SUBALGEBRAS OF THE POLYNOMIAL ALGEBRA IN POSITIVE CHARACTERISTIC AND THE JACOBIAN

ALEXEY V. GAVRILOV

Let \( k \) be a field of characteristic \( p > 0 \) and \( R \) be a subalgebra of \( k[X] = k[x_1, \ldots, x_n] \). Let \( J(R) \) be the ideal in \( k[X] \) defined by \( J(R) \Omega^n_{k[X]/k} = k[X] \Omega^n_R/k \). It is shown that if it is a principal ideal then \( J(R)^q \subset R[x_1^p, \ldots, x_n^p] \), where \( q = p^n(p-1)/2 \).

Key words: Polynomial ring; Jacobian; generalized Wronskian.

2000 Mathematical Subject Classification: 13F20; 13N15.

1. INTRODUCTION

Let \( k \) be a field and \( k[X] = k[x_1, \ldots, x_n] \) be the polynomial ring. For the most of the paper the number \( n \geq 1 \) and the basis \( X = \{x_1, \ldots, x_n\} \) are fixed. Let \( R \) be a subalgebra of \( k[X] \). Denote by \( J(R) \) the ideal in \( k[X] \) generated by the Jacobians of sets of elements of \( R \) (a formal definition will be given below). The main result is the following theorem.

Theorem Let \( k \) be a field of characteristic \( p > 0 \) and \( R \) be a subalgebra of \( k[X] \). If \( J(R) \) is a principal ideal then

\[ J(R)^q \subset R[X^p], \]

where \( R[X^p] = R[x_1^p, \ldots, x_n^p] \) and \( q = p^n(p-1)/2 \).

Presumably the statement holds for a nonprincipal ideal as well. However, a proof of this conjecture probably requires another technique.

Corollary Let \( k \) be a field of characteristic \( p > 0 \) and \( R \) be a subalgebra of \( k[X] \). If \( J(R) = k[X] \) then

\[ R[X^p] = k[X]. \]

Nousiainen [2] proved this in the case \( R = k[F] = k[f_1, \ldots, f_n] \) (see also [1]). In this case the condition \( J(R) = k[X] \) is equivalent to \( j(F) \in k^X \), where \( j(F) \) is the Jacobian of the polynomials \( f_1, \ldots, f_n \). Thus, Nousiainen’s result is a positive characteristic analogue of the famous Jacobian conjecture: if \( \text{char}(k) = 0 \) and \( j(F) \in k^X \) then \( k[F] = k[X] \). The zero characteristic analogue of Corollary is obviously false. (Consider, for example, the subalgebra \( R = k[t-t^2, t-t^3] \) of \( k[t] \). Then \( R \neq k[t] \) but \( J(R) = k[t] \).

Nousiainen’s method is based on properties of the derivations \( \frac{\partial}{\partial t} \in \text{Der}(k[X]) \), which are the natural derivations of \( k[F] \) extended to \( k[X] \). Probably his method can be applied to a more general case as well. However, our approach is based on the calculation of generalized Wronskians of a special kind. This calculation may be an interesting result in itself.
2. PRELIMINARIES AND NOTATION

An element \( \alpha = (\alpha_1, \ldots, \alpha_n) \) of \( N^n_0 \), where \( N_0 \) denotes the set of non-negative integers, is called a multiindex. For \( F \in k[X]^n \) and two multiindices \( \alpha, \beta \in N^n_0 \) we will use the following notation

\[
|\alpha| = \sum_{i=1}^{n} \alpha_i, \quad \alpha! = \prod_{i=1}^{n} \alpha_i!, \quad \binom{\alpha}{\beta} = \prod_{i=1}^{n} \binom{\alpha_i}{\beta_i},
\]

\[
X^\alpha = \prod_{i=1}^{n} x_i^{\alpha_i}, \quad F^\alpha = \prod_{i=1}^{n} f_i^{\alpha_i}, \quad \partial^\alpha = \prod_{i=1}^{n} \partial_i^{\alpha_i},
\]

where \( \partial_i = \frac{\partial}{\partial x_i} \in \text{Der}(k[X]) \).

In several places multinomial coefficients will appear, denoted by \( \binom{\beta_1, \ldots, \beta_k}{\alpha} \), where \( \alpha, \beta_1, \ldots, \beta_k \in N^n_0 \) and \( \alpha = \beta_1 + \cdots + \beta_k \). They are defined exactly by the same way as the binomial ones. The set of multiindices possess the partial order; by definition, \( \alpha \leq \beta \) iff \( \alpha_i \leq \beta_i \) for all \( 1 \leq i \leq n \). For the sake of convenience we introduce the ”diagonal” intervals \( [k, m] = \{ \alpha \in N^n_0 : k \leq \alpha_i \leq m, 1 \leq i \leq n \} \), where \( k, m \in N_0 \).

Let \( R \) be a subalgebra of \( k[X] \). Since \( \Omega^n_{k[X]/k} \) is a free cyclic module, we can make the following definition.

**Definition 1** Let \( R \) be a subalgebra of \( k[X] \), where \( k \) is a field. The Jacobian ideal of \( R \) is the ideal \( J(R) \) in \( k[X] \) defined by the equality

\[
J(R)\Omega^n_{k[X]/k} = k[X]\Omega^n_{R/k},
\]

where \( \Omega^n_{R/k} \) is considered a submodule of \( \Omega^n_{k[X]/k} \) over \( R \).

The exact meaning of the words ”is considered a submodule” is that we write \( k[X]\Omega^n_{R/k} \) instead of \( k[X]\text{Im}(\Omega^n_{R/k} \to \Omega^n_{k[X]/k}) \). This is a slight abuse of notation, because the natural \( R \)-module homomorphism \( \Omega^n_{R/k} \to \Omega^n_{k[X]/k} \) is not injective in general.

There is also a more explicit definition. For \( F \in k[X]^n \), the Jacobian matrix and the Jacobian are defined by

\[
JF = \left\| \frac{\partial f_i}{\partial x_j} \right\|_{1 \leq i, j \leq n} \in M(n, k[X]), \quad j(F) = \det JF \in k[X].
\]

The module \( k[X]\Omega^n_{R/k} \) is generated by \( df_1 \wedge \cdots \wedge df_n = j(F)dx_1 \wedge \cdots \wedge dx_n \), where \( F = (f_1, \ldots, f_n) \in R^n \). Thus

\[
J(R) = \{ j(F) : F \in R^n \},
\]

where \( \langle S \rangle \) denotes the ideal in \( k[X] \) generated by a set \( S \). It is an easy consequence of the chain rule that the Jacobian ideal of a subalgebra generated by \( n \) polynomials is a principal ideal:

\[
J(\langle k[F] \rangle) = k[X]j(F), \quad F \in k[X]^n.
\]

Clearly, the ring \( k[X] \) is a free module over \( k[X^p] \) of rank \( p^n \): the set of monomials \( \{ X^\alpha : \alpha \in [0, p-1] \} \) is a natural basis of this module. This construction became important when \( \text{char}(k) = p \) (note that in this case \( k[X^p] \) does not depend on the choice of generators of \( k[X] \) i.e. it is an invariant).
Definition 2 Let $k$ be a field of characteristic $p > 0$ and $F \in k[X]^n$. The matrix $U(F) \in M(p^n, k[X^p])$ is defined by

$$F^\alpha = \sum_{\beta \in [0, p-1]} U(F)_{\alpha \beta} X^\beta, \quad \alpha \in [0, p-1].$$

3. Generalized Wronskians

In this section we compute generalized Wronskians of a special form. The key tool for this computation is the following simple lemma.

Lemma 1 Let $R$ be a ring and $f \in R$. If $D_1, \ldots, D_l \in \text{Der}(R)$ and if $m \geq l \geq 0$ then

$$\sum_{k=0}^{m} \binom{m}{k} (-f)^{m-k} D_1 \ldots D_l f^k = \begin{cases} 0 & \text{if } m > l \\ l! \prod_{k=1}^{l} D_k f & \text{if } m = l \end{cases} \quad (1)$$

In the case $l = 0$ there are no derivations and the formula becomes

$$\sum_{k=0}^{m} \binom{m}{k} (-f)^{m-k} f^k = \begin{cases} 0 & \text{if } m > 0 \\ 1 & \text{if } m = 0 \end{cases}$$

which is obviously true.

Proof

Denote

$$S_{m,t} = \sum_{k=0}^{m} \binom{m}{k} (-f)^{m-k} D_1 \ldots D_l f^k.$$ 

This sum coincides with the left hand side of (1), except for the reverse order of the derivations. We have $S_{0,0} = 1$ and $S_{m,0} = 0, m > 0$. The following equality can easily be verified

$$S_{m+1,t+1} = D_{t+1} S_{m+1,t} + (m+1)(D_{t+1} f) S_{m,t}.$$ 

By induction on $l$, for $m > l$ we have $S_{m,l} = 0$, and

$$S_{l,l} = l(D_l f) S_{l-1,l-1} = l! \prod_{k=1}^{l} D_k f.$$ 

□

Let $R$ be a ring. Denote by $R[Z_{ij}]$ the polynomial ring in the $n^2$ indeterminates $Z_{ij}, 1 \leq i, j \leq n$. If $h \in R[Z_{ij}]$ and $A \in M(n, R)$ then $h(A)$ denotes the result of the substitution $Z_{ij} \mapsto A_{ij}$.

Proposition 1 For any $r \geq 1$ there exists the homogeneous polynomial $H_r \in Z[Z_{ij}]$ of degree $\frac{nr^n(n-1)}{2}$ with the following property. Let $R$ be a ring with derivations $D_1, \ldots, D_n \in \text{Der}(R)$. If $[D_i, D_j] = 0$, for all $i, j$, then for any $F = (f_1, \ldots, f_n) \in R^n$ the following equality holds

$$\det W = H_r(JF),$$

where $W \in M(r^n, R)$ and $JF \in M(n, R)$ are defined by

$$W_{\alpha \beta} = D^\alpha F^\beta, \quad \alpha, \beta \in [0, r-1]; \quad (JF)_{ij} = D_i f_j, \quad 1 \leq i, j \leq n.$$
Here $JF$ is an obvious generalization of the Jacobian matrix. The determinant $\det W$ is a generalized Wronskian of the polynomials $F^\beta$.

**Proof**

By the Leibniz formula,

$$W_{\alpha\beta} = \sum_{\gamma} \binom{\beta}{\alpha} \prod_{i=1}^{n} (D^\theta f_i^\gamma),$$

where $\theta^1, \ldots, \theta^n \in \mathbb{N}_0^n$ and the sum is taken over the multiindices satisfying the equality $\sum_{i=1}^{n} \theta^i = \alpha$.

Let $T \in M(r^n, R)$ be determined by

$$T_{\alpha\beta} = \binom{\beta}{\alpha} (-F)^{\beta-\alpha}, \quad \alpha, \beta \in [0, r - 1].$$

Let $W' = WT \in M(r^n, R)$. Then

$$W'_{\alpha\beta} = \sum_{\gamma} W_{\alpha\gamma} T_{\gamma\beta} = \sum_{\gamma} \binom{\beta}{\alpha} \prod_{i=1}^{n} S_r(\beta_i, \theta_i),$$

where

$$S_r(m, \theta) = \sum_{k=0}^{m} \binom{m}{k} (-f_i)^{m-k} \prod_{j=1}^{n} (D_j f_j)^{\theta_j}.$$

By Lemma 1, if $m \geq |\theta|$ then

$$S_r(m, \theta) = \begin{cases} 0 & \text{if } m > |\theta| \\ m! \prod_{j=1}^{n} (D_j f_j)^{\theta_j} & \text{if } m = |\theta| \end{cases}$$

Thus if the product in the right hand side of (3) is not zero then $\beta_i \leq |\theta^i|$ for all $1 \leq i \leq n$. The latter implies $|\beta| \leq |\alpha|$. It follows that if $|\alpha| < |\beta|$ then $W'_{\alpha\beta} = 0$. In the case $|\alpha| = |\beta|$ the product is zero unless $\beta_i = |\theta^i|, 1 \leq i \leq n$. Thus, if $|\alpha| = |\beta|$ then

$$W'_{\alpha\beta} = \binom{\beta}{\alpha} \sum_{|\theta^1| = \beta_1} \cdots \sum_{|\theta^n| = \beta_n} \binom{\alpha}{\theta^1 \ldots \theta^n} \prod_{i=1}^{n} \prod_{j=1}^{n} (D_j f_j)^{\theta_j}.$$  \hfill (4)

Put the multiindices in a total order compatible with the partial order (e.g., in the lexicographic order). Then the matrix $T$ becomes upper triangular with the unit diagonal, hence $\det T = 1$. The matrix $W'$ becomes block lower triangular, hence $\det W'$ is equal to the product of the $nr - n + 1$ determinants of the blocks. Each block determinant $\det \left| W'_{\alpha\beta} \right|_{|\alpha|=|\beta|=l}$ (where $0 \leq l \leq nr - n$) is by (4) a homogeneous polynomial in the variables $D_j f_j$ of degree $s_l$, where $s_l$ is the size of the block. Clearly $s_l = \# \left\{ \alpha \in \mathbb{N}_0^n : \alpha \in [0, r - 1], |\alpha| = l \right\}$. The determinant $\det W = \det W'$ is then a homogeneous polynomial of degree

$$\sum_{l=0}^{nr-n} s_l = \sum_{\alpha \in [0, r - 1]} |\alpha| = \frac{nr^n(r - 1)}{2}.$$  \hfill (5)

One can see from (5) that all the coefficients of this polynomial are integers. \hfill $\square$

When $n = 1$, the determinant in the left hand side of (2) is a common Wronskian $W(1, f, \ldots, f^{r-1})$. In this case $H_r$ is a polynomial in one variable, which can be easily computed. The matrix $W' \in M(r, R)$ is a triangular matrix with the diagonal
elements \( W'_{k,k} = k!(DF)^k \), \( 0 \leq k \leq r - 1 \), hence \( \det W = \det W' \) is equal to the product of these elements. So, we have the following equality

\[
\det \left| \begin{array}{c}
D^k f^l \\
k \leq k, l \leq r - 1
\end{array} \right| \prod_{k=1}^{r-1} k! = (DF)^\left(\frac{r(r-1)}{2}\right) \prod_{k=1}^{r-1} k!
\]

(5)

where \( f \in R \) and \( D \in \text{Der}(R) \).

The formula (5) may be considered a consequence of the known Wronskian chain rule [3, Part Seven, Ex. 56].

4. THE DETERMINANT

For the rest of the paper \( \k \) is a field of fixed characteristic \( p > 0 \), and \( q = \frac{n^p(p-1)}{2} \).

For \( F \in \k[X]^n \), denote

\[
\Delta(F) = \det U(F) \in \k[X^q].
\]

Our aim is to compute this determinant.

Denote by \( \phi_F \) the algebra endomorphism

\[
\phi_F \in \text{End}(\k[X]), \phi_F : x_i \mapsto f_i, 1 \leq i \leq n.
\]

**Lemma 2** Let \( F, G \in \k[X]^n \). Let \( \phi_F G = (\phi_F G_1, \ldots, \phi_F G_n) \in \k[X]^n \). Then

\[
\Delta(\phi_F G) = (\phi_F \Delta(G)) \cdot \Delta(F).
\]

(6)

**Proof**

By definition,

\[
G^\alpha = \sum_{\gamma} U(G)_{\alpha \gamma} X^\gamma, \alpha \in [0, p-1].
\]

Applying the endomorphism \( \phi_F \) to the both sides of this equality, we get

\[
(\phi_F G)^\alpha = \sum_{\gamma} (\phi_F U(G)_{\alpha \gamma}) F^\gamma = \sum_{\beta \gamma} (\phi_F U(G)_{\alpha \gamma}) U(F)_{\gamma \beta} X^\beta.
\]

On the other hand,

\[
(\phi_F G)^\alpha = \sum_{\beta} U(\phi_F G)_{\alpha \beta} X^\beta.
\]

As the monomials \( X^\beta \) form a basis, the coefficients are the same:

\[
U(\phi_F G) = (\phi_F U(G))U(F).
\]

Taking the determinant, we have (6). \( \square \)

If \( F \in \k[X]^n \) consists of linear forms, then

\[
F_i = \sum_{j=1}^{n} A_{ij} X_j, 1 \leq i \leq n
\]

for some matrix \( A \in M(n,k) \). We write this as

\[
F = AX;
\]

in this notation \( X \) and \( F \) are considered column vectors.

**Lemma 3** Let \( A \in M(n,k) \). If \( F = AX \), then

\[
\Delta(F) = (\det A)^q.
\]

(7)

**Proof**
Let $A, B \in M(n, k)$. Let $G = BX$ and $F = AX$. Then $\phi_F G = BAX$. One can see that the elements of the matrix $U(BX)$ belong to the field $k$. It follows that $\phi_F \Delta(BX) = \Delta(BX)$, and by (6) we have
\[
\Delta(BAX) = \Delta(BX)\Delta(AX).
\]
It is well known that any matrix over a field is a product of diagonal matrices and elementary ones. Thus, because of the latter equality, it is sufficient to prove (7) for diagonal and elementary matrices. If $A$ is elementary, then for some $j \neq k$ we have $f_j = x_j + \lambda x_k$, where $\lambda \in k$, and $f_i = x_i$, $i \neq j$. Then $U(F)$ is a (upper or lower) triangular matrix with the unit diagonal, hence $\Delta(F) = \det A = 1$, and (7) holds. If $A$ is diagonal then $f_i = A_{ii}x_i$, $1 \leq i \leq n$. In this case $U(F)$ is diagonal as well and $U(F)_{ii} = \prod_{k=1}^{n} A_{ii}$. The equality (7) can be easily checked.

**Lemma 4** Let $F \in k[X]^n$ and $W = \|\partial^\alpha F^\beta\|_{\alpha, \beta \in [0, p-1]}$. Then
\[
\det W = c_p^n \Delta(F),
\]
where $c_p = \prod_{k=1}^{p-1} k! \in k^\times$.

**Proof**
Denote $Q = \|\partial^\alpha X^\beta\|_{\alpha, \beta \in [0, p-1]} \in M(p^n, k[X])$. This is a Kronecker product
\[
Q = Q_1 \otimes \cdots \otimes Q_n; Q_i = \|\partial^\alpha x_i^\beta\|_{0 \leq \alpha, \beta \leq p-1} \in M(p, k[x_i]), 1 \leq i \leq n.
\]
Applying the equality (5) to the rings $k[x_i]$, we have $\det Q_i = c_{p, i} = 1 \leq i \leq n$. Then
\[
\det Q = \prod_{i=1}^{n} (\det Q_i)^{p_{n-1}} = c_p^n p^{n-1} = c_p^n.
\]
The elements of $U(F)$ belong to the kernels of derivations $\partial_i$, hence
\[
\partial^\alpha F^\beta = \sum_{\gamma} U(F)_{\beta, \gamma} \partial^\alpha X^\gamma.
\]
This can be written in the matrix notation as
\[
W = QU(F)^T.
\]
The formula is a consequence. \qed

5. PROOF OF THE THEOREM

**Proposition 2** Let $F \in k[X]^n$. Then
\[
\Delta(F) = j(F)^q.
\]

**Proof**
Let $W = \|\partial^\alpha F^\beta\|_{\alpha, \beta \in [0, p-1]} \in M(p^n, k[X])$. By Lemma 4 and Proposition 1,
\[
\det W = c_p^n \Delta(F) = H_p(JF).
\]
If $A \in M(n, k)$ and $F = AX$ then $JF = A$, hence
\[
H_p(A) = c_p^n (\det A)^q
\]
by Lemma 3. Without loss of generality, $k$ is infinite. The latter equality holds for any matrix, hence it is valid as a formal equality in the ring $k[Z_{ij}]$. Thus
\[
H_p(JF) = c_p^n (\det JF)^q = c_p^n j(F)^q.
\]
\qed
We have the following corollary, proved first by Nousiainen [2].

**Corollary** Let \( k \) be a field of characteristic \( p > 0 \) and \( F \in k[X]^n \). Then the set \( \{ F_\alpha : \alpha \in [0, p-1] \} \) is a basis of \( k[X] \) over \( k[X^p] \) if and only if \( j(F) \in k^\times \).

**Proposition 3** Let \( F \in k[X]^n \). Then
\[
k[X]j(F)^q \subset k[X^p][F].
\]

**Proof**
From linear algebra we have
\[
\Delta(F)U(F)^{-1} = \text{adj } U(F) \in M(p^n, k[X^p]).
\]
Thus
\[
j(F)^q X_\alpha = \Delta(F)X_\alpha = \Delta(F) \sum_\beta U(F)_{\alpha\beta}^{-1} F_\beta \in k[X^p][F]
\]
for any multiindex \( \alpha \in [0, p-1] \). The set \( \{ X_\alpha \} \) is a basis of \( k[X] \) over \( k[X^p] \), hence the inclusion follows.

**Proof of Theorem**
We have
\[
J(R) = \langle \{ j(F) : F \in R^n \} \rangle = \langle P \rangle, \quad P \in k[X].
\]
If \( P = 0 \), the statement is trivial. Suppose \( P \neq 0 \). Since \( P \in J(R) \), there exists a number \( m \geq 1 \), such that
\[
P = \sum_{i=1}^m g_i j(F_i),
\]
where \( g_i \in k[X] \), \( F_i \in R^n \), \( 1 \leq i \leq m \). On the other hand, \( J(R) \subset \langle P \rangle \), hence
\[
\mu_i = j(F_i)/P \in k[X], \quad 1 \leq i \leq m.
\]
Consider the following two ideals:
\[
J = \{ f \in k[X] : k[X]f \subset R[X^p] \}; \quad I = \langle \mu_1^q, \ldots, \mu_m^q \rangle.
\]
By Proposition 3, \( \mu_i^q P^q = j(F_i)^q \in J \) for all \( 1 \leq i \leq m \), hence
\[
IP^q \subset J.
\]
Raising the equality \( \sum_{i=1}^m g_i \mu_i = 1 \) to the power \( qm \), it follows that \( 1 \in I \), whence \( P^q \in J \).

**ACKNOWLEDGMENT**
The author thanks Prof. Arno van den Essen for giving him the information about the Nousiainen’s preprint.

**REFERENCES**
[1] H. Bass, E.H. Connell, D. Wright. The Jacobian Conjecture: Reduction of degree and formal expansion of the inverse, Bull. A.M.S. 7(2)(1982) 287-330.
[2] P. Nousiainen. On the Jacobian problem in positive characteristic. Pennsylvania State Univ. preprint. 1981
[3] G. Polya, G. Szegö. Problems and Theorems in Analysis, Vol II. Springer-Verlag. 1976

E-mail address: gavrilov198@gmail.com