THE TOTAL REDUCIBILITY ORDER OF A POLYNOMIAL IN TWO VARIABLES

BY

YOSEF STEIN

Center for Technological Education Holon affiliated with Tel Aviv University, 52 Golomb St., P.O.B. 305, Holon 58102, Israel

ABSTRACT

Let K be an algebraically closed field of characteristic zero. For $A \in K[x, y]$ let $\sigma(A) = \{\lambda \in K : A - \lambda \text{ is reducible}\}$. For $\lambda \in \sigma(A)$ let $A - \lambda = \Pi_{i=1}^{n(\lambda)} A_{i\lambda}^{k_{i\lambda}}$ where $A_{i\lambda}$ are distinct primes. Let $\rho_\lambda(A) = n(\lambda) - 1$ and let $\rho(A) = \Sigma_{\lambda \in \sigma(A)} \rho_\lambda(A)$. The main result is the following:

THEOREM. *If $A \in K[x, y]$ is not a composite polynomial, then $\rho(A) < \deg A$.*

Introduction

Let K be an algebraically closed field of characteristic zero. For $P, Q \in K[x, y]$ let

$$[P, Q] = \frac{\partial P}{\partial x}\frac{\partial Q}{\partial y} - \frac{\partial P}{\partial y}\frac{\partial Q}{\partial x}.$$

For $F \in K(x, y)$ set $D_P(F) = [P, f]$; D_P is a derivation of both $K[x, y]$ and $K(x, y)$. The operation $[\ ,\ ]$ imposes a Lie-algebra structure on $K[x, y]$.

The main goal of this paper is to study the interplay between this Lie-algebra structure and the structure of $K[x, y]$ as a polynomial ring. The operators D_P play a prominent role in studying seemingly purely algebraic properties of $K[x, y]$. On the other hand, these operators play a very important role in the analytic case $K = \mathbf{C}$, especially in studying problems related to the Jacobian

Received November 15, 1988 and in revised form July 14, 1989

Conjecture (see [1], [6], [7], [8]). Similar operators are very important in the non-commutative case (see [2]).

Most of this paper is concerned with the following problem: For $P \in K[x, y]$, what is the set of those constants $\lambda \in K$, for which $P - \lambda$ is reducible? This set is called the spectrum of P and will be denoted by $\sigma(P)$. This question was answered in part by the Bertini theorem, which states that $\sigma(P)$ is at most a finite set if P is non-composite (not a non-linear polynomial of another polynomial $Q \in K[x, y]$). In this connection see [4] Section 11. The Bertini theorem, however, does not give any indication how large $\sigma(P)$ can be. This question was considered by W. Ruppert in [3]. He proves the following result: Given a pencil of plane curves of the form $\alpha P + \beta Q$, $(\alpha, \beta) \in \mathbf{P}^1$. If the generic curve in this pencil is irreducible of degree d, then the pencil contains at most $d^2 - 1$ reducible curves (see [3], Satz 6). We will consider a less general question and will prove a stronger result. For $\lambda \in \sigma(P)$ we can decompose $P - \lambda$ into the product of primes: $P - \lambda = \Pi_{i=1}^{n(\lambda)} F_{\lambda i}^{k_{\lambda i}}$. Geometrically speaking, the curve $\{P = \lambda\}$ is the union of $n(\lambda)$ irreducible curves $\{F_{\lambda i} = 0\}$. The number $\rho_\lambda(P) = n(\lambda) - 1$ is called the reducibility order of P at λ. The number $\rho(P) = \Sigma_{\lambda \in \sigma(P)} \rho_\lambda(P)$ is called the total reducibility order of P. The main result of this paper is the following:

THEOREM. *Let $P \in K[x, y]$ be noncomposite. Then $\rho(P) < \deg P$.*

The rest of the paper is concerned with describing the solutions of the equation $D_P(F) = TF$, where T is a polynomial and F is a rational function. The main result of this part of the paper can be described as follows: those polynomials T for which the equation has non-trivial solutions F form a free $\mathbf{Z}$-module of finite rank. If Q is a non-composite polynomial such that $P \in K[Q]$, then the rank of this module is $\rho(Q)$.

1. The Bertini theorem

Let K be an algebraically closed and uncountable field, char $K = 0$. For $P \in K[x, y] \setminus K$ set:

$$D_P(f) = \frac{\partial P}{\partial x}\frac{\partial f}{\partial y} - \frac{\partial P}{\partial y}\frac{\partial f}{\partial x};$$

D_P is a derivation on both $K[x, y]$ and $K(x, y)$. We will be interested in the kernels of D_P in $K[x, y]$ and in $K(x, y)$. Let $C(P) = \operatorname{Ker} D_P$ in $K[x, y]$ and let

$\tilde{C}(P) = \operatorname{Ker} D_P$ in $K(x, y)$. $C(P)$ is a subring of $K[x, y]$ and $\tilde{C}(P)$ is a subfield of $K(x, y)$. There is a convenient way of describing these kernels:

LEMMA 1.1. *Let $f \in K(x, y)$. Then the following conditions are equivalent:*
(i) $f \in \tilde{C}(P)$.
(ii) *f and P are algebraically dependent.*
(iii) *f is constant on infinitely many irreducible components of level curves $\{P = \lambda\}$.*

PROOF. (i)$\rightarrow$(ii). Assume that P and f are algebraically independent. Then for every non-constant $Q \in K[x, y]$ there exists a polynomial $R(X, Y, Z)$ such that $\partial R/\partial Z \not\equiv 0$ and $R(P, f, Q) \equiv 0$ ($K(x, y)$ does not contain subfields of transcendental degree greater than two). In other words:

$$\sum_{i=0}^{n} R_i(P, f)Q^i \equiv 0$$

and at least the polynomial R_n does not vanish identically. We can assume n to be the least possible for Q. Then:

$$0 \equiv D_P(R(P, f, Q)) = \left(\sum_{i=1}^{n} iR_i(P, f)Q^{i-1}\right) D_P(Q).$$

If $n > 1$, then $D_P(Q) = 0$ because of our choice of n. If $n = 1$, then $R_1(P, f)D_P(Q) = 0$ and $D_P(Q) = 0$ since $R_1(P, f) \not\equiv 0$. Thus $D_P(Q) = 0$ for each $Q \in K[x, y]$. This implies that $P \in K$ — a contradiction.

(ii)$\rightarrow$(iii). Assume that P and f are algebraically dependent:

$$\sum_{i=0}^{m} R_i(P) f^i = 0.$$

Choose a number $\lambda \in K$ and an irreducible component S of the level curve $\{P = \lambda\}$ in such a way that S is not contained in the variety of poles of f. There are infinitely many such curves S since K is infinite. We obtain on $S: \Sigma_{i=0}^{m} R_i(\lambda) f^i = 0$. Therefore f can obtain on S a finite number of values only, which implies that f is constant on S since S is irreducible.

(iii)$\rightarrow$(i). Let S be as above. If f is constant on infinitely many such curves S, then $D_P(f) = 0$ on infinitely many curves. This implies that $D_P(f) \equiv 0$ since $D_P(f) \in K(x, y)$.

COROLLARY. *Let $A \in C(P)$, $\deg A > 0$. Then $C(A) = C(P)$ and $\tilde{C}(A) = \tilde{C}(P)$.*

PROOF. Obvious.

Let S be an irreducible algebraic curve in K^2 and let $\bar{S}$ denote the projective closure of S. Let $\bar{S}^\nu \xrightarrow{\phi} \bar{S}$ be the normalization of $\bar{S}$. The smooth projective curve $\bar{S}^\nu$ is called the smooth projective model of S, and S is birationally isomorphic to $\bar{S}^\nu$. (See [5], Chapter 2, Section 5.) Let $p_1, \ldots, p_r$ be the points of S on infinity, i.e. the points of intersection of $\bar{S}$ with the line on infinity in $\mathbf{P}^2$. Let $q_1, \ldots, q_d$ denote the inverse images $\phi^{-1}(p_i)$. These inverse images exist since ϕ is epimorphic (see [5], Chapter 2, Section 5). The points $q_1, \ldots, q_d \in \bar{S}^\nu$ are called the branches of the curve S on infinity. If S is given by an equation $\{F = 0\}$, where F is an irreducible polynomial, then, obviously, $d \leqq \deg F$.

Let f be a rational function on S. When we discuss the behavior of f at a branch q_i, we should, strictly speaking, consider the behavior of the pull-back $\phi^*(f)$ at q_i, but, since it does not lead to confusion, we will usually speak about values of f at the branches q_i.

LEMMA 1.2. *Let S be an irreducible algebraic curve in K^2 and let $q_1, \ldots, q_d$ be the branches of S on infinity. Let F be a rational function such that the restriction $\bar{F}$ of F to S is regular and does not have zeroes. Let v_j denote the order of $\bar{F}$ at the branch q_j. Then: $\Sigma_{j=1}^d v_j = 0$.*

PROOF. Obvious.

For $\lambda_1, \ldots, \lambda_n \in K$ and $P \in K[x, y]$, $\deg P > 0$ let $G(P, \lambda_1, \ldots, \lambda_n)$ denote the multiplicative group generated by all divisors of the polynomials $P - \lambda_i$.

PROPOSITION 1.3. *Let $F_1, \ldots, F_r \in G(P, \lambda_1, \ldots, \lambda_n)$. If $r \geqq \deg P$, then there exists a non-trivial collection of integers $m_1, \ldots, m_r$ such that the rational function $f = \Pi_{i=1}^r F_i^{m_i} \in \tilde{C}(P)$.*

PROOF. Choose a number $\gamma \in K$, $\gamma \neq \lambda_1, \ldots, \lambda_n$, and an irreducible component S of the level curve $\{P = \gamma\}$. Let $q_1, \ldots, q_d$ be the branches of S on infinity. The functions F_i are regular and do not have zeroes on S since $\gamma \neq \lambda_1, \ldots, \lambda_n$. Let v_{ij} denote the order of F_i at q_j. Consider the matrix

$$M = \begin{pmatrix} v_{11} \cdots v_{1d} \\ \vdots \\ v_{r1} \cdots v_{rd} \end{pmatrix}.$$

By Lemma 1.2, $\Sigma_{j=1}^d v_{ij} = 0$ for $i = 1, \ldots, r$. Therefore $\operatorname{rk} M < d \leqq \deg P$.

Since, by our assumption, $r \geqq \deg P$, there exists a non-trivial collection of integers $m_1(\gamma, S), \ldots, m_r(\gamma, S)$ such that $\Sigma_{i=1}^r m_i(\gamma, S)v_{ij} = 0$ for $j = 1, \ldots, d$. Consider the rational function $f_{\gamma,S} = \Pi_{i=1}^r F_i^{m_i(\gamma,S)}$. This function is regular and does not have zeroes on S. Neither can it have zeroes or poles at the branches q_j since $\Sigma_{i=1}^r m_i(\gamma, S)v_{ij} = 0$ for $j = 1, \ldots, d$. Therefore $f_{\gamma,S}$ is constant on S.

Thus every appropriate choice of γ and S results in a non-trivial collection of integers $\{m_i(\gamma, S)\}$ such that the function $f_{\gamma,S} = \Pi_{i=1}^r F_i^{m_i(\gamma,S)}$ is constant on the curve S. Since K is uncountable, there are infinitely many pairs (γ, S) for which the resulting collection $\{m_i(\gamma, S)\}$ is the same. Therefore there exists a non-trivial collection of integers $\{m_i\}$ such that the rational function $f = \Pi_{i=1}^r F_i^{m_i}$ is constant on infinitely many curves S. Then $f \in \tilde{C}(P)$ by Lemma 1.1.

For $P \in K[x, y]$, $\deg P > 0$, let $\sigma(P) = \{\lambda \in K : P - \lambda \text{ is reducible}\}$. The set $\sigma(P)$ is called the *spectrum* of P. The Bertini theorem states that there are only two possibilities:

Either $\sigma(P) = K$ and there exist $R(Z) \in K[Z]$, $\deg R > 1$ and $Q \in K[x, y]$ such that $P = R(Q)$, or $\sigma(P)$ is at most a finite set.

We will give a new proof of the Bertini theorem and at the same time we will find a sharp upper bound for the number of elements of $\sigma(P)$.

Let $P \in K[x, y]$, $\deg P > 0$. P is called a *composite* polynomial if there exist $R(Z) \in K[Z]$, $\deg R > 1$ and $Q \in K[x, y]$ such that $P = R(Q)$. P is called *non-composite* if it is not composite.

Let $P \in K[x, y]$, $\deg P > 0$, and let $\lambda \in K$. Let

$$P - \lambda = \sum_{i=1}^{n(\lambda)} F_{\lambda i}^{k_{\lambda i}}$$

be the decomposition of $P - \lambda$ into the product of prime factors. The number $\rho_\lambda(P) = n(\lambda) - 1$ will be called the *reducibility order of P at λ* and the number

$$\rho(P) = \sum_{\lambda \in K} \rho_\lambda(P)$$

will be called the *total reducibility order of P*.

Remark. Note that $\rho(P) = \infty$ if P is composite and, on the other hand, for a non-composite P, $\rho_\lambda(P) > 0$ if and only if $\lambda \in \sigma(P)$.

PROPOSITION 1.4. *Let P be a non-constant polynomial. Assume that $\tilde{C}(P) = K(P)$. Then P is non-composite and $\rho(P) < \deg P$.*

PROOF. Assume for a moment that P is composite, i.e. that there exist $R(Z) \in K[Z]$, $\deg R > 1$ and $Q \in K[x, y]$ such that $P = R(Q)$. Then $D_P(Q) = 0$ and $Q \in C(P)$. Hence $Q \in K(P)$, $Q = A(P)/B(P)$ where $A, B \in K[P]$ are coprime. This implies that $B(P) \in K$ since it cannot have zeroes. Hence $Q \in K[P]$, which is clearly impossible. Therefore P is non-composite. Assume that $\rho(P) \geqq \deg P$. This means that there exist $\lambda_1, \dots, \lambda_r \in \sigma(P)$ such that $\Sigma_{j=1}^{r} \rho_{\lambda_j}(P) \geqq \deg P$. Let $P - \lambda_j = \Pi_{i=1}^{n_j} F_{ji}^{k_{ji}}$ be the decomposition of $P - \lambda_j$ into the product of prime factors. Consider the following collection of polynomials: $\{F_{11}, \dots, F_{1\,n_1-1}, \dots, F_{r1}, \dots, F_{r\,n_r-1}\}$. All polynomials in this collection belong to $G(P, \lambda_1, \dots, \lambda_r)$ and the number of elements in it is $\Sigma_{j=1}^{r} \rho_{\lambda_j}(P) \geqq \deg P$. Therefore, by Proposition 1.3 there exists a non-trivial collection of integers

$$\{m_{11}, \dots, m_{1\,n_1-1}, \dots, m_{r1}, \dots, m_{r\,n_r-1}\}$$

such that the rational function

$$f = \prod_{j=1}^{r} \prod_{i=1}^{n_j} F_{ji}^{m_{ji}} \in \tilde{C}(P).$$

Then, by our assumption, $f = A(P)/B(P)$, where $A, B \in K[P]$ are coprime. If we decompose $A(P)$ and $B(P)$ into products of linear (in P) factors, we note that for each such factor all its prime divisors are present, which contradicts our choice of the collection:

$$\{F_{11}, \dots, F_{1\,n_1-1}, \dots, F_{r1}, \dots, F_{r\,n_r-1}\}.$$

Therefore our assumption is false and $\rho(P) < \deg P$.

To proceed further, we now introduce some auxiliary concepts:

Let $G(P)$ denote the multiplicative group generated by all divisors of polynomials $P - \lambda$ for all $\lambda \in K$ and by non-zero elements of K. It is easy to see that

$$G(P) = \bigcup_{\{\lambda_1, \dots, \lambda_n\} \subset K} G(P, \lambda_1, \dots, \lambda_n).$$

A collection $F_1, \dots, F_r \in G(P)$ is called *P-free* if there is no non-trivial collection of integers $\{m_1, \dots, m_r\}$ such that:

$$F_1^{m_1} \cdots F_1^{m_r} \in \tilde{C}(P).$$

It follows from Proposition 1.3 that $r < \deg P$ for any p-free collection $\{F_1, \dots, F_r\}$.

A P-free collection $\{F_1, \dots, F_r\}$ is called *maximal* if $\{F_1, \dots, F_r, F\}$ is not P-free for every $F \in G(P)$. It is obvious that if there exists a P-free collection, then there exists a maximal P-free collection.

A non-constant polynomial $P \in K[x, y]$ is called *basic* if

$$\min_{Q \in C(P) \setminus K} \deg Q = \deg P.$$

Lemma 1.5. *Let P be a basic polynomial. If $\sigma(P) \neq \varnothing$, then there exists a P-free collection (and, therefore, a maximal P-free collection).*

Proof. Let $\lambda \in \sigma(P)$ and let $P - \lambda = \Pi_{i=1}^n F_i^{k_i}$, F_i — irreducible. Then $\{F_1\}$ is a P-free collection. Indeed, assume that $F_1^k \in \tilde{C}(P)$ for some integer $k \neq 0$. Then $F_1 \in C(P)$ by Corollary to Lemma 1.1, but this is impossible since P is basic and $\deg F_1 < \deg P$.

Proposition 1.6. *Let P be a basic polynomial. Then $C(P) = K[P]$ and $\tilde{C}(P) = K(P)$.*

Proof. We will first prove that $\sigma(P) \neq K$. Indeed, assume that $\sigma(P) = K$. By Lemma 1.5 there exists a maximal P-free collection $\{F_1, \dots, F_r\}$. For $\alpha \in K$ choose an irreducible divisor F_α of $P - \alpha$. Then the collection $\{F_1, \dots, F_r, F_\alpha\}$ is not P-free and there exists, therefore, a non-trivial collection of integers

$$\{m_1(\alpha), \dots, m_r(\alpha), m_\alpha\}$$

such that $m_\alpha \neq 0$ and $F_1^{m_1(\alpha)} \cdots F_r^{m_r(\alpha)} F_\alpha^{m_\alpha} \in \tilde{C}(P)$. The same construction for $\beta \neq \alpha$ gives us another collection of integers:

$$\{m_1(\beta), \dots, m_r(\beta), m_\beta\}$$

with similar properties. Since K is uncountable, there exists a pair $\alpha \neq \beta$ such that $m_i(\alpha) = m_i(\beta) = m_i$ and $m_\alpha = m_\beta = m$ $(i = 1, \dots, r)$. Hence

$$F_1^{m_1} \cdots F_r^{m_r} F_\alpha^m \in \tilde{C}(P) \quad \text{and} \quad F_1^{m_1} \cdots F_r^{m_r} F_\beta^m \in \tilde{C}(P).$$

Then $(F_\alpha / F_\beta)^m \in \tilde{C}(P)$ and, by obvious reasons, $F_\alpha / F_\beta \in \tilde{C}(P)$.

Let $F_\alpha G_\alpha = P - \alpha$, $F_\beta G_\beta = P - \beta$. Then

$$F_\alpha G_\beta = \frac{F_\alpha (P - \beta)}{F_\beta} \in \tilde{C}(P)$$

and, since $F_\alpha G_\beta$ is a polynomial, $F_\alpha G_\beta \in C(P)$. Similarly $F_\beta G_\alpha \in C(P)$. Now consider the product $(P-\alpha)(P-\beta) = (F_\alpha G_\beta)(F_\beta G_\alpha)$. If $\deg F_\alpha G_\beta > \deg P$, then $\deg F_\beta G_\alpha < \deg P$, which is impossible since P is basic. Therefore $\deg F_\alpha G_\beta = \deg F_\beta G_\alpha = \deg P$. Let $\overline{F_\alpha G_\beta}$ denote the leading term of $F_\alpha G_\beta$ and let $\bar{P}$ denote the leading term of P. Since $F_\alpha G_\beta \in C(P)$ there exists a constant c such that $\overline{F_\alpha G_\beta} = c\bar{P}$ (this follows from the well-known fact that homogeneous polynomials of the same degree, whose jacobian is zero, must be proportional). Let $A = F_\alpha G_\beta - cP$, $A \in C(P)$ and $\deg A < \deg P$. Since P is basic, it follows that $A = c_1 \in K$. Thus

$$F_\alpha G_\beta = cP + c_1 = c(P + c_1/c).$$

So F_α is a divisor of $P + c_1/c$. Since F_α is also a divisor of $P - \alpha$, it follows that $c_1/c = -\alpha$. Applying the same argument to G_β, we obtain that $c_1/c = -\beta$, which is impossible since $\alpha \neq \beta$. Therefore $\sigma(P) \neq K$ and there exists $\lambda \in K$ such that $P - \lambda$ is irreducible. Choose any polynomial $Q \in C(P)$ and consider its restriction to the irreducible curve $\{P = \lambda\}$. Since Q and P are algebraically dependent by Lemma 1.1, this restriction must be a constant. Therefore $Q = Q_1(P-\lambda) + c_1$, $c_1 \in K$ and $\deg Q_1 < \deg Q$. $Q_1 \in C(P)$ and we can repeat the argument until we obtain that $Q \in K[P]$. Therefore $C(P) = K[P]$.

Now consider a rational function $f \in \tilde{C}(P)$. Let $f = A/B$, where A and B are polynomials without common factors. Since f and P are algebraically dependent by Lemma 1.1, there exists a polynomial $\Sigma_{i=0}^{n} R_i(X)Y^i$, $R_n(X) \neq 0$, such that $\Sigma_{i=0}^{n} R_i(P)f^i = 0$. Then $\Sigma_{i=0}^{n} R_i(P)A^iB^{-i} = 0$ or, in other words, $R_n(P)A^n = -B\,\Sigma_{i=0}^{n-1} R_i(P)A^iB^{n-i-1}$. Since A and B do not have common factors, it follows that $R_n(P) = UB$, $U \in K[x,y]$. Then

$$f = \frac{A}{B} = \frac{UA}{R_n(P)}, \quad UA \in C(P) = K[P] \quad \text{and} \quad f \in K(P).$$

Thus $\tilde{C}(P) = K(P)$.

THEOREM 1.7. *Let $P \in K[x,y]$, $\deg P > 0$. Then the following conditions are equivalent to P being non-composite*:

(i) *P is basic.*

(ii) *$C(P) = K[P]$ and $\tilde{C}(P) = K(P)$.*

(iii) *$\rho(P) < \deg P$.*

PROOF. (i) Assume that P is basic. If P is composite, then there exist

$R(Z) \in K[Z]$, $\deg R > 1$ and $Q \in K[x, y]$ such that $P = R(Q)$. Then $Q \in C(P)$ and $0 < \deg Q < \deg P$, which is impossible since P is basic. Thus P is non-composite.

Now assume that P is non-composite. Let P_1 be a non-constant polynomial of the least degree in $C(P)$. Then, obviously, P_1 is basic and $C(P) = C(P_1) = K[P_1]$ by Proposition 1.6. Thus $P = R(P_1)$. If $\deg R > 1$, then P is composite. Hence $\deg R = 1$ and $P = c_1 P_1 + c_2$, which implies that P is basic.

(ii) If P is non-composite, then by (i) P is basic and the result follows from Proposition 1.6.

If $\tilde{C}(P) = K(P)$, then P is non-composite by Proposition 1.4.

(iii) If P is non-composite, then $\tilde{C}(P) = K(P)$ by (ii) and $\rho(P) < \deg P$ by Proposition 1.4.

If $\rho(P) < \deg P$, then P is non-composite since $\rho(P) = \infty$ for a composite P.

Corollary. *Let $P \in K[x, y]$, $\deg P > 0$. Let $G_0(P)$ denote the multiplicative group of the field $\tilde{C}(P)$ ($G_0(P)$ is, obviously, a subgroup of $G(P)$). Then:*

(i) *There exists a non-composite $Q \in C(P)$ such that $C(P) = K[Q]$ and $\tilde{C}(P) = K(Q)$.*

(ii) *$G(P) = G(A)$ and $G_0(P) = G_0(A)$ for every non-constant $A \in C(P)$.*

Proof. (i) Let Q be a non-constant polynomial of the least degree in $C(P)$. Then Q is basic. The rest follows from Theorem 1.7 and from Corollary to Lemma 1.1.

(ii) Let $A \in C(P)$, $\deg A > 0$. Then $A = R(Q)$ for a non-composite $Q \in C(P)$. Let F be an irreducible divisor of $A - \lambda$ for some $\lambda \in K$. Then F is an irreducible divisor of $R(Q) - \lambda = c(Q - \gamma_1)^{k_1} \cdots (Q - \gamma_n)^{k_n}$. Therefore F is a divisor of $Q - \gamma_i$ for some index i.

Thus $G(A) \subset G(Q)$. Now let F be a divisor of $Q - \gamma$ for some $\gamma \in K$. Then F is a divisor of $R(Q) - R(\gamma) = A - R(\gamma)$. Therefore $G(Q) \subset G(A)$. Hence $G(A) = G(Q)$ for every non-composite $Q \in C(P)$, which implies that $G(A) = G(P)$. $G_0(A) = G_0(P)$ since $\tilde{C}(A) = \tilde{C}(P)$ by Corollary to Lemma 1.1.

A non-composite Q such that $C(Q) = C(P)$ will be called a *generator* of P. The quotient group $\Gamma(P) = G(P)/G_0(P)$ is an important invariant of the polynomial P (or rather of the field $\tilde{C}(P)$) and will be called the *divisor class group of P*. Its structure is described in Section 2. To do this, we need one technical result:

Lemma 1.8. *Let $P \in K[x, y]$ be non-composite. Let $F = \prod_{i=1}^{n} F_i$, $F_i \in$*

$G(P,\lambda_i)$ and $\lambda_i \neq \lambda_j$ for $i \neq j$. If $F \in \tilde{C}(P)$, then $F_i \in \tilde{C}(P)$ for $i = 1, \ldots, n$. Moreover, F_i is a power of $P - \lambda_i$ up to a constant multiplier.

PROOF. $\tilde{C}(P) = K(P)$ by Theorem 1.7. Thus $F = A(P)/B(P)$, where $A(P), B(P) \in K[P]$. Decomposing $A(P)$ and $B(P)$ into linear (in P) factors we obtain:

$$\prod_{i=1}^{n} F_i = c \prod_{j=1}^{m} (P - \gamma_j)^{k_j}, \qquad c, \gamma_1, \ldots, \gamma_m \in K.$$

Decomposing each F_i and each $P - \gamma_j$ into irreducible factors, we immediately obtain that the collections $\{\lambda_1, \ldots, \lambda_n\}$ and $\{\gamma_1, \ldots, \gamma_m\}$ coincide and that F_i is a power of $P - \lambda_i$ up to a constant multiplier.

2. The structure of the group $\Gamma(P)$ and the equation $D_P(F) = TF$

For a non-constant $P \in K[x,y]$ and $F \in K(x,y)$ set:

$$\tau_P(F) = \frac{D_P(F)}{F}.$$

LEMMA 2.1. *Let $F \in K[x,y]$ be irreducible and such that $\tau_P(F) = T \in K[x,y]$. Then there exists $\lambda \in K$ such that F is a divisor of $P - \lambda$.*

PROOF. Consider the partial derivatives $\partial F/\partial x = D_F(y)$ and $\partial F/\partial y = -D_F(x)$. At least one of them is not zero since $F \notin K$. Assume that $\partial F/\partial x \neq 0$. Let $\bar{P}$, $\bar{y}$ denote the restrictions of P and y to the curve $\{F = 0\}$. The regular functions $\bar{P}$ and $\bar{y}$ on the curve $\{F = 0\}$ are algebraically dependent: $R(\bar{P}, \bar{y}) = 0$, where R is a non-trivial polynomial in two variables. Therefore, since F is irreducible, $R(P,y) = AF$ for some $A \in K[x,y]$. Let $R(P,y) = \sum_{i=0}^{n} R_i(P)y^i$ and let n be the least possible. Assume $n > 0$. Then

$$D_F(R(P,y)) = \frac{\partial R}{\partial P} D_F(P) + \frac{\partial R}{\partial y}\frac{\partial F}{\partial x} = \frac{\partial R}{\partial y}\frac{\partial F}{\partial x} - TF\frac{\partial R}{\partial P}.$$

On the other hand $D_F(R(P,y)) = D_F(A)F$. So

$$D_F(A)F = \frac{\partial R}{\partial y}\frac{\partial F}{\partial x} - T\frac{\partial R}{\partial P}F$$

and we obtain that F divides $(\partial R/\partial y)(\partial F/\partial x)$. F cannot divide $\partial F/\partial x$ and, since F is irreducible, it divides $\partial R/\partial y$. This contradicts our choice of n and we conclude that $n = 0$.

Thus there exists a non-trivial polynomial $R(P)$ which is a multiple of F. Therefore P can obtain only a finite number of values on the curve $\{F=0\}$, which implies that P is constant on this curve since F is irreducible.

PROPOSITION 2.2. (i) *The map τ_P, when considered as a map from the multiplicative group $K^*(x,y)$ of the field $K(x,y)$ into the additive group of this field, is a group homomorphism.*

(ii) *If $F_1, F_2 \in K[x,y]$ are polynomials without common factors such that $\tau_P(F_1F_2) \in K[x,y]$ or $\tau_P(F_1/F_2) \in K[x,y]$, then $\tau_P(F_1) \in K[x,y]$ and $\tau_P(F_2) \in K[x,y]$.*

PROOF.

$$\text{(i)} \qquad \tau_P(F_1F_2) = \frac{D_P(F_1F_2)}{F_1F_2} = \frac{D_P(F_1)F_2 + D_P(F_2)F_1}{F_1F_2} = \tau_P(F_1) + \tau_P(F_2),$$

$$\tau_P(F^{-1}) = FD_P(F^{-1}) = -\frac{FD_P(F)}{F^2} = -\tau_P(F).$$

(ii) If $\tau_P(F_1F_2) = T \in K[x,y]$, then $T = D_P(F_1F_2)/F_1F_2$ or, in other words, $TF_1F_2 = D_P(F_1)F_2 + D_P(F_2)F_1$. Thus F_1 divides $D_P(F_1)F_2$ which implies that F_1 divides $D_P(F_1)$ since F_1 and F_2 do not have common factors. So $D_P(F_1) = T_1F_1$ and $D_P(F_2) = (T - T_1)F_2$. Therefore $\tau_P(F_1) = T_1 \in K[x,y]$ and $\tau_P(F_2) = T_2 = T - T_1 \in K[x,y]$. Similarly, if $\tau_P(F_1/F_2) = T \in K[x,y]$, then $TF_1F_2 = D_P(F_1)F_2 - D_P(F_2)F_1$ and the rest follows as above.

PROPOSITION 2.3. $\tau_P(G(P)) = K[x,y] \cap \tau_P(K^*(x,y))$.

PROOF. We will first prove that $\tau_P(G(P)) \subset K[x,y]$. Since τ_P is a homomorphism, it will suffice to prove that $\tau_P(F) \in K[x,y]$ if F is a divisor of $P - \lambda$, $\lambda \in K$. So let $AF = P - \lambda$. Then

$$\tau_P(F) = \frac{D_P(F)}{F} = \frac{D_{P-\lambda}(F)}{F} = \frac{D_{AF}(F)}{F} = D_A(F) \in K[x,y].$$

Now assume that $\tau_P(F) \in K[x,y]$ for some $F \in K^*(x,y)$. Let $F = A/B$, where $A, B \in K[x,y]$ do not have common factors. Then $\tau_P(A) \in K[x,y]$ and $\tau_P(B) \in K[x,y]$ by Proposition 2.2.

Our goal is to prove that $F \in G(P)$. It will therefore suffice to prove that $A \in G(P)$ if $A \in K[x,y]$, $A \neq \text{const}$ and $\tau_P(A) \in K[x,y]$. Let $\Pi_{i=1}^n F_i^{k_i}$ be the decomposition of A into the product of primes. It follows from Proposition 2.2

that $\tau_P(F_i^{k_i}) \in K[x, y]$ for $i = 1, \ldots, n$. But then $\tau_P(F_i) = \tau_P(F_i^{k_i})/k_i \in K[x, y]$. It now follows from Lemma 2.1 that F_i is a divisor of $P - \lambda_i$ for some $\lambda_i \in K$. Thus $A \in G(P)$ and $\tau_P(G(P)) \supset K[X, Y] \cap \tau_P(K^*(x, y))$. This concludes the proof.

Let $\tilde{\Gamma}(P) = \tau_P(G(P))$. $\tilde{\Gamma}(P)$ is a subgroup of the additive group of $K[x, y]$. Since $\operatorname{Ker} \tau_P = G_0(P)$, we can consider τ_P as an isomorphism $\Gamma(P) \xrightarrow{\tau_P} \tilde{\Gamma}(P)$. Let $\pi : G(P) \to \Gamma(P)$ be the natural projection homomorphism and let $\Gamma(P, \lambda) = \pi(G(P, \lambda))$. Let $\tilde{\Gamma}(P, \lambda) = \tau_P(\Gamma(P, \lambda))$.

Strictly speaking, $\tau_P : G(P) \to \tilde{\Gamma}(P)$ and $\tau_P : \Gamma(P) \to \tilde{\Gamma}(P)$ are two different maps, but we use the same notation for both of them since this does not lead to confusion.

If $P \in K[x, y]$ is non-composite, then $\sigma(P)$ is either empty or a finite set $\{\lambda_1, \ldots, \lambda_n\}$. ($\sigma(P)$ is at most finite, since, by Theorem 1.8, the number of elements of $\sigma(P)$ cannot exceed $\rho(P)$ which is finite.)

THEOREM 2.4. *Let $P \in K[x, y]$ be non-composite. Then*:

(i) $\tilde{\Gamma}(P, \lambda) = 0$ *if and only if* $\lambda \notin \sigma(P)$.

(ii) *If* $\lambda \in \sigma(P)$, *then* $\tilde{\Gamma}(P, \lambda)$ *is a free* $\mathbf{Z}$*-module and* $\operatorname{rk} \tilde{\Gamma}(P, \lambda) = \rho_\lambda(P)$.

(iii) $\tilde{\Gamma}(P) = \bigoplus_{\lambda \in \sigma(P)} \tilde{\Gamma}(P, \lambda)$ *and* $\operatorname{rk} \tilde{\Gamma}(P) = \rho(P)$.

PROOF. (i) Assume $\tilde{\Gamma}(P, \lambda) = 0$. Then, obviously, $G(P, \lambda) \subset G_0(P)$. Let F be a divisor of $P - \lambda$. Then $F \in G_0(P) \subset \tilde{C}(P)$ and, by Lemma 1.8, F is a power of $P - \lambda$ up to a constant multiplier. Therefore $P - \lambda$ is irreducible and $\lambda \notin \sigma(P)$.

Now assume that $\lambda \notin \sigma(P)$. Then $P - \lambda$ is irreducible and $G(P, \lambda)$ is generated by K^* and by powers of $P - \lambda$. Hence $G(P, \lambda) \subset G_0(P)$ and $\Gamma(P, \lambda) = 0$. Therefore $\tilde{\Gamma}(P, \lambda) = 0$.

(ii) Let $\lambda \in \sigma(P)$ and let $P - \lambda = \prod_{i=1}^{n(\lambda)} F_{\lambda i}^{k_{\lambda i}}$ be the decomposition of $P - \lambda$ into the product of primes. Set $\Delta_{\lambda i} = \tau_P(F_{\lambda i})$. K^* and $F_{\lambda i}$'s generate $G(P, \lambda)$ as a multiplicative group. Therefore $\Delta_{\lambda i}$'s generate $\tilde{\Gamma}(P, \lambda)$ as a $\mathbf{Z}$-module. So $\tilde{\Gamma}(P, \lambda)$ is a finitely-generated $\mathbf{Z}$-module and, since it is without torsion, $\tilde{\Gamma}(P, \lambda)$ is a free $\mathbf{Z}$-module. We will now prove that $\sum_{i=1}^{n(\lambda)} k_{\lambda i} \Delta_{\lambda i} = 0$ and that this is the only relation between $\Delta_{\lambda i}$'s. Indeed

$$0 = \tau_P(P - \lambda) = \sum_{i=1}^{n(\lambda)} k_{\lambda i} \Delta_{\lambda i}.$$

Now let $\{m_i\}$, $1 \leqq i \leqq n(\lambda)$, be a non-trivial collection of integers such that $\sum_{i=1}^{n(\lambda)} m_i \Delta_{\lambda i} = 0$. Then

$$0=\tau_P\left(\prod_{i=1}^{n(\lambda)} F_{\lambda i}^{m_i}\right) \quad \text{and} \quad \prod_{i=1}^{n(\lambda)} F_{\lambda i}^{m_i}\in G_0(P)\subset \tilde{C}(P).$$

It follows from Lemma 1.8 that $\Pi_{i=1}^{n(\lambda)} F_{\lambda i}^{m_i}=c(P-\lambda)^N$ for $c\in K^*$, $N\in \mathbf{Z}$. Therefore $\Pi_{i=1}^{n(\lambda)} F_{\lambda i}^{m_i}=c\,\Pi_{i=1}^{n(\lambda)} F_{\lambda i}^{Nk_{\lambda i}}$. So $c=1$ and $m_i=Nk_{\lambda i}$ for $1\leqq i\leqq n(\lambda)$. Thus the only relation between $\Delta_{\lambda i}$'s is $\Sigma_{i=1}^{n(\lambda)} k_{\lambda i}\Delta_{\lambda i}=0$ and $\operatorname{rk}\tilde{\Gamma}(P,\lambda)=n(\lambda)-1=\rho_\lambda(P)$.

(iii) Let $T\in\tilde{\Gamma}(P)$. Then $T=\tau_P(F)$ for some $F\in G(P)$. F can be decomposed in the following way:

$$F=A(P)\prod_{\lambda\in\sigma(P)}\prod_{i=1}^{n(\lambda)} F_{\lambda i}^{m_{\lambda i}},$$

where $A(P)\in\tilde{C}(P)$ and $F_{\lambda i}$ is an irreducible divisor of $P-\lambda$. Then

$$T=\tau_P(F)=\sum_{\lambda\in\sigma(P)}\sum_{i=1}^{n(\lambda)} m_{\lambda i}\Delta_{\lambda i}, \qquad \text{where } \Delta_{\lambda i}=\tau_P(F_{\lambda i}).$$

It was shown in (ii) that $\Delta_{\lambda i}$'s generate $\tilde{\Gamma}(P,\lambda)$ as a $\mathbf{Z}$-module. Therefore $\Gamma(P)=\Sigma_{\lambda\in\sigma(P)}\tilde{\Gamma}(P,\lambda)$.

Now we have to prove that this is a direct sum. Indeed, assume that there exists a relation $\Sigma_{\lambda\in\sigma(P)} T_\lambda=0$, where $T_\lambda\in\tilde{\Gamma}(P,\lambda)$. Then $T_\lambda=\tau_P(F_\lambda)$ for some $F_\lambda\in G(P,\lambda)$.

The relation $\Sigma_{\lambda\in\sigma(P)} T_\lambda=0$ implies that $\Pi_{\lambda\in\sigma(P)} F_\lambda\in\tilde{C}(P)$, which implies by Lemma 1.8 that $F_\lambda=(P-\lambda)^{N_\lambda}$. Hence $T_\lambda=0$. Thus $\tilde{\Gamma}(P)=\bigoplus_{\lambda\in\sigma(P)}\tilde{\Gamma}(P,\lambda)$ and

$$\operatorname{rk}\tilde{\Gamma}(P)=\sum_{\lambda\in\sigma(P)}\operatorname{rk}\tilde{\Gamma}(P,\lambda)=\sum_{\lambda\in\sigma(P)}\rho_\lambda(P)=\rho(P).$$

This concludes the proof.

Remark. Much more could be said about the structure of $\tilde{\Gamma}(P)$: Let $L(P)$ denote the K-linear space spanned by $\tilde{\Gamma}(P)$. Then:

(i) $\dim L(P)=\rho(P)$.

(ii) $L(P)\cap D_P(K[x,y])=0$.

The only proof of these statements I was able to construct requires use of analytical methods and will be presented in a separate paper.

References

1. H. Bass, E. H. Connell and D. Wright, *The Jacobian Conjecture: Reduction of degree and formal expansion of the inverse*, Bull. Am. Math. Soc. 7 (1982).
2. J. Dixmier, *Sur les algèbres de Weyl*, Bull. Soc. Math. France **96** (1968), 209–242.

3. W. Ruppert, *Reduzibilität Ebener Kurven*, J. Reine Angew. Math. **369** (1986), 167–191.

4. A. Schinzel, *Selected Topics on Polynomials*, Ann Arbor Publications, University of Michigan Press, 1982.

5. I. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag, Berlin, 1977.

6. Y. Stein, *On linear differential operators related to the Jacobian Conjecture*, J. Pure Appl. Algebra **57** (1989), 175–186.

7. Y. Stein, *On the density of image of differential operators generated by polynomials*, J. Analyse Math. **52** (1989), 291–300.

8. Y. Stein, *Linear differential operators related to the Jacobian Conjecture have a closed image*, J. Analyse Math. **54** (1990), to appear.