manuscripta math. 68, 327 - 335 (1990)

manuscripta mathematica

GENERATORS FOR THE DERIVATION MODULES AND THE RELATION IDEALS OF CERTAIN CURVES

Dilip P. Patil and Balwant Singh

Let $\mathcal{O}$ be a curve in the affine algebroid e-space over a field K of characteristic zero. Let $\mathcal{D}$ be the module of K-derivations and P the relation ideal of $\mathcal{O}$. Generators for $\mathcal{D}$ and P are computed in several cases. It is shown in particular that in the case of a monomial curve defined by a sequence of e positive integers some $e-1$ of which form an arithmetic sequence, $\mu(\mathcal{D}) \le 2e-3$ and $\mu(P) \le e(e-1)/2$.

INTRODUCTION

Let $\mathcal{O}$ be a reduced and irreducible curve in the affine algebroid e-space over a field K of characteristic zero. Let $\mathcal{D} = \mathrm{Der}_K(\mathcal{O})$ and let P be the relation ideal of $\mathcal{O}$. We consider the question of finding minimal sets of generators for the module $\mathcal{D}$ and the ideal P and in particular determining the cardinalities $\mu(\mathcal{D})$ and $\mu(P)$ of these sets. While the question for P is a very standard one and has been studied extensively, the question for $\mathcal{D}$ arose in our attempt to compute the $\mathcal{O}$-module $\mathrm{Diff}^2_K(\mathcal{O})/(\mathrm{Diff}^1_K(\mathcal{O}))^2$, where Diff^i denotes the module of differential operators of order at most i. The computation of this object is of interest in the context of Nakai's Conjecture a stronger version of which states that if $\mathrm{Diff}^2_K(\mathcal{O}) = (\mathrm{Diff}^1_K(\mathcal{O}))^2$ then $\mathcal{O}$ is regular. An additional motivation was provided by a striking similarity we observed in several cases between the behaviours of $\mu(\mathcal{D})$ and $\mu(P)$. We note this similarity while describing our results in the following paragraph.

If $e = 1$ then $\mu(P) = 0$ and $\mu(\mathcal{D}) = 1$. If $e = 2$ then $\mu(P) = 1$ and $\mu(\mathcal{D}) \leq 2$ [4]. We can explicitly construct in this case two generators for $\mathcal{D}$ (Theorem (1.1)). For $e = 3$ both $\mu(\mathcal{D})$ and $\mu(P)$ are unbounded. The unboundedness of $\mu(P)$ was proved by Moh [7] by constructing a sequence $\{P_n\}$ of prime ideals of $R = K[[X_0, X_1, X_2]]$ such that $\mu(P_n) = n + 1$. We can prove the unboundedness of $\mu(\mathcal{D})$ by showing that for the same examples $\mu(\mathrm{Der_K}(R/P_n)) = 2n$ (Theorem (2.1)). For $e = 3$ again the situation is different in the case of monomial curves. In this case $\mu(\mathcal{D}) \leq 3$ [6] and $\mu(P) \leq 3$ [3]. We generalize these two results as follows: A sequence of e terms is called an **almost arithmetic sequence** if some $e - 1$ of its terms form an arithmetic sequence. We show that if $e \geq 3$ and $\mathcal{O}$ is a monomial curve defined by an almost arithmetic sequence then $\mu(\mathcal{D}) \leq 2e - 3$ (Theorem (4.1)) and $\mu(P) \leq e(e-1)/2$ (Theorem (4.3)) and that these bounds are sharp (Examples (4.6)). These results generalize those of [6] and [3], since any 3-term sequence is an almost arithmetic sequence. The results on $\mu(P)$ hold without any restriction on the characteristic of K. For $e \geq 4$ both $\mu(\mathcal{D})$ and $\mu(P)$ are unbounded even for monomial curves [5], [1].

If $\mathcal{O}$ is a monomial curve and its semigroup is symmetric then $\mu(\mathcal{D}) \leq 2$ [5]. So, in consistency with the pattern noted above, one may expect that, for a fixed e, $\mu(P)$ is bounded for monomial curves whose semigroups are symmetric. This is indeed the case if $e \leq 4$ and is an open question in general [2].

In proving our results we give in fact an explicit construction of a set of generators for $\mathcal{D}$ and P in each case. In the case of a monomial curve defined by an almost arithmetic sequence this construction (Theorem (4.5)) is used by Patil [9] to prove that such curves are set-theoretic complete intersections.

While proofs of (1.1) and (2.1) can be found in [8], those of the results on monomial curves are given in section 4. Our main tool for proving these results is an explicit description of a standard basis of the semigroup generated by an almost arithmetic sequence (Theorem (3.5)), which might also be of some interest in the context of a linear Diophantine problem of Frobenius (cf. [10]).

NOTATION. $[a, b] = \{i \in \mathbb{Z} \mid a \leq i \leq b\}$.

1. CONSTRUCTION OF GENERATORS FOR THE DERIVATION MODULE OF A PLANE CURVE

Suppose $e = 2$. Represent $\mathcal{O}$ in the form $\mathcal{O} = K[[X]][Y]/(f)$ with f monic in Y of degree $n = \mathrm{ord}_{(X,Y)}(f)$. Let x, y, f_x, f_y denote respectively the natural images of $X, Y, \partial f/\partial X, \partial f/\partial Y$ in $\mathcal{O}$. Since $\mathcal{O}$ is reduced, f_y is a nonzero divisor in $\mathcal{O}$. Let $L = \bigoplus_{j=0}^{n-1} K((x))y^j$ be the total quotient ring of $\mathcal{O}$. For $j \in [0, n-1]$ define $\pi_j : L \to K((x))$ by $\lambda = \sum_{j=0}^{n-1} \pi_j(\lambda)y^j$ for $\lambda \in L$.

For $i \geq 1$ let $g_i = \sum_{j=0}^{n-1} \pi_j(f_x/f_y)\pi_{n-1}(y^{i+j-1})$. For $I \subseteq [1,n]$ let $M(I)$ denote the $|I| \times |I|$ matrix whose (i,j)-entry is g_{i+j-1} and put $D(I) = \det(M(I))$. For $r \in [0,n]$ let us define $b_r = \inf\{\mathrm{ord}_x(D(I)) \mid I \subseteq [1,n],\ |I| = r\}$. Then $b_0 = 0$. Let $k \in [0, n-1]$ be maximum with $b_{-1} > b_0 > \cdots > b_{k-1} > b_k$, where $b_{-1} = \infty$. If $k > 0$ then let $h \in [0, k-1]$ be maximum with $b_{h-1} - b_h > b_{k-1} - b_k$.

For $r \in [0, n-1]$ denote by N_r the matrix obtained from $M([1, r+1])$ by replacing its last row by $(1, y, y^2, \ldots, y^r)$. Let $\psi_1 = x^{-w}det(N_k)$ with $w = b_k$. If $k > 0$ then let $\psi_2 = x^{-u}det(N_h)$ with $u = b_{h+1}$, and if $k = 0$ then let $\psi_2 = 0$. For $i = 1, 2$, let $D_i \in \mathrm{Der}_K(\mathcal{O}, L)$ be given by $D_i(x) = \psi_i$, $D_i(y) = -\psi_i f_x/f_y$.

(1.1) Theorem. *D_1, D_2 belong to $\mathrm{Der}_K(\mathcal{O})$ and generate it.*

Proof. See [8]. ∎

2. MOH'S EXAMPLES

Let $m, n, \lambda \in \mathbb{Z}$ with $m \geq 2$, $n = 2m - 1$, $\lambda > n(n+1)m$ and $\gcd(m, \lambda) = 1$. Let $\mathcal{O} = K[[X^n(1+Y), X^{n+1}, X^{n+2}]] \subseteq K[[T]]$, where $X = T^m$, $Y = T^\lambda$. Put $\nu = \lambda/nm$, $u = (n-2)(n+1)$, $F_i = X^{u+i}Y^{m-2}$ for $i \geq 0$ and $\delta = T\dfrac{d}{dT}$.

(2.1) Theorem. *The $\mathcal{O}$-module $\mathrm{Der}_K(\mathcal{O})$ is minimally generated by the $2n$ elements $X^{n+2}\delta, F_0(1-\nu Y)\delta, F_2\delta, \ldots, F_{n-1}\delta, F_1Y\delta, \ldots, F_nY\delta$.*

Proof. See [8]. ∎

3. A STANDARD BASIS OF THE SEMIGROUP GENERATED BY AN ALMOST ARITHMETIC SEQUENCE

Let $\Gamma \subseteq \mathbb{Z}^+$ be a semigroup with $\gcd(\Gamma) = 1$ and let $m_0 \in \Gamma - \{0\}$. The set $S = \{\gamma \in \Gamma \mid \gamma - m_0 \notin \Gamma\}$ is called the **standard basis** of Γ w.r.t. m_0, and it has the following obvious property: Every $\alpha \in \mathbb{Z}$ has a unique expression $\alpha = am_0 + \sigma$ with $a \in \mathbb{Z}$, $\sigma \in S$; moreover, $\alpha \in \Gamma$ if and only if $a \geq 0$.

Our aim in this section is to describe S in case Γ is generated by positive integers $m_0, m_1, \ldots, m_{p+1}$, where $m_0 < m_1 < \cdots < m_p$ is an arithmetic sequence and m_{p+1} is arbitrary. It is clear that if $p = -1$ then $S = \{0\}$, whereas if $p = 0$ then $S = \{im_1 \mid i \in [0, m_0 - 1]\}$. So we assume that $p \geq 1$.

Put $n = m_{p+1}$ and let $\Gamma' = \sum_{i=0}^{p} \mathbb{Z}^+ \mathrm{m_i}$. Then $\Gamma = \Gamma' + \mathbb{Z}^+\mathrm{n}$. For $i \geq 0$ let $q_i \in \mathbb{Z}$, $\mathrm{r_i} \in [1,\mathrm{p}]$ and $g_i \in \Gamma'$ be defined by $i = q_i p + r_i$ and $g_i = q_i m_p + m_{r_i}$. Let $u = \min\{i \geq 0 \mid g_i \notin S\}$, $v = \min\{b \geq 1 \mid bn \in \Gamma'\}$ and $V = [0, u-1] \times [0, v-1]$. Let $\equiv$ denote $\equiv$ (mod m_0).

(3.1) Lemma. (a) $0 = g_0 < g_1 < g_2 < \cdots$. *In particular,* $g_0 \in S$ *and* $u \geq 1$.

(b) *Let* $i, j \in [0, p]$. *Then* $m_i + m_j = (1 - \varepsilon)m_0 + m_{i+j-\varepsilon p} + \varepsilon m_p$ *with* $\varepsilon = 0$ *or* 1 *according as* $i + j \leq p$ *or* $i + j > p$.

(c) $g_i + g_j = \varepsilon m_0 + g_{i+j}$ *with* $\varepsilon = 1$ *or* 0 *according as* $r_i + r_j \leq p$ *or* $r_i + r_j > p$.

(d) *Every element of* Γ *(resp.* Γ'*) can be expressed in the form* $am_0 + g_i + bn$ *(resp.* $am_0 + g_i$*) with* $a, i \geq 0, b \in [0, v-1]$.

(e) *Let* $(i, b), (j, c) \in V$ *with* $i \leq j, b \geq c$ *and* $g_i + bn \equiv g_j + cn$. *Then* $(i, b) = (j, c)$.

Proof. (a), (b) and (c) are easily verified using the fact that $m_0 < m_1 < \cdots < m_p$ is an arithmetic sequence.

(d) Let $\gamma = am_0 + dm_p + \sum_{i=1}^{p-1} c_i m_i \in \Gamma'$ with $a, d, c_i \geq 0$. By (b) and induction on $c = \sum_{i=1}^{p-1} c_i$ we may assume that $c \leq 1$. If $c = 0$ then $\gamma = am_0 + dm_p = am_0 + g_{dp}$. If $c = 1$ then $\gamma = am_0 + dm_p + m_i = am_0 + g_{dp+i}$ for some i. This proves the assertion for Γ', whence also for Γ, since $vn \in \Gamma'$.

(e) $(b - c)n \equiv g_j - g_i \equiv g_{j-i}$ by (c). Since $g_{j-i} \in S$ by the definition of u, we get $(b - c)n \in \Gamma'$ whence $b = c$ by the definition of v. So $0 \equiv g_{j-i} \in S$, showing that $g_{j-i} = 0$ whence $i = j$ by (a). ∎

(3.2) Lemma. *There exist unique integers* $w \in [0, v-1]$, $z \in [0, u-1]$, $\lambda \geq 1$, $\mu \geq 0$, $\nu \geq 2$, *such that* (a) $g_u = \lambda m_0 + wn$; (b) $vn = \mu m_0 + g_z$; (c) $g_{u-z} + (v-w)n = \nu m_0$.

Proof. The uniqueness of w and z is immediate from (3.1)(e), since $wn \equiv g_u$ and $g_z \equiv vn$, and the uniqueness of λ, μ, ν is now a consequence. We show their existence. Since $g_u - m_0 \in \Gamma$, we have $g_u = \lambda m_0 + g_i + wn$ with $\lambda \geq 1, i \geq 0$, $w \in [0, v-1]$ by (3.1)(d). By (3.1)(a) $i < u$ and by (3.1)(c) $g_{u-i} = (\lambda + \varepsilon)m_0 + wn \notin S$, since $\lambda \geq 1$. Therefore $i = 0$ and we get (a). Next, by (3.1)(d) write $vn = \mu m_0 + g_z$ with $\mu, z \geq 0$ and z minimal. Suppose $z \geq u$. Then by (3.1)(c) $vn = (\mu - \varepsilon)m_0 + g_{z-u} + g_u$ with $\varepsilon \in [0,1]$ whence by (a) $(v-w)n = (\mu - \varepsilon + \lambda)m_0 + g_{z-u} \in \Gamma'$. Therefore $w = 0$ by the definition of v, and we get a contradiction to the minimality of z. Thus $z < u$, proving (b). (c) is now immediate from (a), (b) and (3.1)(c), noting that $\nu \geq 2$, since $g_{u-z} > m_0$. ∎

In the sequel the symbols w, z, λ, μ, ν will have the meaning assigned to them by the above lemma.

Let $W = [u-z, u-1] \times [v-w, v-1]$. Let $\rho : V \to \Gamma$ be the map defined by $\rho(i,b) = g_i + bn$.

(3.3) Lemma. $S \subseteq \rho(V - W)$.

Proof. For $\gamma, \beta \in \Gamma$ write $\gamma \geq\equiv \beta$ to mean that $\gamma \geq \beta$ and $\gamma \equiv \beta$. Let $\gamma \in \Gamma$. Then by (3.1)(d) there exist $i, b \geq 0$ such that $\gamma \geq\equiv g_i + bn$. Choose this expression with i minimal. Suppose $i \geq u$. Then $g_i + \varepsilon m_0 = g_{i-u} + \lambda m_0 + wn$ with $\varepsilon \in [0,1]$ by (3.1)(c) and (3.2) whence $\gamma \geq\equiv g_{i-u} + (b+w)n$, a contradiction, proving that $i < u$. Now, among all expressions $\gamma \geq\equiv g_i + bn$ with $i \in [0, u-1], b \geq 0$, choose one with b minimal. Suppose $b \geq v$. Then $\gamma \geq\equiv g_{i+z} + (b-v)n$ by (3.1)(c) and (3.2), so that $i + z \geq u$ by the minimality of b. Write $i + z = j + u$. Then $j \in [0, u-1]$ and $g_{i+z} = (\lambda - \varepsilon)m_0 + g_j + wn \geq\equiv g_j + wn$ by (3.1)(c) and (3.2) whence $\gamma \geq\equiv g_j + (b - v + w)n$. This is a contradiction, since $b - v + w < b$. Thus $\gamma \geq\equiv g_i + bn$ with $(i,b) \in V$. Now, if $\gamma \in S$ then $\gamma = g_i + bn \in \rho(V)$. This proves that $S \subseteq \rho(V)$. If $(i,b) \in W$ then by (3.1)(c) and (3.2) $g_i + bn = (\nu - \varepsilon)m_0 + g_{i-u+z} + (b - v + w)n$ with $\nu > \varepsilon$ whence $\rho(i,b) \notin S$. Thus $S \subseteq \rho(V - W)$. ∎

(3.4) Lemma. *Let* $(i,b), (j,c) \in V - W$ *with* $g_i + bn \equiv g_j + cn$. *Then* $(i,b) = (j,c)$.

Proof. We may assume that $i \leq j$. Suppose $(i,b) \neq (j,c)$. Then $b < c$

by (3.1)(e). Now, $g_{j-i} + (c-b)n \equiv 0 \equiv g_{u-z} + (v-w)n$ by (3.1)(c) and (3.2). Since $(j,c) \notin W$, we have $j - i \leq j < u - z$ or $c - b \leq c < v - w$. Therefore by (3.1)(e) $j-i < u-z$ and $c-b < v-w$ whence $(j-i+z, 0)$ and $(0, v+b-c)$ are distinct points of V. Now, since $g_z \equiv vn$, we get $g_{j-i+z} \equiv (v+b-c)n$, contradicting (3.1)(e). ∎

(3.5) Theorem. *ρ induces a bijection $V - W \xrightarrow{\approx} S$.*

Proof. $\rho|_{V-W}$ is injective by (3.4) and $S \subseteq \rho(V-W)$ by (3.3). To show that $\rho(V-W) \subseteq S$, let $(i,b) \in V - W$. Then $\rho(i,b) \equiv \sigma$ for some $\sigma \in S$. By (3.3) $\sigma = \rho(j,c)$ with $(j,c) \in V - W$ whence $(i,b) = (j,c)$ by (3.4). Thus $\rho(i,b) \in S$. ∎

4. GENERATORS

Let $\mathcal{O} = K[[T^{m_0}, T^{m_1}, \ldots, T^{m_{e-1}}]]$, where K is a field, T is an indeterminate, $e \geq 3$ and $m_0, m_1, \ldots, m_{e-1}$ is an almost arithmetic sequence of positive integers. Our aim in this section is to construct generators for the module $\mathcal{D} = \mathrm{Der}_K(\mathcal{O})$ and the relation ideal P of $\mathcal{O}$.

Let Γ be the value semigroup of $\mathcal{O}$. Put $p = e - 2$. We may assume that $\gcd(\Gamma) = 1$ and that $m_0 \leq m_1 \leq \cdots \leq m_p$ is an arithmetic sequence. If $m_0 = m_p$ then $\mathcal{O}$ is a plane monomial curve in which case it is trivial to write down generators for $\mathcal{D}$ and P. We assume therefore that $m_0 < m_1 < \cdots < m_p$ and now use freely the notation of section 3.

(4.1) Theorem. *If char $(K) = 0$ then $\mu(\mathrm{Der}_K(\mathcal{O})) \leq 2e - 3$.*

Proof. Let
$H_1 = [u-p, u-1] \times \{v-w-1\}$, $H_2 = [u-z-p, u-z-1] \times \{v-1\}$, $H = H_1 \cup H_2$ and $I = V \cap H$. Put $\Gamma_+ = \Gamma - \{0\}$. Let $\Delta = \{\alpha \in \mathbb{Z}^+ \mid \alpha + \Gamma_+ \subseteq \Gamma\}$ and let $\Delta' = \Delta - \Gamma$. Then $\mathrm{Der}_K(\mathcal{O})$ is generated (minimally) by the set $\{T^{\alpha+1}\frac{d}{dT} \mid \alpha \in \Delta' \cup \{0\}\}$ [6, p. 875]. So it is enough to prove the following

(4.2) Lemma. $m_0 + \Delta' \subseteq \rho(I)$. *In particular,* $|\Delta'| \leq |\rho(I)| \leq 2p = 2e - 4$.

Proof. Let $\alpha \in \Delta'$ and write $\alpha = am_0 + \sigma$ with $a \in \mathbb{Z}, \sigma \in$ S. Since $\alpha \notin \Gamma$ and $\alpha + m_0 \in \Gamma$, we have $a = -1$ whence $m_0 + \alpha = \sigma$. By (3.5) write $\sigma = g_i + bn$ with $(i,b) \in V - W$. Since $\sigma + n - m_0 = \alpha + n \in \Gamma$, we have $\sigma + n \notin S$. Therefore $(i, b+1) \notin V - W$ by (3.5) whence

$b = v - w - 1$ or $b = v - 1$. Since $\sigma + m_p - m_0 = \alpha + m_p \in \Gamma$, we have $g_{i+p} + bn = \sigma + m_p \notin S$. Therefore $(i+p, b) \notin V - W$ by (3.5). It follows that if $b = v - w - 1$ (resp. $b = v - 1$) then $i + p \geq u$ (resp. $i + p \geq u - z$). Therefore $(i, b) \in I$ whence $\sigma \in \rho(I)$. ∎

(4.3) Theorem. *Let $R = K[[X_0, X_1, \ldots, X_{e-1}]]$ and let $P = \ker(\eta)$, where $\eta : R \to \mathcal{O}$ is given by $\eta(X_i) = T^{m_i}$. Then $\mu(P) \leq e(e-1)/2$.*

The generators are described explicitly in Theorem (4.5) below.

Let J be the ideal of R generated by $\{\xi_{ij} \mid i, j \in [1, p-1]\}$, where $\xi_{ij} = X_i X_j - X_0^{1-\varepsilon} X_{i+j-\varepsilon p} X_p^{\varepsilon}$ with $\varepsilon = 0$ or 1 according as $i + j \leq p$ or $i + j > p$.

Let $\mathcal{M}$ denote the set of all monomials in the X_i's. For $X^\alpha \in \mathcal{M}$ define $\partial(X^\alpha) = \deg_T \eta(X^\alpha)$. For $i \geq 0$ put $G_i = X_p^{q_i} X_{r_i}$. Then $\partial(G_i) = g_i$. Put $Y = X_{p+1}$. For $X^\alpha \in \mathcal{M}$ define $f(X^\alpha) = X^\alpha - X_0^a G_i Y^b$, where by (3.5) $a \geq 0$ and $(i, b) \in V - W$ are the unique elements satisfying the equality $\partial(X^\alpha) = \partial(X_0^a G_i Y^b)$. Then $f(X^\alpha) \in P$, $f(X_0^c X^\alpha) = X_0^c f(X^\alpha)$ for $c \geq 0$ and

$$(*) \qquad X^\alpha - X^\beta \in P \iff \partial(X^\alpha) = \partial(X^\beta)$$
$$\iff f(X^\alpha) - f(X^\beta) = X^\alpha - X^\beta.$$

Let $Q = J + (\theta, \varphi_0, \ldots, \varphi_{p-r_u}, \psi_0, \ldots, \psi_{p-r_{u-z}})$, where $\theta = Y^v - X_0^\mu G_z$, $\varphi_j = G_{u+j} - X_0^{\lambda-1} X_j Y^w$ and $\psi_j = G_{u-z+j} Y^{v-w} - X_0^{\nu-1} X_j$. Then $Q \subseteq P$ by (3.1) and (3.2) and, since $\xi_{ij} = \xi_{ji}$, $\mu(Q) \leq e(e-1)/2$.

(4.4) Lemma. (a) *If $i, j \geq 0$ and $X^\alpha \in \mathcal{M}$ then $f(G_i G_j X^\alpha) - X_0^\varepsilon f(G_{i+j} X^\alpha) \in J$ with $\varepsilon = 1$ or 0 according as $r_i + r_j \leq p$ or $r_i + r_j > p$.*

(b) *If $i \geq u$, $b \geq 0$ then $f(G_i Y^b) \in Q + (f(G_{i-u} Y^{b+w}))$.*

(c) *If $i \geq u - z$, $b \geq v - w$ then $f(G_i Y^b) \in Q + (f(G_{i-u+z} Y^{b-v+w}))$.*

Proof. (a) We have $G_i G_j - X_0^\varepsilon G_{i+j} = X_p^{q+s} \xi_{rt} \in J \subseteq P$, where $q = q_i, r = r_i, s = q_j, t = r_j$ and $\xi_{rt} = 0$ if $r = p$ or $t = p$. So (a) follows from $(*)$.

(b) Let $r = r_u, t = r_{i-u}$. Suppose $t + r \leq p$. Then $i = u + sp + t$ for some $s \geq 0$ whence $G_i = G_{sp} G_{u+t}$. Therefore $f(G_i Y^b) = G_{sp} Y^b \varphi_t + X_0^{\lambda-1} f(X_t G_{sp} Y^{b+w})$ by $(*)$, proving (b) in this case, since $X_t G_{sp} = G_{i-u}$. If $t + r > p$ then by (a) and $(*)$ $f(G_i Y^b) \in f(G_{i-u} G_u Y^b) + Q = G_{i-u} Y^b \varphi_0 + X_0^\lambda f(G_{i-u} Y^{b+w}) + Q$. This proves (b).

(c) is proved similarly by using ψ_j in place of φ_j. ∎

(4.5) Theorem. *The relation ideal P is generated by the set* $\{\xi_{ij} \mid 1 \le i \le j \le p-1\} \cup \{\theta, \varphi_0, \ldots, \varphi_{p-r_u}, \psi_0, \ldots, \psi_{p-r_{u-z}}\}$. *In particular,* $\mu(P) \le e(e-1)/2$.

Proof. For $j = 1,2,3$, let $Q_j = Q + (\{f(G_iY^b) \mid (i,b) \in U_j\})$, where $U_1 = V$, $U_2 = [0, u-1] \times \mathbb{Z}^+$ and $U_3 = \mathbb{Z}^+ \times \mathbb{Z}^+$. Then, since $Q \subseteq P$, it is enough to show that $P \subseteq Q_3 \subseteq Q_2 \subseteq Q_1 \subseteq Q$.

$P \subseteq Q_3$: It is easily checked that P is generated by binomials $X^\alpha - X^\beta$ with $\partial(X^\alpha) = \partial(X^\beta)$. Therefore by $(*)$ P is generated by $\{f(X^\alpha) \mid X^\alpha \in \mathcal{M}\}$. Writing $\alpha = (\alpha_0, \ldots, \alpha_{p+1})$ it is clear by induction on $\alpha_1 + \cdots + \alpha_{p-1}$ that there exist a, i, $b \ge 0$ such that $X^\alpha - X_0^a G_i Y^b \in J$ whence by $(*)$ $f(X^\alpha) \in X_0^a f(G_iY^b) + J \subseteq Q_3$. Thus $P \subseteq Q_3$.

$Q_3 \subseteq Q_2$: If $i \ge u$, $b \ge 0$ then $f(G_iY^b) \in Q + (f(G_{i-u}Y^{b+w}))$ by (4.4). Therefore by induction on i, $f(G_iY^b) \in Q_2$ for all $(i,b) \in U_3$.

$Q_2 \subseteq Q_1$: We show by induction on b that $f(G_iY^b) \in Q_1$ for all $(i,b) \in U_2$. This is clear if $b < v$. Suppose $b \ge v$. Then by $(*)$ $f(G_iY^b) = G_iY^{b-v}\theta + X_0^\mu f(G_iG_zY^{b-v})$ and by (4.4) $f(G_iG_zY^{b-v}) \in J + (F)$, where $F = f(G_{i+z}Y^{b-v})$. So it is enough to show that $F \in Q_1$. If $i + z < u$ then $F \in Q_1$ by induction. If $i + z \ge u$ then by (4.4) $F \in Q + (f(G_{i+z-u}Y^{b-v+w})) \subseteq Q_1$ by induction, since $(i+z-u, b-v+w) \in U_2$ and $b - v + w < b$.

$Q_1 \subseteq Q$: We show by induction on i that $f(G_iY^b) \in Q$ for all $(i,b) \in V$. If $(i,b) \in V - W$ (in particular, if $i = 0$) then $f(G_iY^b) = 0$. If $(i,b) \in W$ then by (4.4) $f(G_iY^b) \in Q + (f(G_{i-u+z}Y^{b-v+w})) \subseteq Q$ by induction, since $(i-u+z, b-v+w) \in V$ and $i - u + z < i$. ∎

(4.6) Examples. Let $p, q \in \mathbb{N}$. Let $m_i = 2q(2p+1) - p + i$ for $i \in [0,p]$, $n = m_{p+1} = m_0 + 2p + 1$ and $e = p + 2$. Then the bounds of Theorems (4.1) and (4.3) are attained, i.e. (a) $\mu(\mathrm{Der}_K(\mathcal{O})) = 2e - 3$ if char $(K) = 0$; (b) $\mu(P) = e(e-1)/2$.

Proof. (a) is proved by showing that the inclusion $m_0 + \Delta' \subseteq \rho(I)$ and the inequality $|\rho(I)| \le 2e - 4$ of (4.2) are equalities. To prove (b) it is checked that $r_u = r_{u-z} = 1$ and the set of generators for P given by (4.5) is minimal. See [8] for details. ∎

REFERENCES

[1] **Bresinsky, H.** : On prime ideals with generic zero $x = t^{n_i}$, Proc. Am. Math. Soc. **47**, 329-332 (1975)

[2] **Bresinsky, H.** : Symmetric semigroups of integers generated by 4 elements, Manuscr. Math. **17**, 205-219 (1975)

[3] **Herzog, J.** : Generators and relations of abelian semigroups and semigroup rings, Manuscr. Math. **3**, 175-193 (1970)

[4] **Kunz E., Waldi, R.** : Über den Derivationenmodul und das Jacobi-Ideal von Kurvensingularitäten, Math. Z. **187**, 105-123 (1984)

[5] **Kraft, J.** : Singularity of monomial curves, Thesis, Purdue University, 1983

[6] **Kraft, J.** : Singularity of monomial curves in $\mathbb{A}^3$ and Gorenstein monomial curves in $\mathbb{A}^4$, Can. J. Math. **37**, 872-892 (1985)

[7] **Moh, T.T.** : On generators of ideals, Proc. Am. Math. Soc. **77**, 309-312 (1979)

[8] **Patil, D.P., Singh, Balwant** : Generators for the derivation modules and the prime ideals of certain curves, Preprint, Tata Inst. Fundam. Res., Bombay, 1990

[9] **Patil, D.P.** : Certain monomial curves are set-theoretic complete intersections, Manuscr. Math.

[10] **Selmer, E.S.** : On the linear Diophantine problem of Frobenius, J. Reine Angew. Math. **293/294**, 1-17 (1977)

School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road
Bombay 400005, India.

(Received March 31, 1990;
in revised form June 22, 1990)