y)/G_Y}Y^{(k)}\cdot Y_{gh}+r!\,d^r\deg(Y^{(k)})\\&=r!\,d^r\deg(Y^{(k)}),\end{aligned}$$

since $Y^{(k)}\cdot Y_{gh}=0$ for $h\in G_0-G_Y$ by the above argument. From (3.5), we have

$$Y\cdot Y_g=(-1)^k r!\,d^r\deg(Y^{(k)})+s_k\deg(Y).$$

Since $\deg(Y^{(r)})=(p!/r!)d^r$ and $\deg(Y^{(r-1)})=(p(p-2)!/r!)d^r$, we get the conclusion. Q.E.D.

§ 4. Proof of main theorem.

In this section we give the proof of Theorem 2-1. First note that

$$[Y]=\sum_{\beta\in\hat{\mathfrak{G}}}P_\beta([Y])=\frac{\#(G_Y)}{m^p}\sum_{\beta\in\hat{\mathfrak{G}}}\omega_\beta(Y),$$

since P_β is the projector. Let

$$S'=\{\beta=(b_0,b_1,\cdots,b_p)\in\mathfrak{A}_m^{p-1}\mid b_0\equiv\cdots\equiv b_{p-1}\ (\operatorname{mod} d)\},$$

$$S=\{\beta=(b_0, \cdots, b_p)\in S' \mid b_p=-pb_0,\ \beta\sim\sigma_{p,b_0}\}.$$

Furthermore, for $0\leqq i\neq j\leqq p-1$, let

$$S_{ij}=\{\beta=(b_0, \cdots, b_p)\in S' \mid b_i=b_j\}.$$

LEMMA 4-1. *If* $\operatorname{Ker}\beta\supset G_Y$, *then* $\beta\in S'\cup\{0\}$.

PROOF. Let $\beta=(b_0, \cdots, b_p)$ and suppose that $\operatorname{Ker}\beta\supset G_Y$. Let ζ be a primitive d-th root of unity and put

$$g_i=(\zeta:1:\cdots:1:\underset{\hat{i}}{\zeta^{-1}}:1:\cdots:1)\in G_Y,$$

then $1=\beta(g_i)=\zeta^{b_0-b_i}$ for each $i=1, \cdots, p-1$. This implies $b_i\equiv b_0 \pmod d$. Hence $\beta\in S'\cup\{0\}$. Q. E. D.

LEMMA 4-2. *If* $\beta\notin S'\cup\{0\}$, *then* $\omega_\beta(Y)=0$.

PROOF. If $\beta\notin S'\cup\{0\}$, then $\operatorname{Ker}\beta\not\supset G_Y$ by Lemma 4-1. Therefore

$$\sum_{h\in G_Y}\overline{\beta(h)}h^*([Y])=\Big(\sum_{h\in G_Y}\overline{\beta(h)}\Big)[Y]=0. \tag{4.1}$$

Since $\omega_\beta(Y)=(1/\#(G_Y))\sum_{g\in G/G_Y}\overline{\beta(g)}g^*(\sum_{h\in G_Y}\overline{\beta(h)}h^*([Y]))$, (4.1) implies $\omega_\beta(Y)=0$. Q. E. D.

PROPOSITION 4-3. *Let* $\sigma=(1, 1, \cdots, 1, -p)\in\hat{G}$ *as before and put*

$$\eta=\sum_{g\in G_0/G_Y}\overline{\sigma(g)}^a g^*([Y]),\qquad \eta_{ij}=\sum_{g\in G_{ij}/G_Y}\overline{\sigma(g)}^a g^*([Y])\quad\text{for } a\in(\boldsymbol{Z}/m)^\times.$$

Then we have

(i) $\eta\cdot\bar{\eta}=(-1)^r p!\,d^p$,

(ii) $\eta_{ij}\cdot\bar{\eta}_{ij}=0$ *for any* i, j $(0\leqq i\neq j\leqq p-1)$.

PROOF. Put $\xi=\eta$ or η_{ij} and $H=G_0$ or G_{ij} according to (i) or (ii). Then

$$\begin{aligned}\xi\cdot\bar{\xi}&=\Big(\sum_{g_1\in H/G_Y}\overline{\sigma(g_1)}^a g_1^*([Y])\Big)\Big(\sum_{g_2\in H/G_Y}\sigma(g_2)^a g_2^*([Y])\Big)\\&=\sum_{g_1, g_2\in H/G_Y}\overline{\sigma(g_1g_2^{-1})}^a g_1^*([Y])\cdot g_2^*([Y])\\&=\sum_{g, g_2\in H/G_Y}\overline{\sigma(g)}^a (g_2g)^*([Y])\cdot g_2^*([Y])\\&=\#(H/G_Y)\sum_{g\in H/G_Y}\overline{\sigma(g)}^a g^*([Y])\cdot[Y]\\&=\#(H/G_Y)\sum_{g\in H/G_Y}\overline{\sigma(g)}^a Y\cdot Y_g.\end{aligned}$$

(i) In this case the above formula means

$$\eta\cdot\bar{\eta}=d\cdot\sum_{g\in G_0/G_Y}\overline{\sigma(g)}^{a}Y\cdot Y_g.$$

Therefore, by Corollary 3-5 (i), we have

$$\begin{aligned}\eta\cdot\bar{\eta}&=d\Big\{(-1)^r p!\,d^{p-1}+\Big(\sum_{g\in G_0/G_Y}\overline{\sigma(g)}^{a}\Big)s_r\deg(Y)\Big\}\\&=(-1)^r p!\,d^p,\end{aligned}$$

since $\sum_{g\in G_0/G_Y}\overline{\sigma(g)}^{a}=0$ by Proposition 3-1 (ii).

(ii) In this case we must show that

$$\sum_{g\in G_{ij}/G_Y}\overline{\sigma(g)}^{a}Y\cdot Y_g=0.$$

By Corollary 3-5 (ii) and the above argument, we have

$$\begin{aligned}\sum_{g\in G_{ij}/G_Y}\overline{\sigma(g)}^{a}Y\cdot Y_g&=\sum_{g\in(G_{ij}-G_0)/G_Y}\overline{\sigma(g)}^{a}Y\cdot Y_g+\sum_{g\in G_0/G_Y}\overline{\sigma(g)}^{a}Y\cdot Y_g\\&=\Big(\sum_{g\in(G_{ij}-G_0)\cap\operatorname{Ker}\sigma/G_Y}\overline{\sigma(g)}^{a}\Big)(-1)^{r-1}p(p-2)!\,d^{p-1}\\&\quad+\Big(\sum_{g\in(G_{ij}-G_0)/G_Y}\overline{\sigma(g)}^{a}\Big)s_{r-1}\deg(Y)+(-1)^r p!\,d^{p-1}.\end{aligned}$$

This is equal to

$$(p-1)(-1)^{r-1}p(p-2)!\,d^{p-1}+(-1)^r p!\,d^{p-1}=0,$$

since $\alpha|_{G_{ij}\cap\operatorname{Ker}\sigma}=1$, $\#((G_{ij}-G_0)\cap\operatorname{Ker}\sigma/G_Y)=p-1$ and $\sum_{g\in(G_{ij}-G_0)}\overline{\sigma(g)}^{a}=0$. This completes the proof. Q.E.D.

PROPOSITION 4-4. *If* $\beta\notin S\cup\{0\}$, *then* $\omega_\beta(Y)=0$.

PROOF. In view of Lemma 4-2, it is sufficient to show that $\omega_\beta(Y)=0$ for all $\beta\in S'-S$. Since $\omega_\beta(Y)=0$ for $\beta\notin S'\cup\{0\}$, we have

$$[Y]=\frac{\#(G_Y)}{m^p}\Big(\omega_0(Y)+\sum_{\beta\in S'}\omega_\beta(Y)\Big).$$

Therefore, putting $\omega_\beta=\omega_\beta(Y)$,

$$\begin{aligned}\eta_{ij}&=\sum_{g\in G_{ij}/G_Y}\overline{\sigma(g)}^{a}g^*([Y])\\&=\frac{\#(G_Y)}{m^p}\Big(\Big(\sum_{g\in G_{ij}/G_Y}\overline{\sigma(g)}^{a}\Big)\omega_0+\sum_{g\in G_{ij}/G_Y}\sum_{\beta\in S'}\overline{\sigma(g)}^{a}g^*\omega_\beta(Y)\Big)\\&=\frac{\#(G_Y)}{m^p}\Big(\sum_{g\in G_{ij}/G_Y}\sum_{\beta\in S'}\overline{\sigma(g)}^{a}\beta(g)\omega_\beta\Big)\end{aligned}$$

$$= \frac{\#(G_Y)}{m^p}\sum_{\beta\in S'}\Big(\sum_{g\in G_{ij}/G_Y}\overline{\sigma(g)}^a\beta(g)\Big)\omega_\beta$$

$$= \frac{\#(G_Y)}{m^p}\#(G_{ij}/G_Y)\sum_{\beta\in S_{ij,a}}\omega_\beta$$

$$= \frac{\#(G_{ij})}{m^p}\sum_{\beta\in S_{ij,a}}\omega_\beta,$$

where $S_{ij,a}=\{\beta\in S_{ij} \mid \beta\equiv\sigma_{p,a} \pmod d\}$. Therefore

$$\eta_{ij}\cdot\bar\eta_{ij} = (\#(G_{ij})/m^p)^2\sum_{\beta,\beta'\in S_{ij,a}}\omega_\beta\cdot\bar\omega_{\beta'}$$

$$= (\#(G_{ij})/m^p)^2\sum_{\beta\in S_{ij,a}}\omega_\beta\cdot\bar\omega_\beta .$$

Hence, by Proposition 4-3 (ii), we have $\eta_{ij}\cdot\bar\eta_{ij}=0$ and so

$$\sum_{\beta\in S_{ij,a}}\omega_\beta\cdot\bar\omega_\beta = 0. \tag{4.2}$$

Here, by the Hodge index theorem ([7], Th. 7, p. 77), we know that $(-1)^r\omega_\beta\cdot\bar\omega_\beta\geqq 0$ for all $\beta\in\mathfrak{A}_m^{p-1}$ and that the equality holds if and only if $\omega_\beta=0$. From this fact and (4.2), we have $\omega_\beta=0$ for all $\beta\in S_{ij,a}$. Since $S'-S$ is covered with $S_{ij,a}$ $(0\leqq i\neq j\leqq p-1,\ 0<a<d)$, we conclude that $\omega_\beta(Y)=0$ for all $\beta\in S'-S$. Q.E.D.

Now we can prove Theorem 2-1. By Proposition 4-4, $[Y]$ can be written as follows:

$$[Y] = \frac{\#(G_Y)}{m^p}\Big(\omega_0+\sum_{\beta\in S}\omega_\beta(Y)\Big).$$

Therefore

$$\eta = \frac{\#(G_Y)}{m^p}\Big\{\sum_{g\in G_0/G_Y}\overline{\sigma(g)}^a g^*\omega_0+\sum_{g\in G_0/G_Y}\sum_{\beta\in S}\overline{\sigma(g)}^a\beta(g)\omega_\beta\Big\}$$

$$= \frac{\#(G_Y)}{m^p}\sum_{\beta\in S}\Big(\sum_{g\in G_0/G_Y}\overline{\sigma(g)}^a\beta(g)\Big)\omega_\beta$$

$$= \frac{\#(G_Y)}{m^p}\sum_{0<b<d}\sum_{\beta\in S_b}\Big(\sum_{g\in G_0/G_Y}\sigma(g)^{b-a}\Big)\omega_\beta,$$

where $S_b=\{\beta\in S \mid \beta\sim\sigma_{p,b}\}$. Since σ induces an isomorphism: $G_0/G_Y\xrightarrow{\sim}\mu_d$, we have

$$\sum_{g\in G_0/G_Y}\sigma(g)^{b-a} = \begin{cases} d & \text{if } b\equiv a \pmod d, \\ 0 & \text{otherwise.}\end{cases}$$

It follows that

$$\eta = \frac{\#(G_Y)}{m^p}\cdot d\cdot\sum_{\beta\in S_a}\omega_\beta = (1/p)^{p-1}\sum_{\beta\in S_a}\omega_\beta .$$

It is easy to see that

$$\omega_{\beta}\cdot\bar{\omega}_{\beta'}=\begin{cases}\omega_{\alpha}\cdot\bar{\omega}_{\alpha} & \text{if } \beta=\beta',\\ 0 & \text{otherwise}.\end{cases}$$

for any $\beta, \beta'\in S_{\alpha}$. Therefore

$$\eta\cdot\bar{\eta}=(1/p)^{2(p-1)}\sum_{\beta,\beta'\in S_{\alpha}}\omega_{\beta}\cdot\bar{\omega}_{\beta'}$$
$$=(1/p)^{2(p-1)}p!\,\omega_{\alpha}\cdot\bar{\omega}_{\alpha},$$

since $\#(S_{\alpha})=p!$. By Proposition 4-3 (i), we have

$$(-1)^{r}p!\,d^{p}=(1/p)^{2(p-1)}p!\,\omega_{\alpha}\cdot\bar{\omega}_{\alpha}.$$

Hence

$$\omega_{\alpha}\cdot\bar{\omega}_{\alpha}=(-1)^{r}d^{p}p^{2(p-1)}=(-1)^{r}p^{p-2}m^{p}.$$

This completes the proof of Theorem 2-1.

References

[1] N. Aoki, On some arithmetic problems related to the Hodge cycles on the Fermat varieties, Math. Ann., **266** (1983), 23-54.
[2] N. Aoki, and T. Shioda, Generators of the Néron-Severi group of a Fermat surface, Progress in Mathematics, Vol. 35, Birkhäuser.
[3] Z. Ran, Cycles on Fermat hypersurfaces, Compositio Math., **42** (1981), 121-142.
[4] T. Shioda, The Hodge conjecture for Fermat varieties, Math. Ann., **245** (1979), 175-184.
[5] T. Shioda, On the Picard number of a Fermat surface, J. Fac. Sci. Univ. Tokyo, **28** (1982), 725-734.
[6] T. Shioda, Lectures on Fermat varieties, in preparation.
[7] A. Weil, Variétés Kählériennes, Hermann, Paris, 1958.

Noboru AOKI
Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Tokyo 171
Japan