HIROSHIMA MATH. J.
18 (1988), 95–111

On Hasse-Witt matrices of Fermat varieties

Keisuke TOKI

(Received May 19, 1987)

Introduction

Let X be an n-dimensional Fermat variety of degree d

$$x_0^d + x_1^d + \cdots + x_{n+1}^d = 0 \quad (d \geqq n+2)$$

in $\mathbf{P}^{n+1}$, where $x_0, x_1, \ldots, x_{n+1}$ are homogeneous coordinates. We are concerned with the p-th power frobenius action F on the n-th cohomology group $H^n(X, \mathcal{O}_X)$ of X over an algebraic closure k of the field $\mathbf{F}_p$ ($p>0$; $p\nmid d$). The F-module $H^n(X, \mathcal{O}_X)$ is canonically isomorphic to the G_h-module $H^{n+1}(\mathbf{P}^{n+1}, \mathcal{O}_{\mathbf{P}^{n+1}}(-d))$, and we know that the vector space $H^{n+1}(\mathbf{P}^{n+1}, \mathcal{O}_{\mathbf{P}^{n+1}}(-d))$ has as basis $\mathscr{W}_0$ (cf. §1). We now consider the matrix (the so-called Hasse-Witt matrix) HW(X) of G_h with respect to $\mathscr{W}_0$.

In this paper, we show mainly the following theorems:

THEOREM I. *For positive integers n, d and p (p; prime number with $p\nmid d$ and $d\geqq n+2$) given as above, we let ρ_i be the number of all elements in $\mathscr{W}_0$ of type i defined in* §1. *We can arrange the ρ_i's by some integers $f_0>f_1>\cdots>f_r>0$ as follows*:

$$\rho_i = 0 \quad \text{for} \quad i > f_0, \quad \rho_{f_s} = \rho_i < \rho_{f_{s+1}} \quad \text{for} \quad f_s \geqq i > f_{s+1}$$
$$\text{and} \quad s < r, \quad \rho_{f_r} = \rho_i \leqq \rho_0 \quad \text{for} \quad f_r \geqq i \geqq 1.$$

We denote by HW$(X)_{nilp}$ *the nilpotent part of* HW(X) *at p. Then the normal form of* HW$(X)_{nilp}$ *becomes the matrix*

$$\begin{pmatrix} \Lambda(1) & & & & & & \\ & \Lambda(2) & & & & 0 & \\ & & \ddots & & & & \\ & & & \Lambda(\rho_{f_r}) & & & \\ & & & & 0 & & \\ & & & & & 0 & \\ & 0 & & & & & \ddots \\ & & & & & & 0 \end{pmatrix} \left.\vphantom{\begin{matrix} 0\\0\\0\\0 \end{matrix}}\right\} \rho_0 - \rho_{f_r}$$

with $\Lambda(\rho)=\Lambda_{f_\alpha+1}$ for $\rho_{f_{\alpha-1}}<\rho\leqq\rho_{f_\alpha}$, $\alpha=0, 1,\ldots, r$, where $\rho_{f_{-1}}=0$, and each

Λ_g *is the square matrix* (λ_{ij}) *of size* g *given by* $\lambda_{ij}=1$ *if* $j=i+1$ *and* $\lambda_{ij}=0$ *otherwise* (cf. §2).

THEOREM II. *Let positive integers* n, d *and* p *be as above.*

1) *We have the property: if* $p\equiv -1 \pmod d$ *then* $\mathrm{HW}(X)$ *at* p *is the zero matrix.*

2) *In case of* $n=1$ *i.e.* X: $x_0^d+x_1^d+x_2^d=0$, *we have moreover the property: if* $\mathrm{HW}(X)$ *at* p *is the zero matrix, then* $p\equiv -1 \pmod d$.

3) *In case of* $n=2$ *i.e.* X: $x_0^d+x_1^d+x_2^d+x_3^d=0$,

(i) *when* d *is even, we have moreover the property: if* $\mathrm{HW}(X)$ *at* p *is the zero matrix, then* $p\equiv -1 \pmod d$,

(ii) *when* d *is odd, we have the property:* $\mathrm{HW}(X)$ *at* p *is the zero matrix if and only if* $p\equiv -1 \pmod d$ *or* $p\equiv -2 \pmod d$ *or* $p\equiv (d-1)/2 \pmod d$ (*cf.* §3).

We should remark that the statement of Th. II, 3), (ii) is suggested by N. Suwa. The first proof of Th. II given by the author has been improved by R. Sasaki later, and the author appreciates him for permitting to write his proof here.

Finally, we observe relations with Newton-polygons of X over the field $\mathbf{F}_{p^f}$, where $f=\mathrm{ord.}\langle p \bmod d\rangle$ in $(\mathbf{Z}/d\mathbf{Z})^\times$ (cf. §4).

The author wish to express his hearty thanks to Prof. M. Nishi and Prof. T. Sekiguchi for their hearty encouragement, and Prof. N. Suwa and Prof. R. Sasaki for their useful conversations.

1. Hasse-Witt matrices HW (X)

Let n, d and p be the positive integers such that p is a prime number with $p\nmid d$ and $d\geqq n+2$. We now consider the Fermat variety X defined by

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

We put $h=x_0^d+x_1^d+\cdots+x_{n+1}^d$, and $k=\overline{\mathbf{F}}_p$. From a commutative diagram of short exact sequences of structure-sheaves:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathcal{O}_{\mathbf{P}^{n+1}}(-d) & \xrightarrow{h} & \mathcal{O}_{\mathbf{P}^{n+1}} & \longrightarrow & \mathcal{O}_X & \longrightarrow & 0 \\ & & {\scriptstyle h^{p-1}F}\downarrow & & {\scriptstyle F}\downarrow & & {\scriptstyle F}\downarrow & & \\ 0 & \longrightarrow & \mathcal{O}_{\mathbf{P}^{n+1}}(-d) & \xrightarrow{h} & \mathcal{O}_{\mathbf{P}^{n+1}} & \longrightarrow & \mathcal{O}_X & \longrightarrow & 0, \end{array}$$

we have a commutative diagram of cohomology groups:

$$\begin{array}{ccc} H^n(X, \mathcal{O}_X) & \overset{\delta}{\xrightarrow{\sim}} & H^{n+1}(\mathbf{P}^{n+1}, \mathcal{O}_{\mathbf{P}^{n+1}}(-d)) \\ {\scriptstyle F}\downarrow & & {\scriptstyle G_h}\downarrow \\ H^n(X, \mathcal{O}_X) & \overset{\delta}{\xrightarrow{\sim}} & H^{n+1}(\mathbf{P}^{n+1}, \mathcal{O}_{\mathbf{P}^{n+1}}(-d)), \end{array}$$

where G_h denotes $h^{p-1}F$ and δ denotes the connecting morphism in the long exact sequence derived from the above short exact sequence (cf. Serre [2], Chap. III, 3, Prop. 8).

Now we put

$$\mathscr{W}_0 = \{w=(w_0, w_1,\dots, w_{n+1})\in \mathbf{Z}_+^{n+2} \mid 0<w_\gamma \text{ for all } \gamma=0,\dots, n+1, |w|=d\},$$

where $\mathbf{Z}_+$ is the set of all non-negative integers and $|w|=\sum_{\gamma=0}^{n+1} w_\gamma$. We note that $\#\mathscr{W}_0=\binom{d-1}{n+1}$, where $\#$ denotes the cardinality. According to Serre [2], loc. cit., we know that the k-vector space $H^{n+1}(\mathbf{P}^{n+1}, \mathcal{O}_{\mathbf{P}^{n+1}}(-d))$ is $\binom{d-1}{n+1}$ -dimensional and has a basis consisting of the classes of sections

$$f_{0,1,\dots,n+1}^{(\beta)} = 1/(x_0^{\beta_0}x_1^{\beta_1}\cdots x_{n+1}^{\beta_{n+1}}) \quad \text{with} \quad \beta = (\beta_0, \beta_1,\dots, \beta_{n+1})\in \mathscr{W}_0,$$

on $U_{0,1,\dots,n+1}(x_0x_1\cdots x_{n+1}\neq 0)$ of $\mathcal{O}_{\mathbf{P}^{n+1}}(-d)$.

We denotes by $[w]$ the class of $f_{0,1,\dots,n+1}^{(w)}$, and by $\mathrm{HW}(X)$ the matrix of the action G_h with respect to basis $\{[w] \mid w\in \mathscr{W}_0\}$.

Now we shall describe $\mathrm{HW}(X)$. For $v\in \mathscr{W}_0$, we have

$$\begin{aligned} G_h\cdot[v] &= (x_0^d+\cdots+x_{n+1}^d)^{p-1}x^{-pv} \text{ mod coboundaries} \\ &= \textstyle\sum_\lambda ((p-1)!/\lambda!)x^{-(pv-\lambda d)} \text{ mod coboundaries,} \end{aligned}$$

where $\sum$ is taken over all $\lambda=(\lambda_0,\dots, \lambda_{n+1})\in \mathbf{Z}_+^{n+2}$ with $|\lambda|=p-1$. Here, $x=(x_0,\dots, x_{n+1})$, $pv=(pv_0,\dots, pv_{n+1})$, $x^{-\alpha}=x_0^{-\alpha_0}\cdots x_{n+1}^{-\alpha_{n+1}}$ $(\alpha=(\alpha_0,\dots, \alpha_{n+1}))$, $\lambda!=\lambda_0!\cdots\lambda_{n+1}!$ and $\lambda d=(\lambda_0 d,\dots, \lambda_{n+1}d)$.

When we put $A_h(v)=\{\lambda\in \mathbf{Z}_+^{n+2} \mid |\lambda|=p-1,\ pv_\gamma>\lambda_\gamma d \text{ for all } \gamma\}$ and $B_h(v)=\{\lambda\in \mathbf{Z}_+^{n+2} \mid |\lambda|=p-1,\ pv_\gamma<\lambda_\gamma d \text{ for some } \gamma\}$, we have

$$G_h\cdot[v] = \left(\textstyle\sum_{\lambda\in A_h(v)} + \sum_{\lambda\in B_h(v)}\right)((p-1)!/\lambda!)x^{-(pv-\lambda d)},$$

since p is a prime number with $p\nmid d$ by assumption. If $A_h(v)\neq\emptyset$, then it consists of only one element λ and $w=pv-\lambda d\in \mathscr{W}_0$. In fact, $|w|=d$ and each pair $(\lambda_\gamma, w_\gamma)$ is uniquely determined via "euclidean algorithm" dividing pv_γ by d. Let $\lambda\in B_h(v)$. Then $pv_{\gamma_0}<\lambda_{\gamma_0}d$ for some γ_0 and $((p-1)!/\lambda!)x^{-(pv-\lambda d)}=p_{\gamma_0}/(x_0\cdots\check{x}_{\gamma_0}\cdots x_{n+1})^m$ for $m=\max\{pv_\gamma \mid 0\leqq\gamma\leqq n+1\}$ and a homogeneous polynomial p_{γ_0} in $x_0,\dots, x_{n+1}$ of degree $-d+m(n+1)$. This is a section on $U_{0,\dots\check{\gamma}_0\dots,n+1}(x_0\cdots\check{x}_{\gamma_0}\cdots x_{n+1}\neq 0)$ of $\mathcal{O}_{\mathbf{P}^{n+1}}(-d)$. Thus $\sum_{\lambda\in B_h(v)}$ is of the coboundary form of an n-cochain with coefficients in $\mathcal{O}_{\mathbf{P}^{n+1}}(-d)$.

Therefore, for each $v\in \mathscr{W}_0$, we have:

$$(*)\qquad \begin{cases} \text{If } A_h(v)\neq\emptyset, & \text{then } G_h\cdot[v] = ((p-1)!/\lambda!)[w] \quad (pv=\lambda d+w). \\ \text{If } A_h(v)=\emptyset, & \text{then } G_h\cdot[v] = 0. \end{cases}$$

Moreover we put

$$\mathscr{W} = \{w=(w_0,\dots, w_{n+1})\in \mathbf{Z}_+^{n+2} \mid 0<w_\gamma<d\ (0\leqq\gamma\leqq n+1),\ |w|\equiv 0 \pmod d\}.$$

As in Koblitz [1], for a positive integer j, we consider the action $j\cdot$ on $\mathbf{Z}_+^{n+2}$,

$$j\cdot w = (\{jw_0\}_d,\dots, \{jw_{n+1}\}_d)$$

for $w=(w_0,\dots, w_{n+1})$, where each $\{jw_\gamma\}_d$ denotes the remainder for the division of jw_γ by d. Especially, suppose $(j, d)=1$. Then we have $j\cdot : \mathscr{W} \simeq \mathscr{W}$ as sets, and $j\cdot = j'\cdot$ (if $j\equiv j' \pmod d$), $(jj')\cdot = j\cdot(j'\cdot)$ for two positive integers j, j' coprime to d. When, for each $v\in\mathscr{W}_0$, we write

$$G_h\cdot[v] = \textstyle\sum_{w\in\mathscr{W}_0} h_{v,w}[w] \quad (h_{v,w}\in k),$$

we have

$$\mathrm{HW}(X) = (h_{v,w})_{w,v}, \quad w \ \text{ and } \ v\in\mathscr{W}_0.$$

From the above (*), we have

$$(*') \qquad \begin{cases} h_{v,w}\neq 0 & (\text{if } w=p\cdot v), \\ h_{v,w}=0 & (\text{if } w\neq p\cdot v). \end{cases}$$

We note that the statement of this fact appears in Koblitz [1].

Let f be the order of $p \bmod d$ as in the introduction. For $w\in\mathscr{W}_0$, when $p^\alpha\cdot w\in\mathscr{W}_0$ for all $\alpha\in\mathbf{Z}_+$, we say that w is of type infinity. We put

$$S(p) = \{w\in\mathscr{W}_0 \mid w;\ \text{of type infinity}\},$$
$$S^*(p) = \mathscr{W}_0 \smallsetminus S(p).$$

For $w\in\mathscr{W}_0$ and $0\leqq i\leqq f-2$, when $p^\alpha\cdot w\in\mathscr{W}_0$ for any α $(0\leqq\alpha\leqq i)$ and $p^{i+1}\cdot w\notin\mathscr{W}_0$, we say that w is of type i. We put

$$S_i(p) = \{w\in\mathscr{W}_0 \mid w;\ \text{of type } i\}.$$

Then we have disjoint unions

$$S^*(p) = \cup_{i=0}^{f-2} S_i(p), \quad \mathscr{W}_0 = S(p) \cup S_0(p) \cup\cdots\cup S_{f-2}(p),$$

a bijection $p\cdot : S(p)\simeq S(p)$, and injections $p\cdot : S^*(p)\smallsetminus S_0(p)\to S^*(p)$, $p\cdot : S_0(p)\to \mathscr{W}\smallsetminus\mathscr{W}_0$ as sets.

Thus, as for $\mathrm{HW}(X)$ at p, we obtain

a) $\mathrm{HW}(X)$ is a square matrix of size $\binom{d-1}{n+1}=\sharp\mathscr{W}_0$ and consists of three minors (i), (ii), (iii):

(i) $(h_{v,w})_{(w,v)\in\mathscr{W}_0\times S(p)}$ of rank $\sharp S(p)$,

(ii) $(h_{v,w})_{(w,v)\in\mathscr{W}_0\times(S^*(p)\setminus S_0(p))}$ of rank $\sharp(S^*(p)\setminus S_0(p))$,

(iii) $(h_{v,w})_{(w,v)\in\mathscr{W}_0\times S_0(p)}$ of rank zero.

Each v^{th} column of these minors is such a type of vectors with only non-zero component at $w=p\cdot v$.

b) $\operatorname{rank} \mathrm{HW}(X) = \sharp S(p) + \sharp(S^*(p)\setminus S_0(p))$.

c) $\mathrm{HW}(X)$ is the zero matrix iff $\mathscr{W}_0=S_0(p)$.

When we put

$$\mathrm{HW}(X)_{ss} = (h_{v,w})_{w,v};\quad w \quad\text{and}\quad v\in S(p),$$

$$\mathrm{HW}(X)_{nilp} = (h_{v,w})_{w,v};\quad w \quad\text{and}\quad v\in S^*(p),$$

we see that $\mathrm{HW}(X)_{ss}$ is non-singular, and $\mathrm{HW}(X)_{nilp}$ is of the form $(*\,|\,0)$, where 0 means $\sharp\mathscr{W}_0\times\sharp S_0(p)$-matrix, with rank $\sharp(S^*(p)\setminus S_0(p))$ and

$$\mathrm{HW}(X) = \begin{pmatrix} \mathrm{HW}(X)_{ss} & 0 \\ 0 & \mathrm{HW}(X)_{nilp} \end{pmatrix}$$

In later sections, we let $[\mathscr{W}_0]$ stand for $H^{n+1}(\mathbf{P}^{n+1}, \mathcal{O}_{\mathbf{P}^{n+1}}(-d))$ and $[S]$ the subspace of $[\mathscr{W}_0]$ generated by a subset S of $[\mathscr{W}_0]$.

2. The normal form of HW (X)

G_h is a p-th power semilinear endomorphism of $[\mathscr{W}_0]$. And, by $(*')$, for every $v\in\mathscr{W}_0$ and for any integer $N>0$, we have

$$(**)\qquad G_h^N\cdot[v] = (h_{v,p\cdot v})^{p^{N-1}}(h_{p\cdot v,p^2\cdot v})^{p^{N-2}}\cdots(h_{p^{N-1}\cdot v,p^N\cdot v})\,[p^N\cdot v],$$

where if $p\cdot w\notin\mathscr{W}_0$ then $h_{w,p\cdot w}$ means the zero.

PROPOSITION 2.1. *G_h acts bijectively on $[S(p)]$, nilpotently on $[S^*(p)]$. Moreover we have*

i) $[\mathscr{W}_0] = [S(p)]\oplus[S^*(p)]$ *as G_h-modules*;

ii) $[S(p)] = \bigcap_{N\in\mathbf{Z}_+} G_h^N\cdot[\mathscr{W}_0]$,
$[S^*(p)] = \bigcup_{N\in\mathbf{Z}_+}\operatorname{Ker}(G^N_{h|[\mathscr{W}_0]})$.

PROOF. For any $v\in S(p)$, we have $v=p\cdot w$ for some w by $p\cdot : S(p)\simeq S(p)$. Put $c=(h_{w,p\cdot w})^{-p^{-1}}\in k$. Then $[v]=G_h\cdot(c[w])$ by $(**)$. Hence $[S(p)]\subset G_h\cdot[S(p)]$. On the other hand, since $G_h\cdot[S(p)]\subset[S(p)]$, we have $G_h\cdot[S(p)]=[S(p)]$. And we also see that $\operatorname{Ker}(G_{h|[S(p)]})=0$ via $p.: S(p)\simeq S(p)$. By $(**)$, G_h acts nilpotently on $S^*(p)$ and hence on $[S^*(p)]$. From the disjoint union

$\mathscr{W}_0=S(p)\cup S^*(p)$, $G_h\cdot[S(p)]=[S(p)]$ and $G_h\cdot[S^*(p)]\subset[S^*(p)]$, the assertion i) follows. Since G_h acts bijectly on $[S(p)]$ (resp. nilpotently on $[S^*(p)]$), we have $[S(p)]\subset\bigcap_{N\in\mathbf{Z}_+}G_h^N\cdot[\mathscr{W}_0]$ (resp. $[S^*(p)]\subset\bigcup_{N\in\mathbf{Z}_+}\operatorname{Ker}(G^N_{h|[\mathscr{W}_0]})$. For an element $\xi\in(\bigcap_{N\in\mathbf{Z}_+}G_h^N\cdot[\mathscr{W}_0])\cap(\bigcup_{N\in\mathbf{Z}_+}\operatorname{Ker}(G^N_{h|[\mathscr{W}_0]}))$, we write

$$\xi=\sum_{v\in S(p)}c_v[v]+\sum_{w\in S^*(p)}d_w[w]\quad(c_v,\ d_w\in k).$$

Then, since $\xi\in\bigcup_{N\in\mathbf{Z}_+}\operatorname{Ker}(G^N_{h|[\mathscr{W}_0]})$, we have $G_h^N\cdot\xi=0$ for sufficiently large N and hence

$$\sum_{v\in S(p)}c_v^{p^N}s[p^N\cdot v]=0\quad\text{for some}\quad s\in k^\times.$$

Then

$$\xi=\sum_{w\in S^*(p)}d_w[w]\in\bigcap_{N\in\mathbf{Z}_+}G_h^N\cdot[\mathscr{W}_0].$$

Therefore, by i), $\xi\in[S(p)]$ and then $\xi=0$. Thus we have

$$[\mathscr{W}_0]=[S(p)]\oplus[S^*(p)]=(\bigcap_{N\in\mathbf{Z}_+}G_h^N\cdot[\mathscr{W}_0])\oplus(\bigcup_{N\in\mathbf{Z}_+}\operatorname{Ker}(G^h_{N|[\mathscr{W}_0]})).$$

Since $[S(p)]\subset\bigcap_{N\in\mathbf{Z}_+}G_h^N\cdot[\mathscr{W}_0]$ and $[S^*(p)]\subset\bigcup_{N\in\mathbf{Z}_+}\operatorname{Ker}(G^N_{h|[\mathscr{W}_0]})$, the assertion ii) holds. Q.E.D.

On the other hand, we denote by $[\mathscr{W}_0]^{G_h}$ the subspace of $[\mathscr{W}_0]$ generated by all G_h-fixed vectors and denote by $[\mathscr{W}_0]_{G_h-nilp}$ the subspace of $[\mathscr{W}_0]$ consisting of all vectors which are killed by powers of G_h. Then we have

$$[\mathscr{W}_0]=[\mathscr{W}_0]^{G_h}\oplus[\mathscr{W}_0]_{G_h-nilp}.$$

Since $[S^*(p)]=[\mathscr{W}_0]_{G_h-nilp}$ and $\bigcap_{N\in\mathbf{Z}_+}G_h^N\cdot[\mathscr{W}_0]\supset[\mathscr{W}_0]^{G_h}$, we have $[\mathscr{W}_0]^{G_h}=[S(p)]$. It is known that $[\mathscr{W}_0]^{G_n}$ has as basis G_h-fixed vectors: e_ν's, $\nu=1,2,\dots,\#S(p)$. Then, with respect to the e_ν's, the normal form of $\mathrm{HW}(X)_{ss}$ at p becomes the unit matrix $\mathbf{1}_\sigma$ of size $\sigma=\#S(p)$.

Now, when $S^*(p)$ is non-empty, we shall choose a basis of $[S^*(p)]$ for the sake of describing the normal form of $\mathrm{HW}(X)_{nilp}$. At first we note that if $S_0(p)=\emptyset$, then $S^*(p)=\emptyset$; and if $S_0(p)\neq\emptyset$, then $f\geqq 2$. In fact, suppose $S^*(p)\neq\emptyset$. Then take $w\in S^*(p)$. Since w is of type i for some i, we have $p^i\cdot w\in S_0(p)$. Suppose $f=1$. Then, since $\mathscr{W}_0=S(p)$, we have $S^*(p)=\emptyset$.

Therefore $S^*(p)$ has a unique non-negative integer $f_0\leqq f-2$ such that $S_i(p)=\emptyset$ for every $i>f_0$ and $\emptyset\neq S_{f_0}(p)\xrightarrow[p\cdot]{}\cdots\xrightarrow[p\cdot]{}S_1(p)\xrightarrow[p\cdot]{}S_0(p)$.
We put

$$\rho_i=\#S_i(p),\quad\text{and}\quad[S^*(p)]^{(i)}=\operatorname{Ker}(G^i_{h|[\mathscr{W}_0]}).$$

PROPOSITION 2.2. *We have the following properties*:

i) $\rho_i\geqq\rho_{i+1}$ *for* $0\leqq i\leqq f_0$ *and* $\rho_\alpha=0$ *for* $\alpha>f_0$.

ii) $[S^*(p)]^{(f_0+1)} = [S^*(p)]$, $[S^*(p)]^{(1)} = [S_0(p)]$.

iii) $G_h\colon [S_i(p)] \longrightarrow [S_{i-1}(p)]$ *is injective for* $i \geqq 1$.

iv) $[S^*(p)]^{(i)} \cap [S_i(p)] = \{0\}$ *for* $i \geqq 0$.

v) $[S^*(p)]^{(i+1)} = [S^*(p)]^{(i)} \oplus [S_i(p)]$ *for* $i \geqq 0$.

And the G_h-action has a commutative diagram:

$$\begin{array}{ccc} [S^*(p)]^{(i+1)} & = [S^*(p)]^{(i)} \oplus & [S_i(p)] \\ {\scriptstyle G_h}\big\downarrow & & {\scriptstyle G_h}\big\downarrow \\ [S^*(p)]^{(i)} & = [S^*(p)]^{(i-1)} \oplus & [S_{i-1}(p)]. \end{array}$$

PROOF. The assertion i) is obvious. We prove the assertion ii). From the definition of f_0, we have $G^{f_0+1}\cdot[v]=0$ for all $v\in S^*(p)$. Therefore $[S^*(p)]^{(f_0+1)} \supset [S^*(p)]$ and hence the equality holds. We have $[S^*(p)]^{(1)}\supset[S_0(p)]$ by (**). Let $\xi\in[\mathscr{W}_0]$ be such an element that $G_h\cdot\xi=0$. Then we can write

$$\xi = \textstyle\sum_{w\in S^*(p)} d_w[w], \quad d_w\in k$$

by Prop. 2.1, and also we can write

$$\xi = \textstyle\sum_{0\leqq i\leqq f_0}(\sum_{w\in S_i(p)} d_w[w]).$$

Hence we have

$$G_h\cdot\xi = \textstyle\sum_{i\geqq 1}(\sum_{w\in S_i(p)} d_w^p h_{w,p\cdot w}[p\cdot w]) = 0.$$

Since the $S_i(p)$'s are disjoint to each other, we have $d_w=0$ for $w\notin S_0(p)$ and hence $\xi\in S_0(p)$. Thus the assertion ii) holds.

Since $G_h\cdot(\sum_{w\in S_i(p)} d_w[w])=\sum_{w\in S_i(p)} d_w^p h_{w,p\cdot w}[p\cdot w]$ and the $p\cdot w$'s are distinct to each other in $S_{i-1}(p)$, if the right hand side is zero then we have $d_w=0$ for $w\in S_i(p)$. Hence the assertion iii) holds.

Suppose $G_h^i\cdot(\sum_{w\in S_i(p)} d_w[w])=0$. By (**), the left hand side is equal to

$$\textstyle\sum_{w\in S_i(p)} d_w^{p^i}(h_{w,p\cdot w})^{p^{i-1}}\cdots(h_{p^{i-1}\cdot w,p^i\cdot w})[p^i\cdot w].$$

Since $w, p\cdot w,\ldots, p^i\cdot w$ ($w\in S_i(p)$) are all contained in $\mathscr{W}_0$ and are distinct to each other, we have $d_w=0$ for $w\in S_i(p)$. Hence the assertion iv) holds. Obviously $[S^*(p)]^{(i+1)}\supset[S^*(p)]^{(i)}$, and $[S^*(p)]^{(i+1)}\supset[S_i(p)]$. Conversely let $\xi\in[\mathscr{W}_0]$ be in $[S^*(p)]^{(i+1)}$. When we write

$$\xi = \textstyle\sum_j \sum_{v\in S_j(p)} c_v^{(j)}[v],$$

we have $G_h^{i+1}\cdot[\sum_{j\geqq i+1}]=0$. By iii) and (**), we have $c_v^{(j)}=0$ for $j\geqq i+1$. Then, since the sum $\sum_{j<i}$ in ξ is in $[S^*(p)]^{(i)}$, we have $\xi\in[S^*(p)]^{(i)}+[S_i(p)]$.

The commutativity with the G_h-action is obvious. Thus the assertion v) holds.

Q.E.D.

Now we have Th. I in the introduction.

THEOREM 2.3. *For positive integers n, d and p (p: prime number with $p \nmid d$ and $d \geqq n+2$) given as above, we let ρ_i be the number of all elements in $\mathscr{W}_0$ of type i defined in* §1. *We arrange the ρ_i's as in Theorem* I *in the introduction. Then, with respect to the basis:*

$$\begin{cases} G_h^{N_\alpha} \cdot [v_\alpha] \ (\alpha=0, 1, \dots, r;\ N_\alpha = f_\alpha, f_\alpha - 1, \dots, 0; \\ \quad v_0 \in S_{f_0}(p),\ v_\alpha \in S_{f_\alpha}(p) \setminus p^{f_{\alpha-1}-f_\alpha} \cdot S_{f_{\alpha-1}}(p) \ for\ \alpha \geqq 1), \\ \quad [w] \ (w \in S_0(p) \setminus p^{f_r} \cdot S_{f_r}(p)), \end{cases}$$

$\mathrm{HW}(X)_{nilp}$ *at p is of the form:*

$$\left(\begin{array}{cccccc} \Lambda(1) & & & & & \\ & \Lambda(2) & & & 0 & \\ & & \ddots & & & \\ & & & \Lambda(\rho_{f_r}) & & \\ & & & & 0 & \\ & 0 & & & 0 & \\ & & & & \ddots & \\ & & & & & 0 \end{array}\right) \Big\} \rho_0 - \rho_{f_r}$$

with $\Lambda(\rho) = \Lambda_{f_\alpha+1}$ for $\rho_{f_{\alpha-1}} < \rho \leqq \rho_{f_\alpha}$, $\alpha = 0, 1, \dots, r$, where $\rho_{f_{-1}} = 0$, and each $\Lambda_g = (\lambda_{ij})_{1 \leqq i,j \leqq g}$, $\lambda_{ij} = 1$ $(j = i+1)$, $\lambda_{ij} = 0$ (otherwise), for all g.

PROOF. If $p \cdot v \in \mathscr{W}_0$, then $G_h \cdot [v]$ is an non-zero constant multiplication of $[p \cdot v]$ by (**). Moreover G_h is injective on $[S^*(p) \setminus S_0(p)]$ by Prop. 2.2. The symbol [ ] is a "one-to-one" map from $\mathscr{W}_0$ to $[\mathscr{W}_0]$.

Now, when we omit constant multiplications and the symbol [ ] in the above arrangement of vectors, we obtain the following list:

$$\begin{aligned} & S_0(p) \\ & = \{p^{f_0} \cdot v \mid v \in S_{f_0}(p)\} \cup \left(\bigcup_{1 \leqq i \leqq r+1} \{p^{f_i} \cdot v \mid v \in S_{f_i}(p) \setminus p^{f_{i-1}-f_i} \cdot S_{f_{i-1}}(p)\}\right), \end{aligned}$$

where $f_{r+1} = 0$,

$$\begin{aligned} & S_{f_m - \alpha_m}(p) \\ & = \{p^{f_0 - f_m + \alpha_m} \cdot v \mid v \in S_{f_0}(p)\} \cup \left(\bigcup_{1 \leqq i \leqq m} \{p^{f_i - f_m + \alpha_m} \cdot v \mid \right. \\ & \qquad \left. v \in S_{f_i}(p) \setminus p^{f_{i-1}-f_i} \cdot S_{f_{i-1}}(p)\}\right) \end{aligned}$$

$(\alpha_m = 0, 1, \dots, f_m - f_{m+1} - 1;\ m = 1, 2, \dots, r)$,

$$S_{f_0-\alpha_0}(p) \\ = \{p^{\alpha_0}\cdot v \mid v\in S_{f_0}(p)\} \quad (\alpha_0=0, 1,\dots, f_0-f_1-1).$$

We note that

$$(f_0+1)\rho_{f_0} + \textstyle\sum_{i=1}^{r}(\rho_{f_i}-\rho_{f_{i-1}})(f_i+1) + (\rho_0-\rho_{f_r}) \\ = \textstyle\sum_{i=0}^{r-1}\rho_{f_i}(f_i-f_{i+1}) + \rho_{f_r}f_r + \rho_0 = \sum_{\alpha=0}^{f_0}\rho_\alpha = \sharp S^*(p).$$

Through this list, we get the above basis of $[S^*(p)]$. It is easily seen that, with respect to these basis, the normal form of HW $(X)_{nilp}$ is as above. Q. E. D.

EXAMPLE 2.4 ($n=1$ or 2; $d=13$). Let $p=41\equiv 2 \pmod{13}$, and hence $f=12$. In the following lists, ". ." denotes other permutations of the first one.

i) ($n=1$ case): $\sharp\mathscr{W}_0=\binom{d-1}{n+1}=66.$

$\mathscr{W}_0 = S^*(p)$

$= S_0(p)$ ∪	$S_1(p)$ ∪	$S_2(p)$ ∪	$S_3(p)$ ∪	$S_4(p)$ ∪	$S_5(p)$
(4, 4, 5). .	(2, 2, 9). .	(1, 1, 11). .	(2, 4, 7). .	(1, 2, 10). .	(1, 5, 7). .
(5, 5, 3). .	(3, 3, 7). .	(1, 4, 8). .			
(6, 6, 1). .	(1, 3, 9). .				
(2, 5, 6). .	(2, 3, 8). .				
(3, 4, 6). . .					

Hence

$$6=\rho_5=\rho_4=\rho_3<9=\rho_2<18=\rho_1<21=\rho_0;$$

$$f_0=5>f_1=2>f_2=1 \quad (r=2).$$

$S_5(p)$	$S_2(p)\smallsetminus p^3\cdot S_5(p)$	$S_1(p)\smallsetminus p\cdot S_2(p)$	$S_0(p)\smallsetminus p\cdot S_1(p)$
v: (1, 5, 7). .	(1, 1, 11). .	(3, 3, 7). .	w: (5, 5, 3). .
		(1, 3, 9). . .	

Hence $\mathrm{HW}(X)=\mathrm{HW}(X)_{nilp}$, and it has the normal form:

$$\underbrace{\Lambda_6,\dots,\Lambda_6}_{\rho_5=6};\ \underbrace{\Lambda_3,\dots,\Lambda_3}_{\rho_2-\rho_5=3};\ \underbrace{\Lambda_2,\dots,\Lambda_2}_{\rho_1-\rho_2=9};\ \underbrace{0,\dots,0}_{\rho_0-\rho_1=3}.$$

ii) ($n=2$ case): $\sharp\mathscr{W}_0=\binom{d-1}{n+1}=220.$

$$\mathscr{W}_0 = S^*(p) = S_0(p) \cup S_1(p) \cup S_2(p)$$

$S_0(p)$	$S_1(p)$	$S_2(p)$
(4, 4, 4, 1)..	(2, 2, 2, 7)..	(1, 1, 1, 10)..
(3, 3, 3, 4)..	(1, 1, 2, 9)..	(1, 1, 4, 7)..
(2, 2, 4, 5)..	(1, 1, 3, 8)..	
(3, 3, 6, 1)..	(2, 2, 8, 1)..	
(2, 2, 6, 3)..	(1, 2, 3, 7)..	
(5, 5, 2, 1)..		
(4, 4, 3, 2)..		
(1, 1, 5, 6)..		
(3, 3, 2, 5)..		
(2, 4, 6, 1)..		
(1, 3, 4, 5)...		

Hence $16=\rho_2<64=\rho_1<140=\rho_0$; $f_0=2>f_1=1$ $(r=1)$.

$S_2(p)$	$S_1(p)\smallsetminus p\cdot S_2(p)$	$S_0(p)\smallsetminus p\cdot S_1(p)$
v: (1, 1, 1, 10)..	(1, 1, 2, 9)..	w: (3, 3, 3, 4)..
(1, 1, 4, 7)..	(1, 1, 3, 8)..	(3, 3, 6, 1)..
	(1, 2, 3, 7)..	(5, 5, 2, 1)..
		(1, 1, 5, 6)..
		(3, 3, 2, 5)..
		(1, 3, 4, 5)...

Hence $\mathrm{HW}(X)=\mathrm{HW}(X)_{nilp}$, and the normal form is as follows:

$$\underbrace{\Lambda_3,\dots,\Lambda_3}_{\rho_2=16};\quad \underbrace{\Lambda_2,\dots,\Lambda_2}_{\rho_1-\rho_2=48};\quad \underbrace{0,\dots,0}_{\rho_0-\rho_1=76}.$$

3. Nullity conditions for HW (X) in case of n = 1 and 2

We start with the following lemma:

LEMMA 3.1. *Let X be the Fermat variety of dimension n defined by*

$$x_0^d + x_1^d + \cdots + x_{n+1}^d = 0 \quad (d \geqq n+2),$$

and let p be a prime number not dividing d. Then we have the following:

i) *If* $d-n \leqq \{p\}_d \leqq d-1$, *then* HW (X) *at* p *is zero.*

ii) *Assume* d *is even. If* $d/2-(n-1-[n/2]) \leqq \{p\}_d \leqq d/2-1$, *then* HW (X) *at* p *is zero.*

iii) *Assume* d *is odd. If*

$$(d-1)/2 - (n-1-[(n+1)/2]) \leqq \{p\}_d \leqq (d-1)/2,$$

then HW (X) *at* p *is zero.*

Here, as usual, $[r]$ *is the largest integer* $\leqq r$.

PROOF. i) Let $w=(w_0,\dots, w_{n+1}) \in \mathscr{W}_0$. Then for $1 \leqq j \leqq n$, $\{p\}_d = d-j$:

$$(-j)\cdot w = (\{-jw_0\}_d,\dots, \{-jw_{n+1}\}_d).$$

Let α_i, $0 \leqq i \leqq n+1$, be the positive integer such that

$$\alpha_i d > jw_i > (\alpha_i - 1)d.$$

Then we have

$$(-j)\cdot w = (\alpha_0 d - jw_0,\dots, \alpha_{n+1} d - jw_{n+1})$$

and $\sum_{i=0}^{n+1} (\alpha_i d - jw_i) \geqq (n+2)d - j \sum_{i=0}^{n+1} w_i = d(n+2-j) \geqq 2d$. This means that none of $(-j)\cdot w$, $1 \leqq j \leqq n$, is contained in $\mathscr{W}_0$.

ii) Let $w=(w_0,\dots, w_{n+1}) \in \mathscr{W}_0$. Then for $1 \leqq k \leqq n-1-[n/2]$, $\{p\}_d = d/2-k$: $(d/2-k)\cdot w = (\{(d/2-k)w_0\}_d,\dots, \{(d/2-k)w_{n+1}\}_d)$. We may assume that

$$w_0,\dots, w_{2\ell-1} \text{ are odd } (2\ell-1 \leqq n+1, \text{ i.e., } \ell-1 \leqq [n/2]),$$
$$w_{2\ell},\dots, w_{n+1} \text{ are even.}$$

It follows that

$$(d/2-k)w_i \equiv d/2 - kw_i \pmod d \quad (0 \leqq i \leqq 2\ell-1),$$
$$(d/2-k)w_j \equiv - kw_j \pmod d \quad (2\ell \leqq j \leqq n+1).$$

Let α_i, α_j be non-negative integers such that

$$d > \alpha_i d + d/2 - kw_i > 0 \quad (0 \leqq i \leqq 2\ell-1),$$
$$d > (\alpha_j+1)d - kw_j > 0 \quad (2\ell \leqq j \leqq n+1).$$

Then we have

$$(d/2-k)\cdot w = (\dots, (\alpha_i+1/2)d - kw_i,\dots, (\alpha_j+1)d - kw_j,\dots)$$

and

$$\sum_{i=1}^{2\ell-1}(\alpha_i+1/2)d - k\sum_{i=0}^{2\ell-1} w_i + \sum_{j=2\ell}^{n+1}(\alpha_j+1)d - k\sum_{j=2\ell}^{n+1} w_j$$
$$\geqq ((1/2)2\ell+n+1-2\ell+1-k)d = (n+2-(k+\ell))d \geqq 2d.$$

Thus we see that $(d/2-k)\cdot w$ is not in $\mathscr{W}_0$.

iii) The similar proof to ii) works. So we omit it. Q. E. D.

THEOREM 3.2 ($n=1$ *case*). *Let* X *be the Fermat curve defined by* $x_0^d+x_1^d+x_2^d=0$ $(d\geqq 3)$, *and* $p\nmid d$ (p: *prime number*). *Then we see that* HW (X) *at* p *is the zero matrix if and only if* $p\equiv -1 \pmod d$.

PROOF. We shall prove the "only if" part, because the "if" part is already proved.

Let j be the smallest positive integer satisfying $j\equiv p \pmod d$. Assume $1\leqq j\leqq d/2$. Since $(d-2)j\equiv -2j\equiv d-2j \pmod d$, both $w=(1, 1, d-2)$ and $j\cdot w=(j, j, \{(d-2)j\}_d)=(j, j, d-2j)$ are contained in $\mathscr{W}_0$. Assume $d/2<j<d-1$. Since $d/2>[d/(d-j)]$, we get $d-2[d/(d-j)]>0$; hence

$$w = ([d/(d-j)], [d/(d-j)], d-2[d/(d-j)])\in\mathscr{W}_0 .$$

We shall show that

$$j\cdot w = (\{j[d/(d-j)]\}_d, \{j[d/(d-j)]\}_d, \{j(d-2[d/(d-j)])\}_d)$$

is contained in $\mathscr{W}_0$. Since $j[d/(d-j)]\equiv d-(d-j)[d/(d-j)] \pmod d$ and $d>d-(d-j)[d/(d-j)]>0$, we have

$$\{j[d/(d-j)]\}_d = d - (d-j)[d/(d-j)] .$$

Moreover we get

$$[d/(d-j)] > d/(d-j) - 1 > d/2(d-j), \quad 2d > 2(d-j)[d/(d-j)] > d$$

and

$$j(d-2[d/(d-j)]) \equiv -2j[d/(d-j)] \equiv 2(d-j)[d/(d-j)] \pmod d .$$

Thus we have

$$\{j(d-2[d/(d-j)])\}_d = 2(d-j)[d/(d-j)] - d;$$

hence we see $j\cdot w\in\mathscr{W}_0$. Q. E. D.

THEOREM 3.3 ($n=2$ *case*). *Let* X *be the Fermat surface defined by* $x_0^d+x_1^d+x_2^d+x_3^d=0$ $(d\geqq 4)$, $p\nmid d$ (p: *prime number*). *Then we see that* HW (X) *at* p *is the zero matrix if and only if* $p\equiv -1$ *or* -2 *or* $(d-1)/2 \pmod d$.

PROOF. By the same reason as in the proof of Th. 3.2, we shall only prove the "only if" part. It is sufficient to show that there exists $w \in \mathscr{W}$ such that both of w and $p \cdot w$ are contained in $\mathscr{W}_0$. As before, let $j = \{p\}_d$.

The proof will be divided into 4 cases plus an exceptional case (5):

(1) $1 \leqq j < d/3$. Let $w = (1, 1, 1, d-3)$; then w and $j \cdot w = (j, j, j, d-3j)$ are contained in $\mathscr{W}_0$.

(2) $d/3 < j < (d-1)/2$. Since $j \leqq (d-1)/2 - 1 = (d-3)/2$ and $d - 2j \geqq 3$, we get

$$j/(d-2j) \leqq (d-3)/2(d-2j) \leqq (d-3)/6.$$

If $d-2j$ divides j, we have $j = (d-1)/2$ by an easy calculation which contradicts the condition on j; hence we get

$$[j/(d-2j)] < (d-3)/6.$$

Therefore we see that

$w = (2[j/(d-2j)]+1,\ 2[j/(d-2j)]+1,\ 2[j/(d-2j)]+1,\ d-6[j/(d-2j)]-3)$ is contained in $\mathscr{W}_0$. Now we shall show $j \cdot w \in \mathscr{W}_0$. Since $2j > (2/3)d$, i.e., $d/3 > d-2j$, we have

$$j/(d-2j) - (j-(d/3))/(d-2j) = d/(3(d-2j)) > 1;$$

hence

$$j - (d/3) < [j/(d-2j)](d-2j).$$

If we put $A = j(2[j/(d-2j)]+1) - [j/(d-2j)]d$, then we have

$$A \equiv j(2[j/(d-2j)]+1) \pmod d \quad \text{and} \quad 0 < A < d/3.$$

Since $j \cdot w = (A, A, A, \{j(d-6[j/(d-2j)]-3)\}_d)$ and $3A < d$, we see $j \cdot w \in \mathscr{W}_0$.

(3) $d/2 < j < (2/3)d$. In this case we assume $d > 6$. The cases $d \leqq 6$ are proved trivially. Put $w = (2, 2, 2, d-6)$. Then we see $j \cdot w \in \mathscr{W}_0$. For we have $d < 2j < (4/3)d$; hence

$$2j \equiv 2j - d \pmod d \quad \text{and} \quad d > 2j - d > 0.$$

Since $-3d > -6j > -4d$, we get $d > -6j + 4d > 0$ and $(d-6)j \equiv -6j + 4d \pmod d$.

(4) $(2/3)d < j < d-2$ (assume $d > 6$). Since $d \geqq (3d)/(d-j) > 3[d/(d-j)]$, we have $w = ([d/(d-j)],\ [d/(d-j)],\ [d/(d-j)],\ d-3[d/(d-j)])$ is contained in $\mathscr{W}_0$. Moreover we get

$$j[d/(d-j)] \equiv d - (d-j)[d/(d-j)] \pmod d,$$

$$d > d - (d-j)[d/(d-j)] > 0 \quad \text{and}$$

$$j(d-3[d/(d-j)]) \equiv 3(d-j)[d/(d-j)] - 2d \pmod d.$$

Since $3(d-j)[d/(d-j)]>3(d-j)(d/(d-j)-1)=3d-3(d-j)=3j>2d$, it follows that $j\cdot w$ is contained in $\mathscr{W}_0$.

(5) d: even, and $j=(d/2)-1$. In this case, put $w=(1, 1, (d/2)-1, (d/2)-1)$. Then we have $j\cdot w=((d/2)-1, (d/2)-1, 1, 1)$. Hence both w and $j\cdot w$ are contained in $\mathscr{W}_0$. Q. E. D.

4. Relations with Newton-polygons Nwt (X)

Let n, d, p, f, X be as previous. We put $q=p^f$. In the rational expression

$$P(T)^{(-1)^{n-1}}/(1-T)\cdots(1-q^nT)$$

of the zeta-function $Z(T; X/\mathbf{F}_q)$, we know that

$$P(T)=\prod_w(1-\beta_wT),$$

where w runs over $\mathscr{W}$, and $\beta_w\in\mathbf{Q}(\zeta)$ $(\zeta=\exp(2\pi(-1)^{1/2}/d))$ and that the P-adic value $v_{\mathfrak{P}}(\beta_w)$ of β_w is given by the so-called Stickelberger's formula

$$v_{\mathfrak{P}}(\beta_w)=((1/d)\textstyle\sum_{i=0}^{f-1}|p^i\cdot w|)-f$$

for $\mathfrak{P}|p$ (cf. Shioda-Katsura [3]).

We now consider the "Newton-polygon" Nwt(X) at p of X, namely, the monotonously increasing sequence of non-negative rational numbers $\lambda(w)=(1/f)\cdot v_{\mathfrak{P}}(\beta_w)$. Let $L(\lambda)$ be the number of times for which the slope λ occurs in this sequence. Then Nwt(X) at p: $\lambda_0<\lambda_1<\lambda_2<\cdots$, where each λ has the multiplicity $L(\lambda)$. Since $|p^i\cdot w|=(\varepsilon(p^i\cdot w)+1)d$, we obviously obtain a formula

$$\lambda(w)=(1/f)\textstyle\sum_{i=0}^{f-1}\varepsilon(p^i\cdot w) \qquad \text{for} \quad w\in\mathscr{W},$$

where $\varepsilon(v)=\alpha$ if $v\in\mathscr{W}_\alpha$.

Now we are concerned with the case of $n=2$.

Proposition 4.1 ($n=2$ *case*: $p\nmid d$, $d\geqq 4$). *As for slopes of* Nwt(X) *at* p, *we have the following*:

i) $\lambda(p^i\cdot w)=\lambda(w)$ *for* $0\leqq i\leqq f-1$, *for every* $w\in\mathscr{W}$.

ii) $\lambda(w)+\lambda((d-1)\cdot w)=2$ *for every* $w\in\mathscr{W}_0$.

iii) *Assume that there exist distinct slopes in* Nwt(X). *Then there exist* $w_0\in\mathscr{W}_0$, $w_1\in\mathscr{W}_1$ *and* $w_2\in\mathscr{W}_2$, *such that* $\lambda(w_0)<1$, $\lambda(w_1)=1$ *and* $\lambda(w_2)>1$ *respectively*.

iv) $\mathrm{Min}\{\lambda(w)\mid w\in\mathscr{W}\}=\mathrm{Min}\{\lambda(w)\mid w\in\mathscr{W}_0\}$.

v) *If* HW(X) *is the zero matrix, then the first slope* λ_0 *of* Nwt(X) *is not less than* $1/2$.

Proof. Put $v=p^{i_0}\cdot w$ for a fixed i_0 with $0\leqq i_0\leqq f-1$. Then

$$\begin{aligned}\textstyle\sum_{i=0}^{f-1} |p^i\cdot v| &= \textstyle\sum_{i=0}^{f-1} |p^{i+i_0}\cdot w| \\ &= \textstyle\sum_{\alpha=i_0}^{f-1}|p^{\alpha}\cdot w| + \sum_{\alpha=f}^{f+i_0-1} |p^{\alpha}\cdot w| \\ &= \textstyle\sum_{j=0}^{f-1} |p^j\cdot w|.\end{aligned}$$

Hence we have i). Next put $w'=(d-1)\cdot w$. Then

$$w' = (d-w_0,\ d-w_1,\ d-w_2,\ d-w_3).$$

We can write

$$p^i(d-w_\gamma) = (p^i-A_i-1)d + (d-\{p^i w_\gamma\}_d),$$

where $p^i w_\gamma = A_i d + \{p^i w_\gamma\}_d$ $(0\leqq A_i<p^i)$ in $\mathbf{Z}_+$. Hence

$$\{p^i(d-w_\gamma)\}_d = d - \{p^i w_\gamma\}_d \quad (\gamma=0,1,2,3).$$

Therefore

$$|p^i\cdot w'| = 4d - |p^i\cdot w|,$$

and hence

$$v_{\mathfrak{P}}(\beta_{w'}) = ((1/d)\textstyle\sum_{i=0}^{f-1}(4d-|p^i\cdot w|)) - f = 2f - v_{\mathfrak{P}}(\beta_w).$$

So we have ii).

We now proceed to iii). Under our assumption, suppose $\lambda(w)\geqq 1$ for all $w\in\mathscr{W}_0$. When, by virtue of the above formula for $\lambda(w)$, we write

$$\lambda(w) = (1/f)(0+(\alpha+\alpha'+\alpha''+\cdots)) \quad \text{with} \quad \alpha, \alpha', \alpha'', \ldots \in \{0, 1, 2\},$$

we have some $\alpha=2$. On the other hand, under our assumption, there exists $w'\in\mathscr{W}_0$ such that $\lambda(w')>1$. In fact, suppose $\lambda(w)=1$ for all $w\in\mathscr{W}_0$. By the isomorphism $(d-1)$: $\mathscr{W}_0 \xrightarrow{\sim} \mathscr{W}_2$, we obtain $\lambda(w)=1$ for all $w\in\mathscr{W}_2$ by ii). Moreover, as for $w\in\mathscr{W}_1$; if $p^i\cdot w\in\mathscr{W}_1$ for all i then $\lambda(w)=1$; if $p^{i_0}\cdot w\in\mathscr{W}_0$ or $\in\mathscr{W}_2$ for some i_0 then $\lambda(w)=1$ by i). Thus $\lambda(w)=1$ for all $w\in\mathscr{W}$. This is contrary to our assumption. For w', let w'' be an element of $\mathscr{W}_2$ corresponding to $\alpha=2$. Then $\lambda(w'')=\lambda(w')>1$. According to ii), $\lambda(w)\leqq 1$ for all $w\in\mathscr{W}_2$. This is a contradiction. Therefore there exists $w\in\mathscr{W}_0$ such that $\lambda(w)<1$ under our assumption. Put $w=(A, A, d-A, d-A)$ with $0<A<d$. Obviously $w\in\mathscr{W}_1$. Put $j=\{p\}_d$. Then $1\leqq j\leqq d-1$ and $(j, d)=1$. We have

$$p\cdot w = (\{jA\}_d, \{jA\}_d, \{j(d-A)\}_d, \{j(d-A)\}_d).$$

Since

$$j(d-A) = (j-B-1)d + (d-\{jA\}_d),$$

where $jA=Bd+\{jA\}_d$ $(0\leqq B<j)$ in $\mathbf{Z}_+$, we have $\{j(d-A)\}_d=d-\{jA\}_d$ and hence $p\cdot w\in\mathscr{W}_1$. Then we have successively $p^i\cdot w\in\mathscr{W}_1$ for $2\leqq i\leqq f-1$, and moreover $\lambda(w)=(1/f)(1+1+\cdots+1)=1$. We can take $w\in\mathscr{W}_0$ such that $\lambda((d-1)\cdot w)>1$ by virtue of ii). Thus the assertion iii) holds.

In the case of all slopes being equal, the assertion iv) trivially holds. In the other case, we put

$$\lambda_0 = \mathrm{Min}\,\{\lambda(w)\,|\,w\in\mathscr{W}\} \quad \text{and} \quad \mu_0 = \mathrm{Min}\,\{\lambda(w)\,|\,w\in\mathscr{W}_0\}\,.$$

Then we have $\mu_0<1$ by iii). Let $w\in\mathscr{W}_1$. If an element of $\mathscr{W}_0$ occures in $\{p\cdot w,\dots, p^{f-1}\cdot w\}$, then $\lambda(w)\geqq\mu_0$. If it is not so, then $\lambda(w)=(1/f)(1+(\alpha+\alpha'+\alpha''+\cdots))$ $(\alpha, \alpha', \alpha'',\dots\geqq 1)$ and hence $\lambda(w)\geqq 1>\mu_0$. Let $w\in\mathscr{W}_2$. Similarly we see $\lambda(w)\geqq\mu_0$. Thus we have $\lambda_0\geqq\mu_0$. On the other hand, from their definitions, we have $\lambda_0\leqq\mu_0$. Thus $\lambda_0=\mu_0$.

Finally we prove v). Using iv), we can easily verify the equivalence of

$$\lambda_0 \geqq 1/2 \quad \text{and} \quad \textstyle\sum_{i=0}^{f-1}|p^i\cdot w| \geqq (3fd)/2 \qquad \text{for all} \quad w\in\mathscr{W}_0\,.$$

When $w\in\mathscr{W}$ is in $\mathscr{W}_\alpha$, we say that w has *of index* α. Assume that $\mathrm{HW}(X)=0$. Then $p\cdot w\notin\mathscr{W}_0$ for all $w\in\mathscr{W}_0$, and hence w, $p\cdot w$, $p^2\cdot w,\dots, p^{f-1}\cdot w$ has the sequence of indices

$$\{0,\ \varepsilon\geqq 1;\ \eta',\ \eta'',\dots,\ (\text{all}\ \geqq 1);\ 0,\ \varepsilon'\geqq 1;,\dots;\ \zeta',\ \zeta'',\dots,\ (\text{all}\ \geqq 1)\}$$

or

$$\{0,\ \varepsilon\geqq 1;\dots;\ 0,\ \varepsilon'\geqq 1;\dots;\ 0,\ \varepsilon''\geqq 1\}\,.$$

When f is even, we have $1\leqq\sharp\{\text{all}\ (0,\ \varepsilon)\}\leqq f/2$. When f is odd, we have $1\leqq \sharp\{\text{all}\ (0,\ \varepsilon)\}\leqq(f-1)/2$. Therefore, if f is even then

$$\textstyle\sum_{i=0}^{f-1}|p^i\cdot w| \geqq (d+2d)(f/2) = (3fd)/2,$$

and if f is odd then

$$\begin{aligned}\textstyle\sum_{i=0}^{f-1}|p^i\cdot w| &\geqq (d+2d)(f-1)/2 + 2d\\ &= (3f+1)d/2 > (3fd)/2.\end{aligned}$$

Thus we have $\lambda_0\geqq 1/2$. Therefore the assertion v) holds. Q. E. D.

When we consider the inverse of v) in the above proposition, it does not hold in case of $n=2$. We have examples as follows.

Example 4.2 ($d=9$ case). At $p\equiv 2\ (\mathrm{mod}\ 9)$, we have $f=6$, $p^{f/2}\equiv -1\ (\mathrm{mod}\ d)$ and $\mathrm{HW}(X)=\mathrm{HW}(X)_{nilp}$. Moreover, the indices: 0 0 1

$$(1, 1, 1, 6) \xrightarrow{p\cdot} (2, 2, 2, 3) \xrightarrow{p\cdot} (4, 4, 4, 6)$$
$$(1, 1, 2, 5) \xrightarrow{p\cdot} (2, 2, 4, 1) \xrightarrow{p\cdot} (4, 4, 8, 2).$$

So, rank $HW(X)=16$ and $Nwt(X)$: $\lambda_0=1$ with $L(\lambda_0)=457$.

EXAMPLE 4.3 ($d=11$ case). At $p\equiv 3 \pmod{11}$, we have $f=5$ and $HW(X)=HW(X)_{nilp}$. Moreover,

the indices: 0 0 1 2

$$(1, 1, 1, 8) \xrightarrow{p\cdot} (3, 3, 3, 2) \qquad\qquad \xrightarrow{p\cdot} (9, 9, 9, 6)$$
$$(4, 4, 1, 2) \xrightarrow{p\cdot} (1, 1, 3, 6) \xrightarrow{p\cdot} (3, 3, 9, 7)$$
$$(1, 1, 4, 5) \xrightarrow{p\cdot} (3, 3, 1, 4) \xrightarrow{p\cdot} (9, 9, 3, 1).$$

So, rank $HW(X)=28$ and

$$\begin{array}{rl} Nwt(X): & \lambda_0 = 3/5 < 4/5 < 1 < 6/5 < 7/5 \\ L(\lambda): & 60 \quad 200 \quad 391 \quad 200 \quad 60. \end{array}$$

EXAMPLE 4.4 ($d=39$ case). At $p\equiv 34 \pmod{d}$, we have $f=4$, $p^{f/2}\not\equiv -1 \pmod{d}$ and $HW(X)=HW(X)_{nilp}$. Moreover

$$\#\{w\in\mathscr{W}_0 \mid p^i\cdot w\in\mathscr{W}_0 (i=0, 1, 2),\ p^3\cdot w\in\mathscr{W}_2\} = 12,$$

$$\#\{w\in\mathscr{W}_0 \mid p^i\cdot w\in\mathscr{W}_0\ (i=0, 1),\ p^2\cdot w\notin\mathscr{W}_0\} = 572;\ \text{rank } HW(X) = 584$$

and

$$\begin{array}{rl} Nwt(X): & \lambda_0 = 1/2 < 3/4 < 1 < 5/4 < 3/2 \\ L(\lambda): & 1{,}264 \quad 12{,}416 \quad 26{,}107 \quad 12{,}416 \quad 1{,}264. \end{array}$$

References

[1] N. Koblitz, *P*-adic variation of the zeta-function over families of varieties defined over finite fields, Compositio Math., **31** (1975), 119–218.

[2] J.-P. Serre, Faisceaux algébriques cohérents, Ann. of Math., **61** (1955), 197–278.

[3] T. Shioda and T. Katsura, On Fermat varieties, Tôhoku Math. J., **31** (1979), 97–115.

Department of Mathematics,
Faculty of Education,
Yokohama National University