Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Francis J. Sullivan

Hasse-Witt matrices and Kummer extension

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **82** (1988), n.3, p. 405–411.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1988_8_82_3_405_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1988.

RENDICONTI

DELLE SEDUTE

DELLA ACCADEMIA NAZIONALE DEI LINCEI

Classe di Scienze fisiche, matematiche e naturali

Luglio-Settembre 1988

SEZIONE I

(Matematica, meccanica, astronomia, geodesia e geofisica)

Atti Acc. Lincei Rend. fis.
(8), LXXXII (1988), pp. 405-411

Matematica. – *Hasse-Witt matrices and Kummer extension.* Nota di FRANCIS J. SULLIVAN, presentata (*) dal Socio G. SCORZA DRAGONI.

ABSTRACT. – A simple calculation of the Hasse-Witt matrix is used to give examples of curves which are Kummer coverings of the projective line and which have easily determined p- rank. A family of curve carrying non-classical vector bundles of rank 2 is also given.

KEY WORDS: Jacobian variety; Hasse-Witt matrix; Cartier operator.

RIASSUNTO. – *Matrici di Hasse-Witt ed estensioni di Kummer.* Sulla base di un calcolo semplice si danno esempi di curve con proprietà legate al rango della matrice di Hasse-Witt.

Recently considerable study has been given to Jacobian varieties of cyclic covers of the projective line over an alg. closed field K of characteristic $p > 0$. Cf. [8] and [13]. Here we consider the problem of effectively calculating the Hasse-Witt matrix for curves X whose function field $K(X)$ admits a minimal generation of the type $K(X) = K(x, y_1, \dots, y_N)$ with each subfield $K(x, y_i)$ a cyclic extension of $K(x)$ of degree ℓ. For simplicity we take ℓ to be a prime, $\ell \neq p$. Thus, we consider curves

(*) Nella seduta del 12 dicembre 1987.

whose function fields are particular Kummer extensions of $K(x)$. Information about the Hasse-Witt matrix of X is useful in problems regarding stable vector bundles on X, in analyzing the zeta function of $K(X)$, and in finding the p-rank of the Jacobian variety J of X.

We begin by reviewing properties of simple Kummer extensions of $K(x)$. For a real number u we will denote the greatest integer *strictly* less than u by $\phi(u)$, and, as usual $[u]$ will denote the greatest integer less than or equal to u. Then, for

$R(x) = \prod_{j=1}^{N} (x - a_j)^{m_j}$, and i a nonnegative integer,

we set $R_i(x) = \prod_{j=1}^{N} (x - a_j)^{[i m_j/\ell]}$.

One then has

PROPOSITION 1. - Let L be a cyclic extension of $K(x)$ of prime degree ℓ, different from p, the characteristic of K. Then,

a.) L admits a representation of the form $L = K(x,y)$ with

$y^\ell = R(x) = \prod_{j=1}^{N} (x - a_j)^{m_j}$, where each $a_j \in K$ and $1 \leq m_j < \ell$ for each m_j

b.) The genus g_L of L is $\frac{1}{2}[(k-1)(\ell-1) - (n_\infty - 1)]$

where $n_\infty = \ell$ if ℓ divides $\deg(R(x))$, and $n_\infty = 1$ otherwise.

A basis for the K space of differentials of the first kind of L is given by the set $\omega_{ij} = x^j R_i(x)\, dx/y^i$ for $i = 1, 2, \ldots, \ell - 1$, and $j = 0, 1, \ldots d_i$ with

d_i defined by $d_i = \phi(i \deg(R(x))/\ell) - 1 - = \sum_{j=1}^{d_i} (i\, m_j/\ell)$,

ordered lexicographically with respect to (i,j).

c.) If $\alpha = (i, j)$ and $\beta = (i^*, j^*)$ are indices of differentials of the basis in b.), then the (α, β) entry of the Hasse-Witt matrix $\mathbf{A}$ of L is

$$A^{\alpha\beta} = \begin{cases} 0 & \text{if } i^* p \text{ is not congruent to } i \bmod \ell \\ \text{coeff. of } x^{(j^*+1)p-1} \text{ in } \dfrac{x^j R_i(x) R(x)^{(i^* p - i)/\ell}}{R_{i^*}^p(x)} & \text{otherwise} \end{cases}$$

Proof: Except for c.) these facts are proved in [12], and the classical proof remains valid under the present hypotheses.

As to c.), we recall that if A is the Hasse-Witt matrix of L then $A^{1/p}$, the matrix obtained from A by taking the p-th root of each entry, is the matrix of the Cartier operator C. So, with ω_{ij} as above, we find

$$C(\omega_{ij}) = C(x^j R_i(x)\,dx/y^i) = C(x^j R_i(x) R_{i'}{}^p(x)\, y^{i'p-i} dx / R_{i'}{}^p(x)\, y^{i'p})$$

where i' is the unique integer with $1 \leq i' \leq \ell - 1$ and $i'p \equiv i$ modulo ℓ. By the p^{-1} -linearity of C the last term above is

$$(R_i(x)/y^{i'})\, C(x^j R_i(x) R(x)^{(i'p-i)/\ell} dx / R_{i'}{}^p(x)),$$

and assertion c.) follows from the linearity of C and the fact that C kills exact differentials. Q.E.D.

Note that c.) tells us that A decomposes into blocks and is, in fact, a "block permutation matrix". For an Artin-Schreier version of Proposition 1 the reader may consult [8] or [11].

We wish to extend these results to the case of the more general Kummer extensions of $K(x)$ mentioned above. In particular, the case $N = 2$ corresponds to that of curves immersed in projective 3-space, and for general N we are considering "Kummer" curves in $N + 2$ space. Such representations seem somewhat neglected in the literature, probably because one can always find a (possibly singular) plane model for any curve.

Let $X_1 \to X_0$ be a separable covering of curves over K and let $\sigma: L_0 \to L_1$ be the corresponding imbedding of function fields. Let C_i be the Cartier operator associated to X_i, $i = 0, 1$, and for any differential ω on X_0 let $(\omega)_1$ indicate the contrace of ω in X_1. Then $(C_0\omega)_1 = C_1(\omega)_1$ so $C_i\omega$ is independent of the field in which it is computed. Thus, we delete the subscript on C in the sequel. For basic information on the Cartier operator and its relation to the Hasse-Witt matrix see, e.g. [1], [6] and [10]. We now extend Proposition 1 to general Kummer extensions.

THEOREM 1. – Let L be a Galois extension of $K(x)$ with elementary abelian Galois group G of order ℓ^s with ℓ a prime different from $p = \mathrm{char}(K)$.
Let L_i, for $0 \leq i \leq (\ell^s - 1)/(\ell - 1) = m$ be the minimal subfields of L containing $K(x)$. Let G be the genus of L and g_i the genus of L_i. Then,
a.) $G = g_1 + \ldots + g_m$;
b.) a basis for the space of differentials of the first kind on L is obtained by taking the union of bases for such differentials on the L_i;
c.) the Hasse-Witt matrix A of L decomposes into a block diagonal matrix made up of Hasse-Witt matrices A_i of the L_i with $g_i > 0$.

Proof: a.) By Kummer theory and Proposition a.) $L = K(x, y_1, \ldots, y_s)$ where $y_t{}^\ell = f_t(x)$ for $1 \leq t \leq s$ and each $f_t(x)$ is as in Prop. 1a).

The m distinct minimal subfields of L then have the form

$$L_i = K(x, y_1^{i_1} y_2^{i_2} \dots y_{u-1}^{i_{u-1}} y_u)$$

where $1 \leq u \leq s$ and $0 \leq i_j \leq \ell - 1$ for each i_j.

These L_i are indeed the m distinct minimal subfields of L since the corresponding subgroups of G are distinct. Let z_i denote the product of the y's appearing in the definition of L_i. Then, if $r_i(x)$ denotes the polynomial obtained from z_i by replacing each y_j with $f_j(x)$, we see that the defining equation of L_i is $z_i^\ell = r_i(x)$. As for g_i, a simple modification of the formula in Proposition 1 b) gives $g_i = {}^1/_2(\ell - 1)(k - 1 - \#\text{unram})$, where #unram is the number of places among the roots of $r_i(x)$ and infinity which do not ramify in L_i.

Let ν be the number of distinct places of $K(x)$ which ramify in at least one L_i. Thus, ν is the number of distinct roots of the polynomials $f_t(x)$, $1 \leq t \leq s$, including the root infinity if at least one $f_t(x)$ has degree prime to ℓ. For each i, $1 \leq i \leq m$, let ν_i be the number of places of $K(x)$ ramifying in some L_j but NOT in L_i. The Hurwitz formula then gives $g_i = (\ell - 1) + {}^1/_2(\ell - 1)(\nu - \nu_i)$, whence

$$\sum_{i=1}^{m} g_i = m(\ell - 1) + \frac{1}{2} m(\ell + 1)\nu - \frac{1}{2}(\ell - 1)\sum_{j=1}^{m} \nu_i .$$

To evaluate $\Sigma\, \nu_i$ let $x - a$ define a place $\mathfrak{p}$ of $K(x)$ which ramifies in some L, and let e_t be the exact power of $x - a$ dividing $f_t(x)$, $1 \leq t \leq s$. Then $\mathfrak{p}$ does not ramify in the field $K(x, y_1^{d_1} \dots y_s^{d_s})$ if and only if

$$\sum_{t=1}^{6} e_t d_t \equiv 0 \text{ modulo } \ell$$

Obviously, this congruence has exactly ℓ^{s-1} non-trivial solutions $(d_1, \dots, d_s)$ modulo ℓ. Furthermore, each of the fields L_j appears exactly $\ell - 1$ times as a $K(x, y_1^{d_1} \dots y_s^{d_s})$, where $0 \leq d_t \leq \ell - 1$, $1 \leq t \leq s$, and not all $d_t = 0$. It follows that the contribution of $\mathfrak{p}$ to $\Sigma\, \nu_j$ is $(\ell^{s-1} - 1)/(\ell - 1)$. The place at infinity may be treated in the same way if it ramifies in any L_j. Hence

$$\sum_{i=1}^{m} \nu_i = \nu(\ell^s - 1)/(\ell - 1), \text{ and so one has}$$

$$(*) \qquad \sum_{i=1}^{m} g_i = (1 - \ell^s) + \frac{1}{2}\nu(\ell^s - \ell^{s-1}).$$

We now compute G. Let $L' = K(x, y_1, y_2, \dots, y_{s-1})$. Then $L = L'(y_s)$, and since all the assertions of our proposition are trivial when $s = 1$ we may assume inductively that we have the desired equality between G', the genus of L' and $\Sigma'\, g_j$, where the prime on the summation indicates that the sum is to be taken over the minimal subfields of L. Let $\nu = \nu' + \nu''$ where ν' is the number of places of $K(x)$ ramifying in some minimal subfield of L', and ν'' is the number ramifying only in minimal subfields of L which are not contained in L'.

By our inductive hypothesis and (*) we have

$$G' = (1 - \ell^{s-1}) + {}^1/_2\nu'(\ell^{s-1} - \ell^{s-2})$$

Each of the ν'' places of $K(x)$ not ramifying in L' must split into ℓ^{s-1} distinct places of L', and each of the resulting places must ramify with index ℓ in L. Moreover, since $\Sigma\, e_t d_t \equiv 0$ modulo ℓ for any place of $K(x)$ there is a subfield of L of degree equal to ℓ^{s-1} over $K(x)$ in which the given place is unramified. Thus, any place of $K(x)$ is either unramified in L, or has ramification index exactly ℓ. It follows that the only places of L' which ramify in L are the $\ell^{s-1}\nu''$ places already considered. Hence, the degree of the different $\mathfrak{D}_{L'/L}$ is $\nu(\ell^s - \ell^{s-1})$. Again using the Hurwitz formula, we find

$$2G - 2 = 1(2G' - 2) + \deg(\mathfrak{D}_{L/L'}),\ \text{whence by (*)}$$

$$G = 1 + \ell(G' - 1) + {}^1/_2\nu''(\ell^s - \ell^{s-1})$$

$$= 1 - \ell^s + {}^1/_2\nu(\ell^s - \ell^{s-1}) = \sum_{i=1}^{m} g_i,\ \text{which proves a).}$$

To prove b.) it suffices to do so for the special bases described in Proposition 1b). Suppose that $\sum_{j=1}^{\nu} c_j\omega_j = 0$ is a minimal non-trivial dependence relation. Clearly not all the ω_j come from a fixed subfield L_i. Hence, there is an automorphism σ of $L/K(x)$ which fixes ω_ν but does not fix all the other ω_j. The action of σ on differentials multiplies each ω_j by a non-zero scalar. Hence, applying σ to our minimal relation gives

$$\sum_{j=1}^{\nu} c_j'\omega_j = 0 \text{ with } c_\nu' = c_n \text{ but not all } c'_j = c_j \text{ for } j \neq \nu.$$

Subtraction now gives a contradiction to the assumed minimality.

Part c.) now follows from our earlier comments. Q.E.D.

REMARK. – The preceding proof could be fomulated in a more intrinsic fashion. Indeed, if $\hat{G}$ is the dual group of G, then each element of $\hat{G}$ defines a corresponding subspace of the space of line bundles L on X, and so a subspace of $H^1(X, \mathcal{O}_X)$. The correspondence is given by $L_{\hat{\sigma}} = \{\xi \in L \mid \tau\xi = \hat{\sigma}(\tau)\xi\ \forall \tau \in G\}$. Orthogonality of characters shows that the space of line bundles (or also $H^1(X, \mathcal{O}_x)$) decomposes into the direct sum of such subspaces. The same holds for the space of differentials and $H^0(X, \Omega x)$. The Frobenius mapping and the Cartier operator clearly map such subspaces into one another. This explains the "block form" of the Hasse-Witt matrix.

We can now extract a number of illustrative corollaries.

COROLLARY 1. - Let J_p be the group of p-division points on the Jacobian variety of L, and let $J_{p,i}$ be the corresponding object for L_i. Then rank $(J_p) = \sum_{i=1}^{\nu}$ rank $(J_{p,i})$. Furthermore, if $g^* = \max\{g_i\}$ then rank(J_p) = rank $(AA^{(p)} \ldots A^{(p^{g^*-1})})$. In particular, if rank$(J_p) = 0$, then the Cartier operator on $H^0(X,\Omega x)$ is nilpotent of index $\leq g^*$.

Proof: This follows from the above and standard results in [6]. Q.E.D.

We remark that there are genus G curves of p-rank equal to 0 for which the index of nilpotency of C is G. Thus, Kummer curves form a very restricted and amenable class. As a first example we have.

COROLLARY 2. - For each prime $p \geq 5$ there exist curves of genus 2 with Hasse-Witt matrix 0. In fact, such curves are defined over the quadratic extension of the prime field.

Proof: The Hasse invariant of E: $y^2 = x(x-1)(x-\lambda)$ is

$$A(\lambda) = (-1)^r \sum_{i=0}^{r} \binom{r}{i}^2 \lambda^i, \text{ where } r = (p-1)/2.$$

It is known (cf. [2], [7]) that $A(\lambda)$ has distinct roots and that 0 and 1 are not roots of $A(\lambda)$. Hence, for $p \geq 5$ we can choose $\lambda_1 \neq \lambda_2$ such that $A(\lambda_1) = A(\lambda_2) = 0$. In fact (cf. [2]), such λ may be found in the quadratic extension of the prime field. Then the curve X with function field defined by $L = K(x,y,z)$ with

$$y^2 = x(x-1)(x-\lambda_1), \qquad z^2 = x(x-1)(x-\lambda_2),$$

is of genus 2 with Hasse-Witt matrix 0, as follows from the theorem on observing that the third minimal subfield of L has genus 0. Q.E.D.

The technique used in Corollary 2 permits the construction of other interesting examples. But first, we dispel undue optimism about using it to obtain curves of large genus and 0 Hasse-Witt matrix. Let $p = 7$ and let $L = K(x,y,z,w)$ where $y^2 = x(x-1)(x-2)$, $z^2 = x(x-1)(x+3)$, and $w^2 = x(x-1)(x+1) = x^3 - x$.

Since 2, -3 and -1 are the supersingular invariants modulo 7, each of $K(x,y)$, $K(x,z)$, and $K(x,w)$ are function fields of supersingular elliptic curves and so contribute 0 to the Hasse-Witt matrix of L. However, the minimal subfield $K(x,yzw)$ is of genus 2 and has invertible Hasse-Witt matrix. So L is of genus 5 (other minimal subfields have genus 0) and has Hasse-Witt matrix of rank 2.

We conclude with a family of examples involving vector bundles on curves. For relevant background see [3] and [4]. It is known that in characteristic p there are curves X of genus g carrying vector bundles E of rank 2 such that although every quotient bundle of E has positive degree, E is, nevertheless, not an ample bundle. Such behavior is impossible over the complex numbers. A technical condition which assures the existence of such vector bundles E on X is that the rank σ of the Hasse-

Witt matrix satisfy $\sigma < g - p + 1$. Cf. [5]. The class of curves in the next corollary enjoys the technical property, and so gives an easy construction for a large collection of such examples:

COROLLARY 3. – Let $p > 2$ and consider a Kummer type curve with function field L defined by $L = K(x, y_1, \ldots, y_p)$ where each y_j is such that $K(x, y_j)$ is a supersingular elliptic curve,

$$E_j: \quad y_j^2 = f_j(x) \quad \text{with } \deg(f_j(x)) = 3 \text{ or } 4.$$

Then if σ is the rank of the Hasse-Witt matrix of L and g is the genus of L one has $\sigma < g - p + 1$.

Proof: In fact, it follows from our theorem that $\sigma \leq g - p$. We remark that one can find p such y_j and $f_j(x)$ even though there are only $(p-1)/2$ supersingular invariants. It suffices to take one supersingular $f(x)$, say $f_1(x)$, and then perform $p - 1$ translations on x by elements $t_j \in K$ chosen so that the $f_j(x) = f_1(x - t_j)$ (which remain supersingular) have no common ramification at finite places. Q.E.D.

5. REFERENCES

[1] CARTIER P. – *Sur la rationalité des diviseurs en geometrie algébrique*, «Bulletin Soc. Math. France», 177-251 (1958).

[2] DEURING M. – *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper,* «Abt. Math. Sm. Hamburg», 197-272 (1941).

[3] GRIFFITHS P. and HARRIS I. – *Principles of Algebraic Geometry*, New York, J. Wiley & Sons (1978).

[4] GUNNING R. – *Lectures on Riemann Surfaces*, Princeton U. Press, 1967.

[5] HARTSHORNE R. – *Ample Vector Bundles on Curves*, «Nagoya Math. J.», *43*, 73-80 (1971).

[6] HASSE H. and WITT E. – *Zyklische unverzweigte Erweiterungskörper von Primazahlgrade über ein algebraischen Funktionenkörper, der Charakteristik p*, «Monathft. Math. Phy.», *43*, 477-493 (1936).

[7] IGUSA J. – *On the Transformation Theory of Elliptic Functions*, «Amer. J. Math.», *81*, 436-452 (1959).

[8] MADDEN D. – *Arithmetic in Generalized Artin-Schreier Extensions of k(x)*, «Journ. of Number Theory», *10*, 303-323 (1978).

[9] MILLER L. – *Curves with Invertible Hasse-Witt Matrix*, «Math. Ann.», *197*, 123-5 (1977).

[10] SERRE J.P. – *Sur la topologie des varietés algébriques en characteristique p*, «Sympos. Internac. Topol. Alg. Mexico City», 24-53 (1956).

[11] SUBRAO D. – *The p-rank of Artin-Schreir Curves*, «Manuscripta Math.», *16*, 169-193 (1975).

[12] WEIERSTRASS K. – *Gesammelte Werke, IV*, 135-45 (1905).

[13] YUI N. – *On the Jacobian Variety of the Fermat Curve*, «Journ. of Algebra», *65*, 1-34 (1980).