PACIFIC JOURNAL OF MATHEMATICS
Vol. 43, No. 2, 1972

THE HASSE-WITT-MATRIX OF SPECIAL PROJECTIVE VARIETIES

LEONHARD MILLER

The Hasse-Witt-matrix of a projective hypersurface defined over a perfect field k of characteristic p is studied using an explicit description of the Cartier-operator. We get the following applications. If L is a linear variety of dimension $n+1$ and X a generic hypersurface of degree d, which divides $p-1$, then the Frobenius-operator $\mathscr{F}$ on $H^n(X\cdot L; \mathscr{O}_{L\cdot Y})$ is invertible.

As another application we prove the invertibility of the Hasse-Witt-matrix for the generic curve of genus two. We don't study the Frobenius $\mathscr{F}$ directly, but the Cartier-operator [1]. It is well-known, that for curves Frobenius and Cartier-operator are dual to each other under the duality of the Riemann-Roch theorem. A similar fact is true for higher dimension via Serre duality. We have therefore to extend to the whole "De Rham" ring the description of the Cartier-operator given in [4] for 1-forms. We give this extention in §1. Diagonal hypersurfaces are studied in §2 and the invertibility of the Hasse-Witt-matrix is proved, if the degree divides $p-1$. The same theorem for the generic hypersurface follows then from the semicontinuity of the matrix rank. The §3 is devoted to hyperelliptic curves and is intended as a preparation for a detailed study of curves of genus two.

1. The Cartier-operator of a projective hypersurface.

We extend the explicit construction of the Cartier-operator given in [4] to the whole "De Rham" ring, but restrict ourself to projective hypersurfaces.

As an application we show: Let V be a projective hypersurface of dimension $n-1$, defined by a diagonal equation $F(X) = \sum_{i=0}^{n} a_i X_i^r$, $a_i \in k$ a perfect field of $\operatorname{char} k = p > 0$, $a_i \neq 0$. Let X be a linear variety of dimension $t+1$. If r divides $p-1$, then

$$\mathscr{F}: H^t(X\cdot V, \mathscr{O}_{X\cdot V}) \to H^t(X\cdot V, \mathscr{O}_{X\cdot V})$$

is invertible, $\mathscr{F}$ being the induced Frobenius endomorphism. We have to rely on a technical proposition, which is a collection of some lemmas in [4]. We give first the proposition.

PROPOSITION 1. *Let*

$$\psi: k[T] \to k[T] \qquad (T = (T_1, \cdots, T_n))$$

be k p^{-1}*—linear and*

$$\psi(T^{\mu}) = \begin{cases} T^{\nu} & \text{if } \mu = p\cdot\nu \\ 0 & \text{else} . \end{cases}$$

Then the following holds:

(1) $\psi(T_{\mu_1} \cdots T_{\mu_r} h) = T_{\mu_1} \cdots T_{\mu_1}\bar{h}$, *for some* $\bar{h} \in k[T]$

(2) *Let* $D_\mu = T_\mu\, (\partial/\partial T_\mu)$ *and* $D_\mu g = 0$ *for a given* $1 \leqq \mu \leqq n$, *then* $\psi(D_\mu h\cdot g) = 0$

(3) *Let* $D_\mu g = 0$, *then* $\psi(h^{p-1}D_\mu h\cdot g) = D_\mu h \psi(g)$.

Proof.

(1) By the p^{-1}-linearity of ψ we may assume h to be a monomial. The statement follows then directly from the definition of ψ.

(2) ψ is p^{-1}-linear, so we may assume h to be a monomial

$$h = T_1^{r_1} \cdots T_n^{r_n} , \qquad 0 \leqq r_i \leqq p-1$$

(say $\mu = n$), then $D_n h = r_n\cdot h$. If $r_n = 0$ then (2) is trivially true. So $r_n \neq 0$. Again because of p^{-1}-linearity we may also assume g to be monomial.

But $D_n g = 0$, so

$$g = T_1^{v_1} \cdots T_{n-1}^{v_{n-1}} \qquad 0 \leqq v_i \leqq p-1 .$$

So the exponent of T_n in $D_n h\cdot g$ is r_n and $0 < r_n \leqq p-1$, therefore not divisible by p. The definition of ψ gives

$$\psi(D_n h\cdot g) = 0 .$$

(3) We may write

$$h = f_0 + f_1\cdot T_\mu + \cdots + f_r\cdot T_\mu^r , \qquad 0 \leqq r \leqq p-1$$

and

$$D_\mu f_i = 0 .$$

We proceed by induction on T. $r = 0$ clear. Let $r \geqq 1$, then $h = f + T_\mu \bar{h}$ with $D_\mu f = 0$ $\deg_{T_\mu} \bar{h} < r$. Now

$$T_\mu^{p-1}\bar{h}^{p-1}D_\mu(T_\mu\bar{h}) = (T_\mu\bar{h})^p\Big(\frac{D_\mu T_\mu}{T_\mu} + \frac{D_\mu\bar{h}}{\bar{h}}\Big) .$$

By p^{-1}-linearity of ψ and induction assumption for $\bar{h}$ we get

$$\begin{aligned} \psi(g\cdot T_\mu^{p-1}\bar{h}^{p-1}D_\mu(T_\mu\bar{h})) &= T_\mu\bar{h}\psi(g) + T_\mu\psi(g\cdot\bar{h}^{p-1}D\bar{h}) \\ &= \psi(g)(T_\mu\bar{h} + T_\mu D_\mu\bar{h}) \\ &= D_\mu(T_\mu\bar{h})\cdot\psi(g) . \end{aligned}$$

On the other hand

$$T_\mu^{p-1}\bar{h}^{p-1} = (h - f)^{p-1} = h^{p-1} + \frac{\partial P}{\partial h} ,$$

where P is a polynomial in f and h. We have

$$D_\mu(T_\mu \bar{h}) = D_\mu(h - f) = D_\mu h .$$

So

$$T_\mu^{p-1}\bar{h}^{p-1}D_\mu(T_\mu\bar{h}) = h^{p-1}D_\mu h + D_\mu P .$$

Multiply by g and apply ψ, then one gets

$$D_\mu h\cdot\psi(g) = D_\mu(T_\mu\bar{h})\psi(g) = \psi(h^{p-1}D_\mu h\cdot g) + \psi(D_\mu P\cdot g) .$$

But by (2)

$$\psi(D_\mu P\cdot g) = 0 .$$

Let $F(X_0 \cdots X_n)$ define a absolutely irreducible hypersurface V/k in $\mathscr{P}_{n,k}$ $\operatorname{char} k = p > 0$. We denote by $f(X_1 \cdots X_n)$ an affinization of F. Let $F_\mu = (\partial/\partial X_\mu)F$, similar f_μ $1 \leqq \mu \leqq n$. We assume f_n not to be the zero function on V. Let $K = K(V)$ be the function field of V. We assume that $K = K^p(x_1 \cdots \check{x}_j \cdots x_n)$ for any index j. The x_i are the coordinate functions and $\check{x}_j$ means omit x_j. As a consequence of these assumptions, we have that for a given index j any function $z \in K$ can be represented modulo F by a rational function $G(X_1 \cdots X_n)$, which is X_j-constant, i.e. such that $\partial G/\partial X_j = 0$. Write

$$F_{i_1,\cdots,i_r,n} = (X_{i_1} \cdots X_{i_r}\cdot X_n)^{-1}F .$$

DEFINITION 1. Let

$$\psi_{F_{i_1,\cdots,i_r,n}} = F_{i_1,\cdots,i_r,n}\circ\psi\circ F^{-1}_{i_1,\cdots,i_r,n} .$$

Let $\omega = \sum_{i_1\cdots i_r} h_{i_1,\cdots,i_r}\cdot dx_{i_1} \wedge \cdots \wedge dx_{i_r}$ be r-form on V. Put

$$\omega_{i_1,\cdots,i_r} = \frac{dx_{i_1} \wedge \cdots \wedge dx_{i_r}}{f_n} .$$

Define

$$C(\omega) = \sum_{i_1,\cdots,i_r} \psi_{Fi_1,\cdots,i_r,n}(h_{i_1,\cdots,i_r} - f_n)\omega_{i_r,\cdots,i_r} .$$

The definition is justified by the following theorem.

THEOREM 1. (1) *C is p^{-1}-linear*

(2) *If $\omega = d\varphi$, then $C(\omega) = 0$*

(3) *If* $\omega = z_{i_1}^{p-1} \cdots z_{i_r}^{p-1} dz_{i_1} \wedge \cdots \wedge dz_{i_r}$ *then* $C(\omega) = dz_{i_1} \wedge \cdots \wedge dz_{i_r}$. *In other words, if one restricts* C *to* $Z^r_{V/k}$, *the closed forms, then*

$$C\colon Z^r_{V/k} \to \Omega^r_{V/k}$$

is the Cartier-operator of V [1].

Proof of the theorem.

(1) The p^{-1}-linearity follows from the p^{-1}-linearity of ψ.

(2) Let $\varphi = \sum_{i_1,\dots,i_{r-1}} \varphi_{i_1,\dots,i_{r-1}} dx_{i_1} \wedge \cdots \wedge dx_{i_{r-1}}$ be a $(r-1)$-form, then

$$d\varphi = \sum_j \sum_{i_1,\dots,i_{r-1}} \frac{\partial}{\partial x_j}(\varphi_{i_1,\dots,i_{r-1}}) dx_j \wedge dx_{i_1} \wedge \cdots \wedge dx_{i_{r-1}} .$$

To simplify the notation we put for the moment

$$\varphi_{i_1,\dots,i_{r-1}} = \tilde{\varphi}$$

and

$$F_{j_1 i_1,\dots,i_{r-1},n} = \tilde{F} .$$

To compute $C(d\varphi)$ we have to compute

$$\varphi_{\tilde{F}}\left(\frac{\partial}{\partial x_j}\tilde{\varphi}\cdot f_n\right)$$

for every system $(j, i, \cdots, i_{r-1})$.

Now remembering the definition of $\psi^{\tilde{F}}$ we have to show

$$\psi(F^{p-1} D_n F X_{i_1} \cdots X_{i_{r-1}} D_j \varphi) = 0$$

in order to get $C(d\varphi) = 0$.

We have to use the above proposition. We apply first (3) and then (2) and get:

$$\psi(F^{p-1} D_n F X_{i_1} \cdots X_{ir-1} D_j \varphi) = D_n F \psi(X_{i_1} \cdots X_{i_{r-1}} D_j \varphi) = 0 .$$

Remark, that we assume $j \neq (i_1, \cdots, i_{r-1})$ otherwise

$$dx_j \wedge dx_{i_1} \wedge \cdots \wedge dx_{i_{r-1}} = 0 .$$

That shows $C(d\varphi) = 0$

(3) Let $\omega = z_{i_1}^{p-1} \cdots z_{ir}^{p-1} dz_{i_1} \wedge \cdots \wedge dz_{i_r}$.

We have

$$dz_{i_1} \wedge \cdots \wedge dz_{i_r} = \sum_{j_1 \cdots j_r} D_{j_1} z_{i_1} \cdots D_{j_r} z_{i_r} \frac{dx_{j_1} \wedge \cdots \wedge dx_{j_r}}{x_{j_1} \cdots x_{j_r}} ,$$

$$D_j = x_j \frac{\partial}{\partial x_j} .$$

To Compute $C(\omega)$, we have to work out

$$U = \psi(F^{p-1} D_n F \cdot Z_{i_1}^{p-1} \cdot D_{j_1} Z_{i_1} \cdots Z_{i_r}^{p-1} D_{j_r} Z_{i_r}) \text{ modulo } F .$$

$$Z_j \bmod F = z_j .$$

We apply several times (3) of the propositition and get

$$U \equiv D_n F D_{j_1} Z_{i_r} \cdots D_{j_r} Z_{i_r} \bmod (F) .$$

Therefore

$$C(\omega) = \sum_{j_r j_r} D_n f D_{j_1} z_{i_1} \cdots D_{j_r} z_{i_r} \frac{dx_{j_1} \wedge \cdots \wedge dx_{j_r}}{x_n f_n x_{j_1} \cdots x_{j_r}}$$
$$= dz_i \wedge \cdots \wedge dz_{i_r} .$$

All forms of highest degree $n-1$ are closed. We use the fact, that $H^\circ(V, \Omega^{n-1})$ has a basis of the following form

$$\omega_u = x_1^{u_1} \cdots x_n^{u_n} \omega_0 .$$

where

$$\omega_0 = \frac{dx_1 \wedge \cdots \wedge dx_{n-1}}{x_1 \cdots x_n f_n}$$

$$\sum_{i=1}^{n} u_i \leqq r;\ r = \deg V \quad \text{and} \quad 1 \leqq u_i .$$

Recall $x_i = X_i / X_0$ are coordinate functions on V and of the affinization of $F, f_n = \partial f / \partial x_n$.

We get the important corollary to the theorem.

COROLLARY 1. *Let $A_{u,v}$ be the matrix of the Cartier-operator on $H(V, \Omega^{n-1})$ with respect to the above basis ω_u. Then*

$$A_{u,v} = \textit{coefficient of } X^v \textit{ in } \psi(F^{p-1} \cdot X^u)$$

$$X^u = X_0^{u_0} \cdots X_n^{u_n} , \quad \sum_{i=0}^{n} u_i = \sum_{i=0}^{n} v_i = r$$

$$\left.\begin{matrix} 1 \leqq u_i \\ 1 \leqq v_i \end{matrix}\right. \quad \textit{for} \quad i = 1 \cdots n .$$

Proof. By definition

$$C(\omega_u) = \psi_{F_{1\cdots n}}(x_1^{u_1-1} \cdots x_n^{u_n-1}) \frac{dx_1 \wedge \cdots \wedge dx_{n-1}}{f_n}$$
$$= \psi(f^{p-1} \cdot x^u)\omega_0 .$$

Now recall

$$\psi(f^{p-1} \cdot x^u) = \psi\left(\frac{F^{p-1} X_0^{u_0} \cdots X_r^{u_r}}{X_0^{pr}}\right) \bmod F$$
$$\sum_{i=0}^{n} u_i = r , \quad 1 \leqq u_i , \quad i = 1 \cdots n .$$

If $A_{u,v}$ is the coefficient of X^v in $\psi(F^{p-1} \cdot X^u)$.

Then

$$C(\omega_u) = \sum_{\substack{1 \leqq v_i \leqq r \\ i=1 \cdots n}} A_{u,v} x_1^{v_1} \cdots x_n^{v_n} \omega_0 = \sum_v A_{u,v} \omega_v .$$

Notice

$$\sum_{i=0}^{n} u_i = \sum_{i=0}^{n} v_i = r , \quad 1 \leqq u_i, 1 \leqq v_i, i = 1 \cdots n .$$

REMARK. We have now on explicit description for the Cartier-operator on $H^0(V, \Omega_{V/k}^{n-1})$. We can use Serre duality $H^0(V, \Omega_{V/k}^{n-1})^\vee \cong H^{n-1}(V, \mathcal{O}_U)$. Under this duality $\check{C}$ is the Frobenius $\mathcal{F}$ on $H^{n-1}(V, \mathcal{O}_V)$. We have therefore also an explicit description for $\mathcal{F}$.

2. The Cartier-operator of a diagonal hypersurface. Let $F(X) = \sum_{i=0}^{n} a_i X_i^r$ define a "generic" hypersurface. To compute the Cartier-operator, by the preceding discussion we have to analyse

$$\psi(F^{p-1} X^u) \qquad \left(\sum_{i=0}^{n} u_i = r , \quad u_i > 0\right) .$$

Let us adapt the following notation:

$$\rho! = \rho_0! \cdots \rho_n! , \quad a^\rho = \prod_{i=0}^{n} a_i^{\rho_i} , \quad X^{u+1} = \prod_{i=0}^{n} X_i^{u_i+1} ,$$
$$|u| = \sum_{i=0}^{n} u_i , \quad u > 0 \Leftrightarrow u_i > 0 \quad (i = 0 \cdots n) .$$

THEOREM 2. *Let*

$$\operatorname{char} k = p > 0, F(X) = \sum_{i=0}^{n} a_i X_i^r , \quad \prod_{i=0}^{n} a_i \neq 0 \in k$$

V/k is defined by F. Suppose r divides $p-1$. Then the Cartier-operator

$$C: H^\circ(V, \Omega^{n-1}_{V/k}) \to H^\circ(V, \Omega^{n-11}_{V/k})$$

is invertible.

Proof.

$$F^{p-1} = \sum_{|m|=p-1} \frac{(p-1)!}{m!} a^m X^{rm} .$$

Using p^{-1}-linearity of ψ we get

$$\psi(F^{p-1}X^u) = \sum_{|m|=p-1} \frac{-1}{m!} \bar{a}^m \psi(X^{rm+u}) = \sum_{|m|=p-1} \frac{-1}{m!} \bar{a}^m X^v .$$

We put $\bar{a} = a^{1/p}$, and $rm + u = pv$. Notice if $u > 0$ and $|u| = r$, then also $v > 0$ and $|v| = r$. If we write

$$\psi(F^{p-1}X^u) = \sum_{\substack{|v|=r \\ v>0}} A_{u,v} X^v ,$$

then we have

$$A^p_{u,v} = \begin{cases} -\dfrac{1}{m!} a^m & \text{if} \quad rm = (p-1)v + v - u \\ & \qquad |u| = |v| = r \quad u > 0 \quad v > 0 \\ 0 & \text{else} . \end{cases}$$

Let us now assume:

$$p - 1 = r \cdot s .$$

If r divides $v - u$ put $v - u = r \cdot E(u, v)$ then

$$A^p_{u,v} = \begin{cases} -\dfrac{1}{m!} a^m & \text{if} \quad r | v - u \quad \text{and} \quad m = sv + E(u, v) \\ 0 & \text{else} . \end{cases}$$

We fix now a total ordering of u, v. Let us order the n-tuples $(u_1 \cdots u_n)$ resp $(v_1 \cdots v_n)$ lexicographically and put

$$u_0 = r - \sum_{i=1}^n u_i \quad \text{resp.} \quad v_0 = r - \sum_{i=1}^n v_i$$

$v < u$ means now, that either $v_1 < u_1$ or $v_i = u_i$ for $i = 1 \cdots j - 1$ but $v_j < u_j$. If any case, if $v < u$, then $v_j < u_j$ for some j. We claim if $v < u$, the $A_{u,v} = 0$.

Case 1. r does not divide $u - v$, then $A_{u,v} = 0$.

Case 2. r divides $u - v$. Now if $v < u$ then for some j $u_j - v_j > 0$

and r divides $u_i - v_j$. But $r \geqq u_j$ and $v_j \geqq 1$, so $r - 1 \geqq u_j - v_j$, therefore r cannot divide $u_j - v_j$. This contradiction shows, if $v < u$, then $A_{u,v} = 0$. $A_{u,v}$ is therefore a triangle matrix.

What is the diagonal?

$$A_{u,u}^p = -\frac{1}{m!}a^m$$

with $m = s \cdot u$. Therefore

$$(\det A_{u,v})^p = \prod_u \left(-\frac{1}{(su)!}\right) a^{s\sum_u u} \neq 0$$

COROLLARY 2. *The assumptions are the same as in the theorem. Then*

$$\mathscr{F}: H^{n-1}(V, \mathcal{O}_V) \to H^{n-1}(V, \mathcal{O}_V) \quad (\mathscr{F} \text{ is the Frobenius morphism})$$

is invertible.

Proof. Clear by Serre duality and the fact that $\check{C} = \mathscr{F}$.

The Cartier-operator of $W \cdot H$. The differential operator C as given in Definition 1 on Ω^1 is by p^{-1}-linearity completely determined on Ω^1 by its value on $\omega = h \cdot dx$, where x runs through a set of coordinate functions.

We have $C(\omega) = x^{-1}\psi(xh)dx$, that notation is only intrinsic, if $d\omega = 0$, because ψ depends on the coordinate system. If we choose a different coordinate system, then we get in general a different operator; but for ω with $d\omega = 0$, we get the same, namely the Cartier-operator.

That fact can be exploited in the following way. Suppose

$$W = \{x_1 = x_2 \cdots = x_t = 0\} \cap H .$$

We write now C_H resp. C_W for the the operators. The above definition shows $\bigoplus_{i=1}^t K dx_i$ is stable under C_H. But by the property of ψ, $\psi(X_i H) = X_i \bar{H}$ for some $\bar{H}$, we have for

$$\omega = x_i h dx_j \quad i \neq j \quad i, j \text{ arbitrary}$$
$$C_H(\omega) = x_i \bar{h} dx_j .$$

Let $\mathfrak{A} = \{x_1 \cdots x_t\}$, then $\mathfrak{A}\Omega^1_{H/k} \oplus \bigoplus_{i=1}^t \mathcal{O}_H dx_i$ is stable under C_H. By the exact sequence

$$0 \to \mathfrak{A}\Omega^1_{H/k} + \bigoplus_{i=1}^t \mathcal{O}_H dx_i \to \Omega^1_{H/k} \to \Omega^1_{W/k} \to 0$$

C_H induces an operator C_W on $\Omega^1_{W/k}$. C_W has again the properties

(1) C_W is p^{-1}-linear
(2) $C_W(dh) = 0$
(3) $C_W(h^{p-1}dh) = dh$.

If we restrict C_W to the closed forms on W, then C_W is the Cartier-operator.

Let now L be an arbitrary linear variety. After a suitable coordinate change we may assume L is the intersection of some coordinate hyperplanes. $W = L \cdot H$ has then the above shape.

Let us assume that the hypersurface H has a diagonal defining equation of degree d diving $p - 1$, $p = \operatorname{char} k$. Then the above Theorem 1 shows that C_W is semisimple on $Z^1_{W/k}$. In the same way as before we can extend C_W to any $\Omega^r_{W/k}$, in particular to $\Omega^m_{W/k}$, where $m = \dim W$. As result of this discussion we get:

THEOREM 3. *If L is a linear variety of dimension $m + 1$, then there exists a hypersurface H of degree d, which divides $p - 1$, such that*

$$\mathscr{F}: H^m(L \cdot H, \mathcal{O}_{L \cdot H}) \to H^m(L \cdot H, \mathcal{O}_{L \cdot H})$$

is invertible.

3. The Cartier-operator of plane curves. For curves the explicit description of the Cartier-operator is of special interest if one wants to study, how the Cartier-operator varies with the moduli of the curve. Unfortunately one is restricted to plane curves, because the above explicit form of the Cartier-operator is available only for hypersurfaces.

If one specializes the above results to plane curves, one has to assume, that the curve is singularity free.

The space $W = \{$homogenous forms of degree $d - 3\}$ is for non-singular curves V of degree d isomorphic to $H^\circ(V, \Omega^1_{V/k})$ under

$$W \xrightarrow{\sim} H^0(V, \Omega^1_{V/k})$$
$$P(X) \to P(x)\omega_0$$

where the coordinate functions are given by

$$x = X_1/X_0 \,, \quad y = X_2/X_0 \mod F \,,$$

F being the defining equation for V and $f(x, y)$ the affinization, f_y denotes $\partial f/\partial y$. With that notation $\omega_0 = dx/f_y$.

But it is important to know, that one can give a similar description also for singular curves. Then W is the space of $P(X)$, which define the "adjoint" curves to V. These are those curves, which cut out at least the "double point divisor".

To give an explicit basis depends on nature of the singularities.

Hyperelliptic curves: Let $p = \operatorname{char} k > 2$.

For a detailed study of the Hasse-Witt-matrix of hyperelliptic curves one needs the explicit Cartier-operator with respect to various "normal forms".

Let the hyperelliptic V be given by $y^2 = f(x)$, $\deg f(x) = 2g + 1$ and such that $f(x)$ has no multiple roots. V has a singularity at "infinity". One could apply the above method and work out the adjoint curves in order to get a basis for $H^0(V, \Omega^1_{V/k})$. But we have already a basis, namely if $\omega = dx/y$ then $\{x^i\omega \mid i = 0 \cdots g - 1\}$ form a basis.

We specialize the results of §2 and get from Corollary 1 as matrix for the Cartier-operator with respect to the above basis (let us put $p - 1/2 = m$):

$$A_{u,v} = \text{coefficient of } x^{v+1} \text{ in } \psi(f(x)^m x^{u+1}) \quad 0 \leqq {u \atop v} \leqq g - 1 .$$

Legendre form: We assume now the defining equation in Legendre form.

$$f(x) = x(x-1) \prod_{i=1}^{r} (x - \lambda_i) \qquad \begin{array}{l} r = 2g - 1 \\ \lambda_i \neq \lambda_j \neq 0, 1 . \end{array}$$

Notation: Let

$$|\rho| = \rho_1 + \cdots + \rho_r$$
$$\lambda^\rho = \lambda_1^{\rho_1} \cdots \lambda_r^{\rho_n} .$$

The permutation group of r elements S_r operates on the monomials

$$\lambda^\rho \longrightarrow \lambda^{\pi(\rho)}, \pi \in S_r .$$

Let G_ρ be the fix group of $\lambda^{m-\rho}$ and $G^{(\rho)} = S_r/G_\rho$. Let

$$H^{(\rho)}(\lambda) = \sum_{\pi \in G^{(\rho)}} \lambda^{m-\pi(\rho)} .$$

Apparently

$$H^{(\rho)} = H^{(\bar{\rho})} , \quad \text{iff} \quad \bar{\rho} = \bar{\pi}(\rho) .$$

We may therefore assume

$$0 \leqq \rho_1 \leqq \rho_2 \leqq \rho_r \leqq m .$$

For given

$$0 \leqq {u \atop v} \leqq g - 1 \quad \text{let} \quad \rho_0 = |\rho| - vp + u .$$

Put

$$a_{u,v}^{(\rho)} = (-1)^{u+v+m}\binom{m}{\rho_0}\cdots\binom{m}{\rho_r}$$

and

$$A_{u,v}^{p} = \sum_{\rho} a_{u,v}^{(\rho)} H^{(\rho)}(\lambda) \qquad 0 \leqq {u \atop v} \leqq g-1,\ r = 2g-1$$

the summation condition being:

$$0 \leqq \rho_1 \leqq \cdots \leqq \rho_r \leqq m\,, \quad \rho_0 = |\rho| - vp + u\,, \quad 0 \leqq \rho_0 \leqq m$$

$$vp - u + m \geqq |\rho| \geqq vp - u\,.$$

We state as a proposition

PROPOSITION 2. *Let be* $A_{u,v}$, $0 \leqq {u \atop v} \leqq g-1$, *as defined above, and* $\omega = dx/y$, *then*

$$C(x^u\omega) = \sum_{0 \leqq v \leqq g-1} A_{u,v} x^v \omega$$

is the Cartier-operator.

Applications: We want to investigate, when the Cartier-operator is invertible. It seems that an answer to that question, without any restrictions is not available. It is therefore worthwhile to have various methods even in special cases.[1]

We restrict ourself to genus 2, although the method could be applied to higher genus, but the calculations would be very easy. Let $p > 2$ and $g = 2$

$$\text{i.e. } y^2 = x(x-1)(x-\lambda_1)(x-\lambda_2)(x-\lambda_3)\,, \quad \lambda_i \neq \lambda_j \neq 0, 1 \quad i \neq j\,.$$

The notation is the same as above.

$H^{(\rho)}(\lambda)$ is homogeneous in the λ's of degree $3m - |\rho|$, $m = (p-1)/2$. We have

$$A_{u,v}^{p} = \sum_{0 \leqq \rho_0 \leqq \rho_1 \leqq \rho_2 \leqq \rho_3 \leqq m} a_{u,v}^{(\rho)} H^{(\rho)}(\lambda) \qquad 0 \leqq {u \atop v} \leqq 1$$

$$\rho_0 = |\rho| - vp + u \quad vp - u \leqq |\rho| \leqq vp - u + m\,.$$

We want to know of $A_{u,v}^{p}$, what the forms of lowest homogeneous degree in the λ's are. We have to give $|\rho|$ the maximal possible value.

We use the shorthands

[1] *Added in proof*: We settled this question in the meantime, see [**6**].

$$\binom{m}{\rho} = \prod_{i=1}^{3} \binom{m}{\rho_i}$$

and $D(u, v)$ = degree of the lowest homogeneous term in $A^p_{u,v}$. In the list below is $\rho_0 = \max|\rho| - vp + u$.

(u, v)	$\max\|\rho\|$	ρ_0	$D(u, v)$
(0, 0)	m	m	$p-1$
(0, 1)	$3m$	$m-1$	0
(1, 0)	$m-1$	m	p
(1, 1)	$3m$	m	0

We get therefore:

$$A^p_{0,0}A^p_{1,1} = \text{terms of degree } p-1 + \text{higher terms}$$
$$A^p_{0,1}A^p_{1,0} = \text{terms of degree } p + \text{higher terms}\,.$$

The lowest degree term L in $\det(A_{u,v})^p$ is given by

$$L = m\sum \binom{m}{\rho} H^{(\rho)}(\lambda)$$
$$\rho_1 + \rho_2 + \rho_3 = m$$
$$0 \leqq \rho_1 \leqq \rho_2 \leqq \rho_3\,.$$

Notice, if $\rho \neq \bar{\rho}$, then $H^{(\rho)}$ and $H^{(\bar{\rho})}$ have no monomial in common. Therefore L is not the zero polynomial. We are able to specialize the variables $(\lambda_1, \lambda_2, \lambda_3)$ in the algebraic closure of k, such that $\det(A_{u,v}) \neq 0$. In other words, there exist curves of genus two with invertible Cartier-operator.

We do not know, what the smallest finite field is, over which such a curve exists.

REMARK. For large p we could push through a similar discussion for higher genus. We omit that, because there is a more elegant method for large p by Lubin (unpublished). Let $y^2 = x^{2g+1} + ax^{g+1} + x$. The claim is, that for large p (depending on g) and variable a the Hasse-Witt-matrix of that curve is a permutation matrix.

REFERENCES

1. P. Cartier, *Questions de rationalité des diviseurs en géometrie algébrique*, Bull. Soc. Math. France, **86** (1958). 177-251.

2. H. Hasse, *Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p*, J. f. r. a. Math., **172** (1934), 77-85.

3. H. Hasse and E. Witt, *Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Characteristik p.* Monatshefte

Math. Phys., **43** (1936), 477-493.
4. L. Miller, *Über die Punkte der Ordnung p auf einer Jacobischen k-Varietät, char k* $= p > 0$. Nachr. Akad. Wiss. Göttingen, II. Math.-Phys. Kl. (1969), Nr. 2, 9-23.
5. ———, *Elementarer Beweis eines Satzes von H. Hasse über die Punkte der Ordnung p auf einer elliptischen k-Kurve,* $p = \text{char}\, k$, Nachr. Akad. Wiss. Göttingen, II. Math.-Phys. Kl. (1969), Nr. 1, 1-8.
6. ———, *Curves with invertible Hasse-Witt-matrix* (appears in Math. Annalen)

Received June 28, 1971. This research was supported partially by the Ohio State University and partially by NSF-grant GP-20833.

OHIO STATE UNIVERSITY