COMPOSITIO MATHEMATICA

MASAAKI HOMMA

A souped-up version of Pardini's theorem and its application to funny curves

Compositio Mathematica, tome 71, nº 3 (1989), p. 295-302
<http://www.numdam.org/item?id=CM_1989__71_3_295_0>

Compositio Mathematica **71**: 295–302, 1989.

A souped-up version of Pardini's theorem and its application to funny curves

MASAAKI HOMMA

Department of Mathematics, Ryukyu University, Nishihara-cho, Okinawa, 903-01, Japan

Received 29 August 1988

Dedicated to Professor Yukihiro Kodama on his 60th birthday

0. Introduction

Projective geometry over fields of positive characteristic does not behave like the classical projective geometry. For example, when the characteristic of the ground field is positive, a plane curve is not always reflexive, i.e., the dual map from the curve to its dual is not always birational.

In this context, R. Pardini proved the following theorem.

THEOREM (Pardini [4]). *Let C be a smooth curve of degree d in projective plane $\mathbb{P}^2$ over an algebraically closed field of characteristic $p > 2$. Then C is nonreflexive if and only if $p \mid d - 1$ and the equation of C is of the form;*

$$X_1 P_1(X_1^p, X_2^p, X_3^p) + X_2 P_2(X_1^p, X_2^p, X_3^p) + X_3 P_3(X_1^p, X_2^p, X_3^p) = 0,$$

where the P_i are homogeneous of degree $(d - 1)/p$.

On the other hand, the author showed the following result in the previous paper [1].

THEOREM. *Let C be a smooth projective plane curve of degree $d \geqslant 4$ over a field of characteristic $p > 0$. Then the dual curve of C is smooth if and only if $d - 1$ is a power of p and C is projectively equivalent to the curve defined by*

$$X_1^d + X_2^{d-1} X_3 + X_2 X_3^{d-1} = 0.$$

We proved the theorem through complicated calculation. Purposes of this note are:

(1) to give a souped-up version of Pardini's theorem (see, §2, Cor. 2.5) and
(2) to give a conceptual and straightforward proof of our previous theorem, using the souped-up version of Pardini's theorem and a recent result of H. Kaji [2] (see, §3).

1. Hasse-Schmidt differential operators on a polynomial ring

Throughout this section, we fix a polynomial ring $k[X_1, \ldots, X_n]$ over a field k. First we define differential operators $D_i^{(\alpha)}(i \in \mathbb{Z}$ with $1 \leqslant i \leqslant n; \alpha \in \mathbb{N}_0)$, where $\mathbb{N}_0$ is the nonnegative integers.

DEFINITION 1.1. For integers i $(1 \leqslant i \leqslant n)$ and $\alpha \in \mathbb{N}_0$, we define the k-linear endomorphism $D_i^{(\alpha)}$ of $k[X_1, \ldots, X_n]$ by

$$D_i^{(\alpha)}(X_j^m) = \delta_{ij}\binom{m}{\alpha}X_i^{m-\alpha},$$

where δ_{ij} is Kronecker symbol and $\binom{m}{\alpha} = (m!/\alpha!(m-\alpha)!)$.

REMARK 1.2. The following properties hold:

(1) $\alpha!\ D_i^{(\alpha)} = \dfrac{\partial^\alpha}{\partial X_i^\alpha}$;

(2) $[D_i^{(\alpha)}, D_j^{(\beta)}] = 0$;

(3) $D_i^{(\alpha)} D_i^{(\beta)} = \dbinom{\alpha+\beta}{\alpha} D_i^{(\alpha+\beta)}$;

(4) $D_i^{(\alpha)}(G \cdot H) = \sum_{\nu=0}^{\alpha} D_i^{(\nu)}(G) D_i^{(\alpha-\nu)}(H)$.

DEFINITION 1.3. Let $F(X)$ be a homomogeneous polynomial in $k[X_1, \ldots, X_n]$ of degree d and let j be an integer with $0 \leqslant j \leqslant d$. We define the polynomial

$$F^{(j)}(X; Y) \in k[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$$

by

$$F^{(j)}(X; Y) = \sum_{(\alpha)} (D_1^{(\alpha_1)} \ldots D_n^{(\alpha_n)} F)\ Y_1^{\alpha_1} \ldots Y_n^{\alpha_n},$$

where (α) ranges over the set of nonnegative integers $(\alpha_1, \ldots, \alpha_n)$ with $\alpha_1 + \cdots + \alpha_n = j$.

LEMMA 1.4. (0) *$F^{(j)}(X; Y)$ is bihomogeneous of degree $(d-j, j)$.*

(1) $F^{(j)}(X; X) = \dbinom{d}{j} F(X)$

(2) *Let s and t be two variables. Then*

$$F(sX + tY) = \sum_{j=0}^{d} F^{(j)}(X; Y)s^{d-j}t^j.$$

(3) $F^{(j)}(X; Y) = F^{(d-j)}(Y; X)$.

Proof. (0) is trivial by the defintion. To prove (1), it suffices to show the formula when $F(X)$ is a monomial. This case can be proved by using the following formula; for a fixed nonnegative integers $e_1, \ldots, e_n$ with $e_1 + \cdots + e_n = d$, we have

$$\sum_{\substack{(\alpha) \\ \text{with} \\ \alpha_1 + \cdots \alpha_n = j}} \binom{e_1}{\alpha_1} \cdots \binom{e_n}{\alpha_n} = \binom{d}{j}.$$

[This formula obtained by comparing coefficients of λ^j in $(\lambda + 1)^{e_1} \ldots (\lambda + 1)^{e_n}$ and $(\lambda + 1)^d$.]

(2) It also suffices to show the formula when $F(X)$ is a monomial. In this case, the formula is obvious. (3): By (2), we have

$$\sum_{j=0}^{d} (F^{(j)}(X; Y) - F^{(d-j)}(Y; X))\, s^{d-j}t^j = 0.$$

Hence we have $F^{(j)}(X; Y) = F^{(d-j)}(Y; X)$ for any j.

2. A souped-up version of Pardini's theorem

From now on, we work over a field of characteristic $p > 0$.

Throughout of this section, we fix an irreducible curve $C \subset \mathbb{P}^2$ of degree d, given by the equation $F(X_1, X_2, X_3) = 0$.

For a smooth point $P \in C$, we define an integer $m(P)$ ($\geqslant 2$) by the intersection multiplicity of the tangent line $T_P(C)$ and C at P. Let $M(C) = \min\{m(P) \mid P \in \operatorname{Reg} C\}$, where Reg C is the set of smooth points of C. Obviously, $M(C) = m(P)$ if P is a general point of C. It is known that if $M(C) > 2$, then $M(C)$ is a power of p and $m(P)$ or $m(P) - 1$ is divided by $M(C)$. In this case, $M(C)$ coincides with the inseparable degree of the dual map $C \to C^*$, where C^* is the dual curve of C. (see, for example, [1].)

PROPOSITION 2.1. *Let us fix an integer $m \geqslant 3$. Let $P = (x) = (x_1, x_2, x_3)$ be a smooth point of C. Then $m(P) \geqslant m$ if and only if $F^{(1)}(x; Y) \mid F^{(i)}(x; Y)$ as* *polynomials in* $(Y) = (Y_1, Y_2, Y_3)$ *for any* i *with* $2 \leqslant i \leqslant m-1$.

Proof. Let $(y) \in \mathbb{P}^2$ with $(y) \neq (x)$ and let $l((x),(y))$ the line joining (x) and (y). Then the divisor on C cut out by the line $l((x),(y))$ is equal to $\Sigma_{(s:t)} s(x) + t(y)$, where $(s:t)$ ranges over the zeros counting multiplicities of the following equation:

$$(*)\left(\begin{aligned} 0 &= F(s(x) + t(y)) \\ &= F(x)s^d + F^{(1)}(x;y)s^{d-1}t + \cdots \\ &\qquad + F^{(m-1)}(x;y)s^{d-m+1}t^{m-1} + \cdots + F^{(d)}(y)t^d. \end{aligned}\right.$$

Therefore, choosing (y) on $T_p(C)$, we have

$$m(P) \geqslant m \Leftrightarrow (1:0) \text{ is a root of } (*) \text{ with multiplicity } \geqslant m$$

$$\Leftrightarrow F(x) = F^{(1)}(x;y) = \cdots = F^{(m-1)}(x;y) = 0.$$

Note that the condition $F(x) = F^{(1)}(x;y) = 0$ is satisfied automatically, because $P = (x) \in C$ and $(y) \in T_P(C)$. Hence $m(P) \geqslant m$ if and only if $F^{(i)}(x;Y)$ (as a polynomial in Y) vanishes on $T_P(C)$ for $2 \leqslant \forall i \leqslant m-1$. Since, $T_P(C)$ is the line determined by $F^{(1)}(x;Y) = 0$, the above condition is equivalent to the condition that $F^{(1)}(x;Y) \mid F^{(i)}(x;Y)$ for $2 \leqslant \forall i \leqslant m-1$.

To prove our main theorem, we need the following lemma, whose proof is easy and omitted.

LEMMA 2.2. *Let* C_1 *and* C_2 *be complete smooth curves and let* D *and* E *be effective divisors on* $C_1 \times C_2$ *such that*

(1) *D has no components of type* $\{P\} \times C_2$;
(2) *for any* $P \in C_1, D \cap \{P\} \times C_2 \prec E \cap \{P\} \times C_2$ *as divisors on* $C_2 \simeq \{P\} \times C_2$.
Then we have $C \prec E$.

THEOREM 2.3. *Suppose that C is smooth. Let* $q = p^e (e > 0$ *if* $p \neq 2$; $e > 1$ *if* $p = 2)$. *Then* $M(C) \geqslant q$ *if and only if* $F^{(i)}(X;Y) = 0$ *(as a polynomial in* (X) *and* (Y)*) for* $2 \leqslant \forall i \leqslant q-1$.

Proof. Proposition 2.1 implies the "if" part. We prove the "only if" part. Suppose the contrary: there exists i $(2 \leqslant i \leqslant q-1)$ with $F^{(i)}(X;Y) \neq 0$. Let H be the divisor on $\mathrm{P}^2 \times \mathrm{P}^2$ determined by the equation $F^{(i)}(X;Y) = 0$. First we show that $H \cap C \times C$ is a divisor on $C \times C$. To prove this, by the irreducibilty of $C \times C$, and by the unmixedness theorem, it suffices to show that $H \not\supset C \times C$. Suppose that $H \supset C \times C$. Restricting the both sides of $H \supset C \times C$ to $C \times \{P\}$, we have that $F^{(i)}(X;y)$ vanishes on C. Since $\deg_X F^{(i)}(X;y) = d - i < d = \deg C$, we have $F^{(i)}(X;y) = 0$ as a polynomial in (X). This holds for any $y \in C$. Hence, putting

$$F^{(i)}(X;Y) = \sum_{(\gamma)} f_\gamma(Y) X^{\gamma_1} X^{\gamma_2} X^{\gamma_3},$$

we have $f_\gamma(Y) = 0$ on C. Since $\deg f_\gamma(Y) = i < d$, we have $f_\gamma(Y) = 0$ as a polynomial in (Y). Hence we have $F^{(i)}(X;Y) = 0$, which is a contradiction.

Since $F^{(1)}(x;Y)$ is an equation of the (embedded) tangent line to C at (x) if $(x) \in C$, the polynomial $F^{(1)}(X;Y)$ is nontrivial. Therefore, by an argument similar to the one above, the equation $F^{(1)}(X;Y) = 0$ determines a divisor, say D, on $C \times C$.

Let $E = H \cap C \times C$. Since C is smooth, D has no components of type $\{x\} \times C$ (because $F^{(1)}(x;Y) = \Sigma_{i=1}^{3} (\partial F/\partial X_i)(x) Y_i$), and since $F^{(1)}(x;Y) \mid F^{(i)}(x;Y)$ (by Proposition 2.1), we have

$$D \cap \{x\} \times C \prec E \cap \{x\} \times C$$

for any $(x) \in C$. Therefore $D < E$ by Lemma 2.2. Hence, for any point $(y) \in C$, $D \cdot C \times \{y\} \prec E \cdot C \times \{y\}$ on $C \times \{y\} \simeq C$. This is impossible, because

$$\deg D \cdot C \times \{y\} = \deg_X F^{(1)}(X;y) \cdot d = (d-1)d.$$

$$\deg E \cdot C \times \{y\} = \deg_X F^{(i)}(X;y) \cdot d = (d-i)d.$$

Hence we have $F^{(i)}(X;Y) = 0$ for $2 \leqslant \forall i \leqslant q-1$.

COROLLARY 2.4 (Pardini). *Suppose that C is smooth. If $M(C) > 2$, then $M(C) \mid d-1$.*

Proof. Since $M(C)$ is a power of p and $S(C)M(C)d^* = d(d-1)$, where $S(C)$ is the separable degree of the dual map $C \to C^*$ and $d^* = \deg C^*$ (see, for example, [1] the proof of 5.1), it suffices to show $p \mid d-1$. One can prove this by using our theorem and an argument similar to the proof of ([4], Corollary 2.2). □

COROLLARY 2.5. *Let C be a smooth plane curve of degree d. Let $q = p^e$ ($e > 0$ if $p > 2$; $e > 1$ if $p = 2$). Then $M(C) \geqslant q$ if and only if q divides $d-1$ and there are three homogeneous polynomials $P_1, P_2, P_3 \in k[X_1, X_2, X_3]$ of degree $(d-1)/q$ such that*

$$F(X_1, X_2, X_3) = \sum_{i=1}^{3} P_i(X_1^q, X_2^q, X_3^q) X_i.$$

Proof. Since $M(C)$ is a power of p if $M(C) \geqslant q$, the assumption $M(C) \geqslant q$ implies $q \mid d-1$ (by Corollary 2.4). So it suffices to show the assertion under the condition $q \mid d-1$. Say $(d-1)/q = r$. From Theorem 2.3, $M(C) \geqslant q$ if and only if

$$D^{(\alpha_1)}D^{(\alpha_2)}D^{(\alpha_3)}F = 0$$

for any triples $(\alpha_1, \alpha_2, \alpha_3)$ with $2 \leqslant \alpha_1 + \alpha_2 + \alpha_3 \leqslant q-1$. Writing

$$F = \sum_{\beta_1+\beta_2+\beta_3=d} c_{(\beta)} X_1^{\beta_1} X_2^{\beta_2} X_3^{\beta_3},$$

the above condition means that if $c_{(\beta_1,\beta_2,\beta_3)} \neq 0$ then

$$(A)\begin{cases} \binom{\beta_1}{\alpha_1}\binom{\beta_2}{\alpha_2}\binom{\beta_3}{\alpha_3} \equiv 0 \mod p \\ \text{for any } (\alpha_1,\alpha_2,\alpha_3) \text{ with } 2 \leqslant \alpha_1+\alpha_2+\alpha_3 \leqslant q-1. \end{cases}$$

The condition (A) is equivalent to the condition:

$$(B)\begin{cases} \text{there is a permutation } \{i,j,k\} \text{ of } \{1,2,3\} \text{ and integers } r_i,\ r_j,\ r_k \\ \text{such that} \\ \beta_i = r_i q + 1 \\ \beta_j = r_j q \\ \beta_k = r_k q \\ r_i + r_j + r_k = r. \end{cases}$$

To prove this, we use the following lemma.

LEMMA 2.6. *Let u and v be nonnegative integers and p a prime number. Expand u and v by p as follows:*

$$u = a_0 + a_1 p + \cdots + a_e p^e \quad (0 \leqslant a_i < p).$$
$$v = b_0 + b_1 p + \cdots + b_e p^e \quad (0 \leqslant b_i < p).$$

Then $\binom{u}{v} \not\equiv 0 \bmod p$ if and only if $a_i \geqslant b_i$ for $i = 0, 1, \ldots, e$.

Proof. See Schmidt [5].

Let us continue the proof of Corollary 2.5. Assume that the condition (A) is satisfied for a fixed triple $(\beta_1, \beta_2, \beta_3)$ with $\beta_1+\beta_2+\beta_3 = rq+1$. Put $\beta_\nu = r_\nu q + r'_\nu$ $(0 \leqslant r'_\nu < q-1)$ for $\nu = 1, 2, 3$. Suppose that some r'_ν, say r'_1, is greater than 1. Then we may put $\alpha_1 = r'_1$, $\alpha_2 = \alpha_3 = 0$ in (A), and then we have

$$\binom{\beta_1}{\alpha_1}\binom{\beta_2}{\alpha_2}\binom{\beta_3}{\alpha_3} = \binom{r_1 q + r'_1}{r'_1} \not\equiv 0 \mod p,$$

by Lemma 2.6. This is a contradiction. Hence we have $r_\nu = 0$ or 1 for any $\nu = 1, 2, 3$. Since $\beta_1 + \beta_2 + \beta_3 = rq + 1$, we have $r'_1 + r'_2 + r'_3 \equiv 1 \bmod q$. Recall $q = p^e$ with $e > 0$ if $p > 2$ or $e > 1$ if $p = 2$. Hence we have that there is a permutation $\{i, j, k\}$ of $\{1, 2, 3\}$ such that $r'_i = 1$, $r'_j = r'_k = 0$. So the condition (A) implies (B). Conversely, (B) implies (A) by Lemma 2.6. Therefore the equivalence of the two conditions has been established. This completes the proof.

3. An application to funny curves

In this section, we give another proof of our previous theorem which is stated in Introduction.

Let C be a smooth plane curve of degree $d \geqslant 4$ over an algebraically closed field of characteristic $p > 0$.

First we review our previous proof. The proof divides into two parts. The first one is to show that

(I) if C^* is smooth, then $M(C) = d - 1$. (Hence $M(C)$ is a power of p, say q.)

The second one is to show that

(II) if $M(C) = d - 1 = q$, then C is projectively equivalent to the curve defined by $X_1^{q+1} + X_2^q X_3 + X_2 X_3^q = 0$.

Our new proof is as follows. Concerning the first step, we can use a nice theorem by H. Kaji [2], which is the answer to the problem posed by Kleiman ([3], page 342).

KAJI'S THEOREM (a restricted version). *If C is a smooth plane curve of degree $\geqslant 4$, then $S(C) = 1$, where $S(C)$ is the separable degree of the dual map $C \to C^*$.*

Leg g (resp. g^*) be the genus of C (resp. C^*) and d (resp. d^*) the degree of C (resp. C^*). Since both C and C^* are smooth plane curve, we have $g = \frac{1}{2}(d-1)(d-2)$ and $g^* = \frac{1}{2}(d^*-1)(d^*-2)$. Thanks to Kaji's theorem, we have $g = g^*$ and hence $d = d^*$. Since $S(C)M(C)d^* = d(d-1)$, we have $M(C) = d - 1$.

Next, we show (II). By Corollary 2.5, we have that there are three linear polynomials P_1, P_2, P_3 such that C is defined by the equation $\Sigma_{i=1}^3 P_i(X_1^q, X_2^q, X_3^q)X_i = 0$. By an argument similar to that of Pardini ([4], the proof of 3.7), we can show that such equations are projectively equivalent to each other. In particular, the curve C is projectively equivalent to the curve with

$$X_1^{q+1} + X_2^q X_3 + X_2 X_3^q = 0.$$

This completes the proof.

References

1. M. Homma, Funny plane curves in characteristic $p > 0$, *Comm. Algebra* 15 (1987) 1469–1501.
2. H. Kaji, On the Gauss map of space curves in characteristic p, to appear in *Comp. Math.*
3. S.L. Kleiman, Intersection theory and enumerative geometry: A decade review, *Proc. of Symposia in Pure Math.* 46, Amer. Math. Soc., (1987) 321–370.
4. R. Pardini, Some remarks on plane curves over fields of finite characteristic, *Comp. Math.* 60 (1986) 3–17.
5. F.K. Schmidt, Die Wronskisch Determinante in belebigen differenzierbaren Funktionenkörpern, *Math. Z.* 45 (1939) 62–74.

Note added in proof. After the paper was submitted, the author received a preprint from A. Hefez: Nonreflexive curves (to appear in Comp. Math.). He found a proof of Corollary 2.5 independently of the author.