Kähler differentials of affine monomial curves*

S. Geller[1], Alok Kumar Maloo[2], D. P. Patil[3] and L. G. Roberts[4]

[1] Department of Mathematics, Texas A & M University, College Station, Texas 77802, USA.
E-mail : geller@math.tamu.edu

[2] Department of Mathematics, Indian Institute of Technology, Kanpur 208 016, UP, India.
E-Mail : akmaloo@iitk.ernet.in

[3] Department of Mathematics, Indian Institute of Science, Bangalore 560 012, India.
E-mail : patil@math.iisc.ernet.in

[4] Department of Math. and Stat., Queen's University, Kingston, Ontario, Canada, K7L 3N6.
E-mail : robertsl@mast.QueensU.CA

§0 Introduction.

For a field k and a k-algebra C let $\Omega^1_{C/k}$ denote the module of Kähler differentials, $d_C : C \to \Omega^1_{C/k}$ the universal derivation, $\Omega^q_{C/k} = \Lambda^q_C(\Omega^1_{C/k})$ for $q \geq 0$ and $\Omega^*_{C/k} = \oplus_{q\geq 0}\Omega^q_{C/k}$. For simplicity of notation, we will write d instead of d_C. For a submonoid Γ of $\mathbb{Z}^+ = \{0, 1, 2, \ldots\}$, let $k[\Gamma]$ be the monoid ring of Γ. In this paper we describe $\Omega^*_{k[\Gamma]/k}$ in the case where characteristic $k = 0$ and Γ is generated by an arithmetic progression.

For fixed integers m, p, d with $m \geq 2,\ 1 \leq p \leq m-1,\ d \geq 1,\ \gcd(m, d) = 1$ we define $m_i = m + id,\ (i \in \mathbb{Z}^+, 0 \leq i \leq p),\ S = \{m_0, m_1, m_2, \ldots, m_p\}$ and Γ to be the monoid generated by the arithmetic progression S. We will write A for $k[\Gamma] = k[t^{m_0}, t^{m_1}, \ldots, t^{m_p}]$. The ring A is graded by weight if we set $\mathrm{wt}(t) = 1$ and grade the A-modules $\Omega^q_{A/k}$ by in addition setting $\mathrm{wt}(dt) = 1$. It should be clear from the context whether d denotes the differential or the common difference of the arithmetic progression. The n-th weight piece of $\Omega^q_{A/k}$ will be denoted by $(\Omega^q_{A/k})_n$.

This work is motivated in part by the relation between the $\Omega^q_{k[\Gamma]/k}$ and K-Theory, as discussed for example in [6 ; appendix]. It is hoped that the results obtained here will at least partially survive in subrings of $k[t]$ that are not generated by monomials, for example as considered in [2]. We expect our calculation to yield interesting invariants of the singularity of $k[\Gamma]$ at the origin or of the monoid Γ itself.

In § 3 we compute $\dim_k(\Omega^1_{A/k})_n$ in terms of partitions of n as the sum of integers from the set S. For general Γ, $\dim_k(\Omega^1_{k[\Gamma]/k})_n$ is likely too fine an invariant to be easily interpreted. However in the arithmetic progression case we are able to give a combinatorial interpretation in terms of certain subsets of S that are introduced in § 2. This was surprising to us and fails if either the characteristic of k is non-zero or S is not an arithmetic progression. In § 4 we determine the index of regularity of $\Omega^1_{A/k}$ and in § 5 we describe an interesting relationship between the Hilbert functions of $\Omega^1_{A/k}$ and $\Omega^1_{A'/k}$ where $A' = k[t^m, t^{m+1}, \ldots, t^{m+p}]$. Another motivation for this

*This work was partially supported by the NSERC grant of the fourth author. The first and third authors thank Department of Mathematics and Statistics, Queen's University, Kingston, Canada for its hospitality. The second author thanks Department of Mathematics, Indian Institute of Science, Bangalore for its hospitality.

paper was to explain the symmetry of the Hilbert function of $\Omega^1_{A/k}/dA$ proved in [6] in the case where $p = m-1$ and $d = 1$. In § 5 we generalize this result to the case $p = m-1, d > 1$. Our improved methods suggest that the symmetry is an accident. In § 6 we completely describe $\Omega^q_{A/k}$ for $q \geq 3$, generalizing the result of [7] to the case $p \leq m-1$. This permits us to determine the Hilbert function of $\Omega^2_{A/k}$ in terms of $\Omega^1_{A/k}$ and the Gaussian polynomials. In each section examples are given to illustrate the results.

§1 Presentation of $\Omega^1_{A/k}$.

In addition to the notation fixed in the introduction, let $\varphi : R = k[X_0, \ldots, X_p] \longrightarrow A$ be the k-algebra homomorphism defined by $X_i \mapsto t^{m_i}$, $0 \leq i \leq p$, and let $\mathfrak{p}$ be the kernel of φ. For $0 \leq i \leq p$, define $x_i = t^{m_i}$, $\deg(X_i) = 1$ and $\mathrm{wt}(X_i) = m_i$. Then $\mathfrak{p}$ is homogeneous if R is graded by weight, but not if R is graded by degree.

Recall (from [3 ; (4.13)]) the presentation for $\Omega^*_{A/k}$ given by $\Omega^*_{A/k} \cong \Omega^*_{R/k}/(\mathfrak{p}, d\mathfrak{p})$, where $(\mathfrak{p}, d\mathfrak{p})$ is the 2-sided ideal of $\Omega^*_{R/k}$ generated by $\{F, dF \mid F \in \mathfrak{p}\}$.

For $\mathbf{a} = (a_0, \ldots, a_p) \in (\mathbb{Z}^+)^{p+1}$, let $X^{\mathbf{a}} = \prod_{i=0}^p X_i^{a_i}$. The image of a monomial $X^{\mathbf{a}} \in R$ of weight $n = \sum_{i=0}^p a_i m_i$ in A is t^n. Therefore the n-th weight piece $\mathfrak{p}_n$ of $\mathfrak{p}$ is generated by binomials $\{X^{\mathbf{a}} - X^{\mathbf{b}} \mid \sum_{i=0}^p a_i m_i = \sum_{i=0}^p b_i m_i = n\}$ as a k-vector space. (An explicit minimial set of ideal generators for $\mathfrak{p}$ is given in [5 ; (4.5)]).

It is more convenient to consider $\Omega^1_{A/k}/dA$ rather than $\Omega^1_{A/k}$ as we then have a simpler presentation. But we should be careful to remember that $\Omega^1_{A/k}/dA$ is only a k-vector space, not an A-module.

(1.1) Theorem. *Let m, p, d be positive integers with $\gcd(m, d) = 1$ and let $A = k[t^{m_0}, t^{m_1}, t^{m_2}, \ldots, t^{m_p}]$. For any non-negative integer n, let V_n be the k-vector space with basis $\{t^{n-m_i} dt^{m_i} \mid i \in [0, p],\ t^{n-m_i} \in A, n - m_i \neq 0\}$, and W_n the subspace of V_n spanned by $\{\sum_{i=0}^p a_i t^{n-m_i} dt^{m_i} \mid \sum_{i=0}^p a_i m_i = n,\ a_i \geq 0\}$. Then $(\Omega^1_{A/k}/dA)_n \cong V_n/W_n$.*

Proof. Since $\Omega^1_{R/k}$ is the free R-module with basis $dX_0, \ldots, dX_p$, we have that $\Omega^1_{R/k} \otimes_R A = \Omega^1_{R/k}/(\mathfrak{p}\Omega^1_{R/k})$ is a free A-module with basis $dx_0, \ldots, dx_p$. We know that $\mathfrak{p}$ is generated by $\{X^{\mathbf{a}} - X^{\mathbf{b}} \mid \sum_{i=0}^p a_i m_i = \sum_{i=0}^p b_i m_i = n\}$ and $dt^n = d((t^{m_0})^{a_0} \ldots (t^{m_p})^{a_p}) = \sum_{i=0}^p a_i (t^{m_0})^{a_0} \ldots (t^{m_i})^{a_i - 1} \ldots (t^{m_p})^{a_p}\, dt^{m_i}$ for $(a_0, \ldots, a_p)$ with $\sum_{i=0}^p a_i m_i = n$. Since $(\Omega^1_{A/k}/dA)_n$ is $(\Omega^1_{R/k}/(\mathfrak{p}\Omega^1_{R/k}, d\mathfrak{p}))_n$ modulo dt^n, the assertion follows. ∎

(1.2) Remark. For large n, $\dim_k(\Omega^1_{A/k})_n = 1$ and $\dim_k(\Omega^q_{A/k})_n = 0$ for all $q \geq 2$. If $i, j \in \Gamma$, $j > 0$ then $t^i dt^j \neq 0$ in $\Omega^1_{A/k}$.

Proof. Since the quotient field of A is $k(t)$ and $\Omega^q_{A/k} \otimes_A k(t) \cong \Omega^q_{k[t]/k} \otimes_A k(t) \cong \Omega^q_{k(t)/k}$ for all $q \geq 0$, the assertions follow. ■

Before translating (1.1) into explicit results about $\Omega^1_{A/k}$, we will make some remarks about partitions.

§2 Partitions.

In addition to the notation previously introduced, for non-negative integers a, b, let $[a, b, d]$ denote $\{a + id \mid i \in \mathbb{Z}^+, a + id \leq b\}$, Floor$[a]$ the largest integer less than or equal to a, and Ceiling$[a]$ the smallest integer greater than or equal to a. We will write $[a, b]$ instead of $[a, b, 1]$. Note that in this notation the set $S = [m, m + pd, d]$.

For integers n, r, let $S(n, r)$ to be the set of all integers in S that can occur in a partition of n as a sum of r elements of S, that is,

$$S(n, r) = \{m_j \mid n = \sum_{i=0}^{p} a_i m_i \ \text{ with } \sum_{i=0}^{p} a_i = r \ \text{ and } \ a_j \neq 0\}\,.$$

Let $S(n) = \cup_{r \geq 1} S(n, r)$. Further, the cardinality $|S(n, r)|$ of $S(n, r)$ will be denoted by $s(n, r)$ and $P(n) = \{r \in \mathbb{Z}^+ \mid S(n, r) \neq \emptyset\}$.

For example, if $m = 6,\ p = 2,\ d = 1$, then $S = \{6, 7, 8\}$, $S(14, 2) = \{6, 7, 8\}$ since we have $14 = 7 + 7 = 6 + 8$, $S(18, 3) = \{6\}$ since 18=6+6+6 is the only way to write 18 as the sum of three elements of S, and $S(17, 3) = \emptyset$.

The set $\{m_j \mid 0 \leq j \leq p$ and $a_j \neq 0\}$ is called the support of the partition $n = \sum_{i=0}^{p} a_i m_i$ of n, and the integer $1 + (l - s)$ is called the spread of this partition, where m_l and m_s are the largest and smallest element in the support respectively.

For example, if $S = \{5, 7, 9, 11\}$ then the partition $5 + 5 + 9 + 11$ of 30 has support $\{5, 9, 11\}$ and spread 4. Note that if $S(n, r) \neq \emptyset$ then $n \equiv rm \bmod d$. A partition of n with spread 1 is of the form $n = rx, x \in S$.

(2.1) Lemma. *Let n, r be non-negative integers.*

(a) *For $x \in S$, $n - x$ lies in the monoid generated by S if and only if $x \in S(n)$. In particular V_n has basis $\{t^{n-m_i} dt^{m_i} \mid m_i \in S(n)\}$.*

(b) *$S(n, 2) \cap S(n, r) = \emptyset$ for $r > 2$.*

(c) *If $S(n, r) \neq \emptyset$ then n has a partition as the sum of r elements of S with either spread 1 or 2, but not both.*

(d) *There are exactly* Ceiling$[s(n, 2)/2]$ *partitions of n as the sum of two elements of S. More precisely, $n = m_s + m_l = m_{s+1} + m_{l-1} = \cdots\cdots = m_{s+j} + m_{l-j}$, where m_l and m_s are the largest and smallest elements of $S(n, 2)$ respectively and $j = \Big(\text{Ceiling}[\frac{s(n,2)}{2}] - 1\Big)$.*

(e) *If $r \geq 3$ then for $i = 3, \ldots, s(n,r)$ there is a partition of n as the sum of r elements of S with spread i. Furthermore these partitions can be chosen to have "nested" supports* (see example (2.2) below).

(f) *For fixed r, $\{n \mid S(n,r) \neq \emptyset\} = [rm, rm_p, d]$, which is a set of consecutive elements in the congruence class of rm mod d. Moreover, if $n = rm + jd$, $0 \leq j \leq rp$ then*

$$S(n,r) = \begin{cases} [m, m_j, d] & \text{if } 0 \leq j \leq p-1 \\ S & \text{if } p \leq j \leq (r-1)p \\ [m_{j-(r-1)p}, m_p, d] & \text{if } (r-1)p+1 \leq j \leq rp. \end{cases}$$

Explicitly, $S(n,r) = [\max(m, n-(r-1)m_p), \min(m_p, n-(r-1)m), d]$, which is a set of consecutive elements of S containing either m or m_p (or both).

(g) *For fixed n, $P(n)$ is a set of consecutive elements in a congruence class mod d.*

(h) *If $S(n,r) \neq \emptyset$ and $S(n,r+d) \neq \emptyset$ then $m \in S(n,r+d)$ and $m_p \in S(n,r)$. If $S(n,r)$, $S(n,r+d)$ and $S(n,r+2d)$ are all non-empty then $S(n,r+d) = S$.*

Proof. (a) Straightforward from the definitions.

(b) Immediate since S is the minimal set of generators of Γ.

(c) Since $S(n,r) \neq \emptyset$ we have $n = rm + id$ where $0 \leq i \leq rp$. Write $i = \alpha r + \beta$ with $0 \leq \beta \leq r-1$. Then, $\beta = 0 \iff n = rm_\alpha \iff n$ has a partition with spread 1. If $\beta > 0$ then $\alpha \leq p-1$ so $m_\alpha, m_{\alpha+1} \in S$. Therefore $n = (r-\beta)m_\alpha + \beta m_{\alpha+1}$ expresses n as the sum of r elements of S with spread 2.

(d) is straightforward to verify.

(e) If $r \geq 3$ we can increase the spread of the partition in the proof of (c) 1 at a time (by 2 when going from spread 1 to spread 3) by replacements of the type $m_i + m_j \mapsto m_{i-1} + m_{j+1}$, $1 \leq i \leq j \leq p-1$ which proves (e).

(f) is straightforward to verify.

(g) From (f) we have $S(n,r) \neq \emptyset \iff n \equiv rm \bmod d$ and $rm \leq n \leq r(m+pd) \iff r \equiv m'n \pmod{d}$ and $n/(m+pd) \leq r \leq n/m$, where m' is an inverse mod d of m.

(h) follows from (f). ∎

(2.2) Example. Let $m = 5, d = 2$ and $p = 3$. Then $S = \{5,7,9,11\}$ and for $n = 32, r = 4$, we have $n = 7+7+9+9 = 7+7+7+11 = 5+7+9+11$. The supports of these partitions are $\{7,9\}, \{7,11\}, \{5,7,9,11\}$ respectively. By "nested" we mean that $[7,9] \subset [7,11] \subset [5,11]$, i.e. the smallest intervals containing the supports are nested.

(2.3) Lemma. *Let n and r be non-negative integers and let $n = \sum_{i=0}^{p} c_i(m+id)$ be a partition of n as the sum of r elements of S. Let $\mathbf{c} = (c_0, \ldots, c_p)$ and $\mathbf{b}_r = (b_{r,0}, \ldots, b_{r,p})$ where $b_{r,i} = rm_i - n$. Then $\mathbf{b}_r \cdot \mathbf{c} = 0$. Furthermore if m_s and m_l are the smallest, respectively largest, elements of $S(n,r)$ then $b_{r,s} < 0$ and $b_{r,l} > 0$.*

Proof. We have $n = \sum_{i=0}^{p} c_i m_i$, $c_i \geq 0$ for all $0 \leq i \leq p$ and $\sum_{i=0}^{p} c_i = r$. Therefore $0 = rn - rn = r\left(\sum_{i=0}^{p} c_i m_i\right) - n\left(\sum_{i=0}^{p} c_i\right) = \sum_{i=0}^{p}(rm_i - n)c_i = \mathbf{b}_r \cdot \mathbf{c}$. The second part follows from the fact that the co-ordinates of $\mathbf{b}_r$ are in an increasing arithmetic progression and the $\mathbf{c}$ have non-negative co-ordinates. ∎

The notation $S(n,r), s(n,r), P(n)$ introduced in this section will be used later without explicit reference.

§3 The Hilbert function of $\Omega^1_{A/k}$.

In this section we use the results on partitions in § 2 to determine the Hilbert function of $\Omega^1_{A/k}$.

(3.1) Definition. For n, r positive integers let $V_{n,r}$ be the k-vector space with basis $\{t^{n-m_i}dt^{m_i} \mid m_i \in S(n,r)\}$ and let $W_{n,r}$ be the k-subspace of $V_{n,r}$ spanned by $\{\sum_{i=0}^{p} a_i t^{n-m_i} dt^{m_i} \mid a_i \geq 0,\ \sum_{i=0}^{p} a_i = r,\ \sum_{i=0}^{p} a_i m_i = n\}$.

Note that $V_n = \sum_r V_{n,r}$ and $W_n = \sum_r W_{n,r}$ where V_n and W_n are as in (1.1).

(3.2) Lemma. *Let n, r be positive integers and let $\mathbf{b}_r = (rm_0 - n, \cdots, rm_p - n)$ as in* (2.3).

(a) $W_{n,r} \subseteq \mathbf{b}_r^{\perp} = \{\sum_{m_i \in S(n,r)} \lambda_i t^{n-m_i} dt^{m_i} \in V_{n,r} \mid \sum \lambda_i b_{r,i} = 0\}$.

(b) $V_{n,1}/W_{n,1} = 0$.

(c) $\dim_k V_{n,2}/W_{n,2} = \mathrm{Floor}[s(n,2)/2]$ *with relations*

$$\{t^{m_j}dt^{m_i} + t^{m_i}dt^{m_j} = 0 \mid n = m_i + m_j,\ 0 \leq i \leq j \leq p\}.$$

(d) *Suppose that $r \geq 3$. If $m_i \in S(n,r)$ and $b_{r,i} \neq 0$ then*

$$\{b_{r,i}t^{n-m_j}dt^{m_j} - b_{r,j}t^{n-m_i}dt^{m_i} \mid m_j \in S(n,r), j \neq i\}$$

is a basis of $W_{n,r}$. In particular, equality holds in (a) *and*

$$\dim_k V_{n,r}/W_{n,r} = \begin{cases} 0 & \text{if } s(n,r) = 1 \\ 1 & \text{if } s(n,r) > 1 \end{cases}$$

Moreover, if $s(n,r) > 1$ then $t^{n-m_i}dt^{m_i}$ is a basis for $V_{n,r}/W_{n,r}$ provided $b_{r,i} \neq 0$ (in particular, by (2.3)*, m_i can be either the largest or the smallest element of $S(n,r)$).*

Proof. (a) and (b) are immediate from (2.3) and (2.1a). (c) Follows from (2.1d).

(d) If $s(n,r)=1$ then $\dim_k V_{n,r}=1$ and $W_{n,r}\neq 0$, so $V_{n,r}/W_{n,r}=0$. If $s(n,r)>1$ then $\dim_k V_{n,r}/W_{n,r}\leq 1$ by the "nested" part of (2.1d) and $\dim_k V_{n,r}/W_{n,r}\geq 1$ by (a) since $\mathbf{b}_r$ has at most one co-ordinate equal to 0. Now, the equality in (a) follows. ■

Note that (3.2) permits effective computation in $\Omega^1_{A/k}/dA$, not just the computation of Hilbert functions. It is not difficult to lift this computation to $\Omega^1_{A/k}$ and, using the results of § 6, to $\Omega^2_{A/k}$. However we will not pursue the latter.

(3.3) Lemma. *Let n, r be positive integers. Then*

(a) *If $P(n)=\{r\}$ then $(\Omega^1_{A/k}/dA)_n = V_{n,r}/W_{n,r}$.*

(b) *If $S(n,r)\neq\emptyset$, $S(n,r+d)\neq\emptyset$, and $S(n,r)\cap S(n,r+d)=\emptyset$, then $(\Omega^1_{A/k}/dA)_n = V_{n,r}/W_{n,r}\oplus V_{n,r+d}/W_{n,r+d}$.*

(c) *If $s(n,r)\geq 2$, $s(n,r+d)\geq 2$ and $|S(n,r)\cap S(n,r+d)|=1$, then $\dim_k(\Omega^1_{A/k}/dA)_n = 1$.*

(d) *If $|S(n,r)\cap S(n,r+d)|=1$ and either $s(n,r)=1$ or $s(n,r+d)=1$, then $(\Omega^1_{A/k}/dA)_n=0$.*

(e) *If $|S(n,r)\cap S(n,r+d)|\geq 2$ then $(\Omega^1_{A/k}/dA)_n=0$. In particular, if $|P(n)|\geq 3$ then $\left(\Omega^1_{A/k}/dA\right)_n=0$.*

Proof. (a) Follows from (1.1), since $V_n=V_{n,r}$, $W_n=W_{n,r}$.

(b) $V_n=V_{n,r}\oplus V_{n,r+d}$ and $W_n=W_{n,r}\oplus W_{n,r+d}$ since $S(n,s)=\emptyset$ for $s\neq r, r+d$ by (2.1h). The assertion now follows from (1.1).

(c) Since $|S(n,r)\cap S(n,r+d)|=1$ we have $r\geq 3$ by (2.1b) and $S(n,s)=\emptyset$ if $s\neq r, r+d$ by (2.1h). Suppose $S(n,r)\cap S(n,r+d)=m_i$. By (2.1h), m_i is the smallest element of $S(n,r)$ and the largest of $S(n,r+d)$. By (2.3) $b_{r,i}\neq 0$ and $b_{r+d,i}\neq 0$. Now (c) follows from (3.2d) and (1.1).

(d) If $|S(n,r)\cap S(n,r+d)|=1$ and $s(n,r)=1$ then $S(n,r)=\{m_p\}$ and $S(n,r+d)=S$ by (2.1h) and (2.1f). By (3.2d) $V_{n,r+d}/W_{n,r+d}$ is one dimensional with basis $t^{n-m_p}dt^{m_p}$. Furthermore the canonical map $V_{n,r+d}/W_{n,r+d}\to(\Omega^1_{A/k}/dA)_n$ is onto. Since $S(n,r)=\{m_p\}$ we have $n=rm_p$ from which it follows that $t^{n-m_p}dt^{m_p}\in W_{n,r}$ and hence $t^{n-m_p}dt^{m_p}=0$ in $(\Omega^1_{A/k}/dA)_n$. Therefore $(\Omega^1_{A/k}/dA)_n=0$ as claimed. If $|S(n,r)\cap S(n,r+d)|=1$ and $s(n,r+d)=1$ then $S(n,r)=S$ and $S(n,r+d)=\{m\}$. From this it follows similarly that $(\Omega^1_{A/k}/dA)_n=0$.

(e) Since $|S(n,r)\cap S(n,r+d)|>1$ we have $r\geq 3$ by (2.1b). By (3.2d) $W_{n,r}=\mathbf{b}_r^{\perp}, W_{n,r+d}=\mathbf{b}_{r+d}^{\perp}$. Suppose that $m_i, m_j\in S(n,r)\cap S(n,r+d)$, $i\neq j$. Then

$b_{r,j}t^{n-m_i}dt^{m_i} - b_{r,i}t^{n-m_j}dt^{m_j} \in W_{n,r}$ and $b_{r+d,j}t^{n-m_i}dt^{m_i} - b_{r+d,i}t^{n-m_j}dt^{m_j} \in W_{n,r+d}$. Since the determinant of the coefficient matrix is $(m_i - m_j)nd \neq 0$, by (1.1) $t^{n-m_i}dt^{m_i} = t^{n-m_j}dt^{m_j} = 0$ in $\Omega^1_{A/k}/dA$. Thus $(\Omega^1_{A/k}/dA)_n = 0$ by (3.2d) and (2.1h). Finally if $|P(n)| \geq 3$ then either $|S(n,r) \cap S(n,r+d)| \geq 2$ for some r, in which case we have just proved that $(\Omega^1_{A/k}/dA)_n = 0$, or $s(n,r) = 1$, $S(n,r+d) = S$ and $s(n,r+2d) = 1$ for some r. In this case $(\Omega^1_{A/k}/dA)_n = 0$ by (3.3d). ■

The $S(n,r)$ are described explicitly in (2.1). These sets completely determine the Hilbert function of $\Omega^1_{A/k}$:

(3.4) Theorem. *Let m, p, d be integers with $m \geq 2$, $1 \leq p \leq m-1$, $d \geq 1$, and* $\gcd(m,d) = 1$. *Let $A = k[t^m, t^{m+d}, \ldots, t^{m+pd}]$ and let $H : \mathbb{Z}^+ \to \mathbb{Z}^+$, where $H(n) =$* $\dim_k(\Omega^1_{A/k})_n$, *be the Hilbert function of $\Omega^1_{A/k}$. Then for any $n \in \mathbb{Z}^+$ we have:*

(a) *$H(0) = 0$ and* $H(n) = \begin{cases} 0 & \text{if } S(n) = \emptyset \\ 1 + \dim_k(\Omega^1_{A/k}/dA)_n & \text{if } S(n) \neq \emptyset \end{cases}$.

(b) *Suppose that $P(n) = \{r\}$. Then*
$$H(n) = \begin{cases} 1 & \text{if } s(n,r) = 1 \\ 1 + \mathrm{Floor}[s(n,2)/2] & \text{if } r = 2 \text{ and } s(n,2) > 1 \\ 2 & \text{if } r > 2 \text{ and } s(n,r) > 1 \end{cases}.$$

(c) *Suppose that there are distinct integers r_1, r_2 such that $\emptyset \neq S(n,r_1) \subseteq S(n,r_2)$. Then $H(n) = 1$. In particular, if $|P(n)| \geq 3$ then $H(n) = 1$.*

(d) *Suppose that $|P(n)| = 2$. Then there is an integer $r \geq 2$ such that $S(n,r) \neq \emptyset$ and $S(n,r+d) \neq \emptyset$.*

(d1) *Suppose that $S(n,r) \cap S(n,r+d) = \emptyset$* (which is necessarily the case if $r = 2$). *Then if $r = 2$*
$$H(n) = \begin{cases} 1 + \mathrm{Floor}[s(n,2)/2] & \text{if } s(n,2+d) = 1 \\ 2 + \mathrm{Floor}[s(n,2)/2] & \text{if } s(n,2+d) > 1 \end{cases}$$
and if $r > 2$
$$H(n) = \begin{cases} 1 & \text{if } s(n,r) = 1,\ s(n,r+d) = 1 \\ 2 & \text{if exactly one of } s(n,r),\ s(n,r+d) \text{ is } 1 \\ 3 & \text{if } s(n,r) > 1,\ s(n,r+d) > 1 \end{cases}.$$

(d2) *Suppose that $|S(n,r) \cap S(n,r+d)| = 1$* (necessarily $r > 2$). *Then*
$$H(n) = \begin{cases} 1 & \text{if one of } s(n,r),\ s(n,r+d) \text{ is } 1 \\ 2 & \text{if both } s(n,r) > 1,\ s(n,r+d) > 1. \end{cases}$$

(d3) *Suppose that $|S(n,r) \cap S(n,r+d)| > 1$. Then $H(n) = 1$.*

Proof. (a) The final assertion of (a) follows from (1.2). (b) Follows from (3.2c), (3.2d), and (3.3a). (c) Follows from (3.3d) and (3.3e). (d) (d1) Follows from (3.3b), (3.2c), and (3.2d). (d2) Follows from (3.3c) and (3.3d). (d3) follow from (3.3e). ∎

(3.5) Examples. The following examples show that all the cases in (3.4) can occur. For use in the table we number consecutively the cases in each part of (3.4). For example, (3.4d1)(case 3) means (among the cases of (3.4d1)) $r > 2$ and $s(n,r) = 1 = s(n, r+d)$. This case can occur only if $p = 1$ by (2.1h). The hardest to find is (3.4d2)(case 2).

(m,p,d)	S	n	$P(n)$	r	$S(n,r)$	$H(n)$	Reason
$(4,3,1)$	$\{4,5,6,7\}$	4	$\{1\}$	1	$\{4\}$	1	(3.4b)(case 1)
		11	$\{2\}$	2	$\{4,5,6,7\}$	3	(3.4b)(case 2)
		15	$\{3\}$	3	$\{4,5,6,7\}$	2	(3.4b)(case 3)
		12	$\{2,3\}$	2	$\{5,6,7\}$	2	(3.4d1)(case 1)
				3	$\{4\}$		
		13	$\{2,3\}$	2	$\{6,7\}$	3	(3.4d1)(case 2)
				3	$\{4,5\}$		
		16	$\{3,4\}$	3	$\{4,5,6,7\}$	1	(3.4d2)(case 1)
				4	$\{4\}$		
		17	$\{3,4\}$	3	$\{4,5,6,7\}$	1	(3.4c) or (3.4d3)
				4	$\{4,5\}$		
		20	$\{3,4,5\}$	3	$\{6,7\}$	1	
				4	$\{4,5,6,7\}$		
				5	$\{4\}$		(3.4c)
$(3,1,1)$	$\{3,4\}$	12	$\{3,4\}$	3	$\{4\}$	1	(3.4d1)(case 3)
				4	$\{3\}$		
$(9,4,1)$	$\{9,\ldots,13\}$	36	$\{3,4\}$	3	$\{10,\ldots,13\}$	2	(3.4d1)(case 4)
				4	$\{9\}$		
		37	$\{3,4\}$	3	$\{11,12,13\}$	3	(3.4d1)(case 5)
				4	$\{9,10\}$		
$(12,6,1)$	$\{12,\ldots,18\}$	49	$\{3,4\}$	3	$\{13,\ldots,18\}$	2	(3.4d2)(case 2)
				4	$\{12,13\}$		

We conclude this section with the following interesting application of (3.2) and (3.3).

(3.6) Proposition. *Let $\Gamma^1 \subseteq \Gamma$ the monoid generated by $S^1 = \{m_s, m_{s+1}, \ldots, m_l\} \subseteq S$ and let $A^1 = k[\Gamma^1]$. Then, for all n, the induced homomorphism of k-vector spaces $\omega_n : (\Omega^1_{A^1/k}/dA^1)_n \to (\Omega^1_{A/k}/dA)_n$ is either injective or surjective.*

Proof. The notation of §2 and §3 will be applied to A^1 by applying ^{1} to the corresponding notation for A. Then $S^1(n,r) \subseteq S(n,r)$ for all r, n so $P^1(n) \subseteq P(n)$. If $|P(n)| \geq 3$

then $(\Omega^1_{A/k}/dA)_n = 0$ by (3.3e) so ω_n is surjective. From $V^1_{n,r} \cap W_{n,r} = W^1_{n,r}$ we have an inclusion $V^1_{n,r}/W^1_{n,r} \hookrightarrow V_{n,r}/W_{n,r}$. It follows from this that if $|P(n)| = 1$ or if $|P(n)| = 2$, say $P(n) = \{r, r+d\}$, and $S(n,r) \cap S(n, r+d) = \emptyset$ (which is the case if $r = 2$ by (2.1b)), then ω_n is injective by (3.3b). The only case remaining is $P(n) = \{r, r+d\}, r \geq 3$ and $S(n,r) \cap S(n,r+d) \neq \emptyset$. If $|S(n,r) \cap S(n,r+d)| > 1$ or if one of $S(n,r)$ or $S(n,r+d)$ is a singleton, then $(\Omega^1_{A/k}/dA)_n = 0$ by (3.2d,e) and ω_n is surjective. If $|S(n,r) \cap S(n,r+d)| = 1$, $s(n,r) > 1$, and $s(n,r+d) > 1$ then $\dim_k(\Omega^1_{A/k}/dA)_n = 1$ by (3.3c). In this case if $(\Omega^1_{A^1/k}/dA^1)_n = 0$ then ω_n is an injection; otherwise by (1.1) $\Omega^1_{A^1/k}/dA^1$ contains non-zero elements of the form $t^{n-m_i}dt^{m_i}$, $m_i \in S^1$. Any such element maps to a non-zero element in $(\Omega^1_{A/k}/dA)_n$ by (3.2d) and (3.3c) so ω_n is surjective. ∎

(3.7) Corollary. *For fixed non-negative integers m, d and n, with $\gcd(m,d) = 1$, the function $p \mapsto \dim_k(\Omega^1_{A/k}/dA)_n$ is a unimodal function of p on the interval $[1, m-1]$.*

Proof. Recall that A depends on parameters m, p and d. As p ranges from 1 to $m-1$ we get an increasing sequence of monoids, to which we apply (3.6) in weight n. The assertion is then immediate from the fact that a composition of k-vector space homomorphisms $V_1 \to V_2 \to V_3$ cannot be injective or surjective if $\dim_k(V_2) < \min\{\dim_k V_1, \dim_k V_3\}$. ∎

§4 The index of regularity of $\Omega^1_{A/k}$.

The least integer N such that $\dim_k A_n = 1$ for all $n \geq N$ is called the conductor or index of regularity of A. It follows from [4 ; Ch. 3, (5.24)] that if we define integers $q \geq 1$, $1 \leq r \leq p$ by the equation $m = qp + r$, then the index of regularity of A is $qm_p + m_{r-1} - m + 1$ if $r > 1$ and $qm_p - m + 1$ if $r = 1$. Similarly, we define the "index of regularity" of $\Omega^1_{A/k}$ to be the least integer n_0 such that $\dim_k(\Omega^1_{A/k})_n = 1$ for all $n \geq n_0$, which exists by (1.2). In this section we shall determine n_0 explicitly.

Let ℓ be an integer with $2 \leq \ell \leq d+1$. Then

$$((\ell + id)m - d) - ((\ell + (i-2)d)m_p) = 2dm - d\,(1 + (\ell + (i-2)d)p)$$

is positive if $i = 0$ and decreases as i increases. Therefore we can make the following definition.

(4.1) Definitions. For $2 \leq \ell \leq d+1$, let i_ℓ be the largest integer i (necessarily ≥ 0) such that the inequality $(\ell + (i-2)d)\,m_p < (\ell + id)m - d$ holds. Further, let $n_\ell = (\ell + i_\ell d)m - d$ and $r_\ell = \ell + (i_\ell - 1)d$.

These definitions are motivated by the following considerations : $S(n_\ell, r_\ell + d) = \emptyset$ (by the definition of r_ℓ) and $S(n_\ell, r_\ell - d) = \emptyset$ (by the inequality in (4.1)).

(4.2) Lemma. *For $2 \le \ell \le d+1$, we have* $i_\ell = \text{Ceiling}\left[\frac{2m-1-\ell p}{pd}\right] + 1$.

Proof. The inequality in (4.1) $\iff i < \frac{2m-1}{pd} + 2 - \frac{\ell}{d} \iff i < \frac{2m-1-\ell p}{pd} + 2$. Since $i < \alpha \iff i \le \text{Ceiling}[\alpha] - 1$ (for i an integer and α real), the assertion follows. ∎

(4.3) Remarks. For $2 \le \ell \le d+1$, let i_ℓ and n_ℓ be as in (4.1).

(i) i_ℓ is a non-increasing function of ℓ and takes at most two values which are consecutive integers.

(ii) If $i_\ell = i_{\ell+1}$ then $n_{\ell+1} = n_\ell + m$.

(iii) Suppose that there is an integer l such that $2 \le l \le d$ and $i_l = i_{l+1} + 1$. Then $n_l = n_{l+1} + (d-1)m$ and $\max\{n_\ell \mid 2 \le \ell \le d+1\} = n_l$. Otherwise, $\max\{n_\ell \mid 2 \le \ell \le d+1\} = n_{d+1}$.

(iv) Let l be any integer. Define $i_l = \text{Ceiling}\left[\frac{2m-1-lp}{pd}\right] + 1$, $n_l = (l + i_l d)m - d$ and $r_l = l + (i_l - 1)d$. Then n_l and r_l (but not i_l) depend only on the congruence class of l modulo d. We chose ℓ with $2 \le \ell \le d+1$ for definiteness in our proofs.

(4.4) Theorem. *Let ℓ be an integer $2 \le \ell \le d+1$, let i_ℓ and n_ℓ be as in* (4.1). *Then* $\dim_k(\Omega^1_{A/k})_{n_\ell} = 2$ *and* $\dim_k(\Omega^1_{A/k})_n = 1$ *for all $n > n_\ell$ with $n \equiv m\ell \pmod d$. Moreover, $n_0 = \max\{n_\ell \mid 2 \le \ell \le d+1\} + 1$ is the index of regularity for $\Omega^1_{A/k}$.*

Proof. Since $r_\ell \ge 3$ by (4.5c) below, the assertions follow from (4.6) and (3.4). ∎

(4.5) Lemma. *Let ℓ be an integer with $2 \le \ell \le d+1$ and let i_ℓ and r_ℓ be as in* (4.1). *Then for an integer $i \ge i_\ell$, we have :*

(a) $m - 1 \le (\ell + id - 1)p$.

(b) $2m - 1 \le (\ell + (i-1)d)p$.

(c) *$i_\ell \ge 1$ and $r_\ell \ge \ell$. Moreover, $i_2 \ge 2$ and $r_2 \ge 2 + d$.*

(d) *If either $(m,p) \ne (2,1)$ or $i > i_\ell$ then $m < (\ell + (i-1)d - 1)p$.*

(e) *If $(m,p) = (2,1)$ then $S((\ell + id)m, \ell + (i-1)d) = S$.*

Proof. (a) follows from (b), since $d \ge 1$. To prove (b) we may assume $i = i_\ell$. Then by substituting the value of i_ℓ from (4.2) we get $(i_\ell - 1)pd = \text{Ceiling}[\frac{2m-1-\ell p}{pd}]\, pd \ge 2m - 1 - \ell p$, from which (b) follows.

(c) If $i_\ell = 0$ then from (b) we have $2m - 1 \le (\ell - d)p \le p$ which contradicts the assumption $p \le m-1$. So $i_\ell \ge 1$. If $i_2 = 1$ then from (b) we have $2m - 1 \le 2p$ which again contradicts $p \le m - 1$. Lastly, $r_\ell \ge \ell$ and $r_2 \ge 2 + d$ by the definition of r_ℓ.

(d) Note that $p \le m-1$ by assumption. If $p < m-1$ then (b) $\Rightarrow$ (d) and if $p = m-1$, (b) $\Rightarrow m \le (\ell + (i-1)d - 1)p$. Further, if $p = m-1$ and $(m,p) \ne (2,1)$ then p does not divide $2m-1-\ell p$ (since $p>1$), and so $\frac{2m-1-\ell p}{pd}$ is not an integer. Therefore $m < (\ell+(i_\ell-1)d-1)\,p \le (\ell+(i-1)d-1)\,p$.

(e) Since $(m,p)=(2,1)$, by (4.2) we have $i_\ell=2$ if $\ell=2$ and $i_\ell=1$ if $\ell\ge 3$. Let $r=\ell+id$ and $n=(\ell+id)m$. Then $(r-d-1)p=r-d-1\ge \ell+(i_\ell-1)d-1\ge 2=m$. Since $n=rm=(r-d)m+md$, it follows from (2.1f) that $S(n,r-d)=S$. ■

(4.6) Lemma. *Let ℓ be an integer $2\le\ell\le d+1$ and let i_ℓ, r_ℓ, n_ℓ be as in* (4.1). *Then*

(a) *$P(n_\ell)=\{r_\ell\}$ and $S(n_\ell,r_\ell)=S$. In particular, $s(n_\ell,r_\ell)>1$.*

(b) *Let n be an integer with $n\equiv m\ell \pmod d$ and $n>n_\ell$. Then there exists an integer r such that either $|S(n,r-d)\cap S(n,r)|>1$ or one of $S(n,r-d)$, $S(n,r)$ has cardinality 1 and the other equals S.*

Proof. (a) Since $n_\ell=r_\ell m+(m-1)d$ and $p\le m-1\le (r_\ell-1)p=(\ell+(i_\ell-1)d-1)p$ by (4.5b), we have $S(n_\ell,r_\ell)=S$ by (2.1f). From the definition of i_ℓ it now follows that $P(n_\ell)=\{r_\ell\}$.

(b) Since $n>n_\ell$ and $n\equiv m\ell \pmod d$, we have that $n=(\ell+id)m+jd$ with $i\ge i_\ell$ and $0\le j\le m-1$. For fixed $i\ge i_\ell$, put $r=\ell+id$. Then $n=rm+jd$ and, since $0\le j\le m-1\le(\ell+id)p=rp$ by (4.5a), $S(n,r)\neq\emptyset$ by (2.1f). Furthermore, $n=rm+jd=(r-d)m+(j+m)d$ and $0\le j+m\le 2m-1\le(\ell+(i-1)d)p=(r-d)p$ by (4.5b), whence $S(n,r-d)\neq\emptyset$ by (2.1f). We shall prove that this r is the desired one by considering the two cases $0\le j\le p-1$ and $p\le j\le m-1$ separately.

Case 1 : $0\le j\le p-1$. In this case we have $S(n,r)=[m,m_j,d]$ by (2.1f). If $S(n,r-d)=S$ then we are done. Therefore assume $S(n,r-d)\neq S$. Then $(m,p)\neq(2,1)$ by (4.5e). Since $n=(r-d)m+(j+m)d$, by (2.1f) we have $(r-d-1)p+1\le j+m\le(r-d)p$ and $S(n,r-d)=[m_k,m_p,d]$ with $k=j+m-(r-d-1)p$. By (4.5d) $j-k=(r-d-1)p-m=(\ell+(i-1)d-1)p-m>0$, so $|S(n,r-d)\cap S(n,r)|>1$.

Case 2 : $p\le j\le m-1$. In this case $S(n,r)=S$ by (4.5a) and (2.1f), so we are done. ■

(4.7) Examples. The index of regularity n_0 can be any congruence class modulo d. This and remarks (4.3) are illustrated by the examples in the following tables.

(m,p,d)	ℓ	i_ℓ	r_ℓ	n_ℓ	n_0
$(7,5,3)$	2	2	5	53	54
	3	1	3	39	
	4	1	4	46	
$(7,4,3)$	2	2	5	53	
	3	2	6	60	61
	4	1	4	46	
$(7,3,3)$	2	2	5	53	
	3	2	6	60	
	4	2	7	67	68

(m,p,d)	ℓ	i_ℓ	r_ℓ	n_ℓ	n_0
$(7,5,2)$	2	2	4	40	41
	3	1	3	33	
$(7,4,2)$	2	2	4	40	
	3	2	5	47	48

The entire Hilbert function of two of the above cases is given in the table below. The box indicates the index of regularity.

(m,p,d)	Hilbert function of $\Omega^1_{A/k}$		
$(7,5,3)$	n	0-13	14-27
	$H(n)$	0,0,0,0,0,0,0,1,0,0,1,0,0,1,	1,0,1,2,0,1,2,1,1,3,2,0,3,2,
	n	28-41	42, ... ,53,$\boxed{54}$,55
	$H(n)$	1,4,2,2,3,2,2,3,2,2,3,2,2,3,	1,2,2,1,2,2,1,1,2,1,1,2,$\boxed{1}$,1,

(m,p,d)	Hilbert function of $\Omega^1_{A/k}$		
$(7,5,2)$	n	0-13	14-27
	$H(n)$	0,0,0,0,0,0,0,1,0,1,0,1,0,1,	1,1,2,1,2,0,3,1,3,2,4,2,3,2,
	n	28, ... ,40, $\boxed{41}$	42-55
	$H(n)$	3,2,3,2,3,2,2,1,2,1,2,1,2,$\boxed{1}$,	1,1,1,1,1,1,1,1,1,1,1,1,1,1,

§5 Symmetry and comparison of the case $d = 1$ with $d > 1$.

As usual let $A = k[t^m, t^{m+d}, \ldots, t^{m+pd}]$, and define $A' = k[t^m, t^{m+d'}, \ldots t^{m+pd'}]$ for $1 \leq d' < d$. The notation of §2 and §3 will be applied to A' by applying $'$ to the corresponding notation for A. For example $S' = [m, m+pd', d']$.

In this situation we investigate a curious relationship between the Hilbert functions of $\Omega^1_{A/k}/dA$ and $\Omega^1_{A'/k}/dA'$ when p is not "too small" compared to m and show that, if $p = m-1$, then the Hilbert function of $\Omega^1_{A/k}/dA$ is symmetric, a generalization of [6 ; (8.5)]. We were initially interested in the case $d' = 1$ but essentially the same proof works for $d' \geq 1$.

Let $h(n) = \dim_k(\Omega^1_{A/k}/dA)_n$ and $h'(n) = \dim_k(\Omega^1_{A'/k}/dA')_n$. Given two arithmetic progressions $a,\ a+d,\ \ldots,\ a+sd$ and $a',\ a'+d',\ \ldots,\ a+sd'$, we will say that h and h' "coincide" on $[a, a+sd, d]$ and $[a', a'+sd', d']$ if $h(a+id) = h'(a'+id')$ for $i = 1, 2, \ldots, s$.

(5.1) Theorem. *Let* $I = [2m+d, 2m+(2m-1)d, d]$, $I' = [2m+d', 2m+(2m-1)d', d']$, $J = [2m+d, 2m+(2m-1)d]$ *and* $J' = [2m+d', 2m+(2m-1)d']$.

(a) *If* $m/(2+d') \leq p \leq m-1$ *then* h *and* h' *coincide on the intervals* I *and* I' *respectively.*

(b) *If* $(2m-1)/3 \leq p \leq m-1$ *then* $h(n) = 0$ *if* $n \notin J$ *and* $h'(n') = 0$ *if* $n' \notin J'$.

(c) *If* $m = p+1$ *then* h *is symmetric on the interval* J *and* 0 *outside* J.

Proof. (a) Define $\sigma : I' \to I$ by $2m + jd' \mapsto 2m + jd$ for $1 \le j \le 2m - 1$. Then we need only show that $h(\sigma(n')) = h'(n')$ for $n' \in I'$. If $n \in I$ then $P(n) = \{r | S(n, r) \neq \emptyset\} \subseteq \{2, 2 + d\}$ (cf. 2.1g), and if $n' \in I'$ then $P'(n') \subseteq \{2, 2 + d'\}$. In view of (2.1b) and (3.4) it suffices to show that

(i) if $n' \in I'$ then $\tau(S'(n', 2)) = S(\sigma(n'), 2)$ where τ is the bijection $\tau : S' \to S$ defined by $m + jd' \mapsto m + jd$, $0 \le j \le p$, and

(ii) $\sigma(\{n' \in I' \mid s'(n', 2 + d') > 1\}) = \{n \in I \mid s(n, 2 + d) > 1\}$.

(i) follows from the equality $\sigma(a + b) = \tau(a) + \tau(b)$ for all $a, b \in S'$. For (ii) note that $\{n \mid s(n, 2+d') > 1\} = [(2+d')m+d', (2+d')(m+pd')-d', d']$ and $\{n \mid s(n, 2+d) > 1\} = [(2+d)m+d, (2+d)(m+pd)-d, d]$ by (2.1f). Since $\sigma((2+d')m+d') = (2+d)m+d$ the proof will be complete if $(2+d')(m+pd')-d' \ge 2m+(2m-1)d'$ and $(2+d)(m+pd)-d \ge 2m+(2m-1)d$. These inequalities are equivalent to $m/(2+d') \le p$ and $m/(2+d) \le p$ respectively. The second follows from the first, which is our hypothesis.

(b) Note that J and J' are the entire intervals containing the arithmetic progressions I and I' respectively. It is enough to prove the result for h (since the result for h' is obtained by putting $d = d'$). For $n < 2m + d =$ the left endpoint of J, $s(n, r) \le 1$ so $h(n) = 0$ by (3.4). If $\ell \ge 3$ then $2m - 1 - \ell p \le 2m - 1 - 3p \le 0$ (by hypothesis). Therefore, by (4.2) $i_\ell \le 1$, and by (4.5c), $i_\ell \ge 1$, so $i_\ell = 1$ for $\ell \ge 3$, whence $r_\ell = \ell$ and $n_\ell = (\ell + d)m - d$. Furthermore $i_2 = 2$ by (4.5c) and (4.3i), so $r_2 = 2 + d$, $n_2 = (2 + 2d)m - d$. Thus $\max\{n_\ell \mid 2 \le \ell \le d + 1\} = n_2$ which is the right end point of J. The assertion follows from (4.4).

(c) The midpoint of the interval J is $2m + md$. Let $\rho : J \to J$ be the reflection $n \mapsto 2(2m + md) - n$. We have to show that $h(\rho(n)) = h(n)$ for $n \in J$ which follows from the observations below :

(i) Let $I_2 = I$ and for $3 \le \ell \le d+1$, let $I_\ell = [\ell m + d, \ell m + (m-1)d, d]$. Then $\cup_{\ell=2}^{d+1} I_\ell$ is a disjoint union and $h = 0$ outside $\cup_{\ell=2}^{d+1} I_\ell$.

(ii) $\rho(I_2) = I_2$ and $h(\rho(n)) = h(n)$ for $n \in I_2$.

(iii) For $\ell \ge 3$, $\rho(I_\ell) = I_{d+4-\ell}$ and $h(n) = 1$ for all $n \in I_\ell$.

Proof of (i) : The disjointness follows from the fact that $\gcd(m, d) = 1$. From the proof of (b) we have $r_2 = 2 + d$, $n_2 = (2 + 2d)m - d$, and for $\ell \ge 3$ $r_\ell = \ell$ and $n_\ell = \ell m + (m - 1)d$. Therefore, since n_ℓ is the right hand end point of I_ℓ for $2 \le \ell \le d + 1$, we have by (4.4) $h(n) = 0$ if $n \equiv \ell m \pmod d$ and $n > n_\ell$. If $n \equiv \ell m \pmod d$ and $n < \ell m + d$, then $S(n, \ell)$ is either $\{m\}$ or $\emptyset$, and so $h(n) = 0$ by (3.4).

Proof of (ii) : In view of (a), we may assume that $d = 1$. This case was proved in [6 ; (8.5)] (see (5.2) for further discussion).

Proof of (iii) : From $\rho(\ell m + d) = (d + 4 - \ell)m + (m - 1)d$ and $\rho(\ell m + (m - 1)d) = (d + 4 - \ell)m + d$ the first part follows. If $n \in I_\ell$ then $n < (\ell + d)m$ so $P(n) = \{\ell\}$ by (2.1g), $s(n, \ell) > 1$ by (2.1f), and $h(n) = 1$ for all $n \in I_\ell$, $3 \le \ell \le d + 1$ by (3.4). ■

(5.2) Examples. We illustrate (5.1) with several examples (each with $d' = 1$).

(1) Let $(m, p) = (7, 5)$. Then $h'(n)$ is displayed in the following table.

ℓ	n	$h'(n)$ $\downarrow$
2	[15,27]	1, 1, 2, 2, 3, 2, 2, 2, 2, 1, 1, 1, 1,

If $d = 3$ then $h(n)$ is displayed in the rows of the following table according as n varies in the congruence class $\equiv \ell m \pmod{d}$, $2 \leq \ell \leq 4 = d + 1$.

ℓ	n	$h(n)$ $\downarrow$
2	[17,53,3]	1,-,-,1,-,-,2,-,-,2,-,-,3,-,-,2,-,-,2,-,-,2,-,-,2,-,-,1,-,-,1,-,-,1,-,-,1,
3	[18,51,3]	-,0,-,-,0,-,-,1,-,-,1,-,-,1,-,-,1,-,-,1,-,-,1,-,-,0,-,-,0,-,-,0,-,-,0,-,-,
4	[19,52,3]	-,-,0,-,-,0,-,-,0,-,-,0,-,-,1,-,-,1,-,-,1,-,-,1,-,-,1,-,-,1,-,-,0,-,-,0,-,
	[17,53]	1,0,0,1,0,0,2,1,0,2,1,0,3,1,1,2,1,1,2,1,1,2,1,1,2,0,1,1,0,1,1,0,0,1,0,0,1,

Note that $h'(n)$ from the first table is same as the $\ell = 2$ row of the second table, illustrating (5.1a). In this example h' is not symmetric (about the midpoint 21 of $I' = [15, 27]$ which is indicated by the down-arrow $\downarrow$).

(2) Let $(m, p) = (7, 6)$. Then as in the example (1) $h'(n)$ and $h(n)$ for $d = 3$ are displayed in the following two tables :

ℓ	n	$h'(n)$ $\downarrow$
2	[15,27]	1, 1, 2, 2, 3, 3, 3, 3, 3, 2, 2, 1, 1,

ℓ	n	$h(n)$ $\downarrow$
2	[17,53,3]	1,-,-,1,-,-,2,-,-,2,-,-,3,-,-,3,-,-,3,-,-,3,-,-,3,-,-,2,-,-,2,-,-,1,-,-,1,
3	[18,51,3]	-,0,-,-,0,-,-,1,-,-,1,-,-,1,-,-,1,-,-,1,-,-,1,-,-,0,-,-,0,-,-,0,-,-,0,-,-,
4	[19,52,3]	-,-,0,-,-,0,-,-,0,-,-,0,-,-,1,-,-,1,-,-,1,-,-,1,-,-,1,-,-,1,-,-,0,-,-,0,-,
	[17,53]	1,0,0,1,0,0,2,1,0,2,1,0,3,1,1,3,1,1,3,1,1,3,1,1,3,0,1,2,0,1,2,0,0,1,0,0,1,

Again $h'(n)$ from the first table is same as the $\ell = 2$ row of the second table, illustrating (5.1a). This time h' is symmetric (about the midpoint 21 of $I' = [15, 27]$ which is indicated by the down-arrow $\downarrow$), illustrating (5.1c).

In the above two examples the rows corresponding to $\ell = 3$ are equal and so are the rows $\ell = 4$. Under the reflection about the midpoint 35 of $J = [17, 53]$ the rows $\ell = 3$ and $\ell = 4$ are interchanged, illustrating (5.1c) part (iii) in the proof.

(3) In the above two examples the row $\ell = 2$ contains contributions to $h(n)$ from $V_{n,r}/W_{n,r}$, $r = 2, 2 + d$. To illustrate this, in view of (5.1a), it suffices to consider $d = 1$. For $(m, p, d) = (7, 5, 1)$ and $(7, 6, 1)$, this is displayed in the following tables respectively.

r	n	$\dim_k(V_{n,r}/W_{n,r})$
2	[15,27]	1, 1, 2, 2, 3, 2, 2, 1, 1, 0, 0, 0, 0
3	[15,27]	0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1
$h'(n)$	[15,27]	1, 1, 2, 2, 3, 2, 2, 2, 2, 1, 1, 1, 1

r	n	$\dim_k(V_{n,r}/W_{n,r})$												
2	[15,27]	1,	1,	2,	2,	3,	3,	3,	2,	2,	1,	1,	0,	0
3	[15,27]	0,	0,	0,	0,	0,	0,	0,	1,	1,	1,	1,	1,	1
$h'(n)$	[15,27]	1,	1,	2,	2,	3,	3,	3,	3,	3,	2,	2,	1,	1

In each case the contribution for $r = 2$ and $r = 3$ are individually symmetric, but the sum is symmetric only in the case $p = 6$. More generally, for any m the sum is symmetric if and only if $p = m - 1$. This symmetry seems to be an accident.

(5.3) Remark. Even though the Hilbert function h of $\Omega^1_{A/k}/dA$ is symmetric, the Hilbert function H of $\Omega^1_{A/k}$ need not be symmetric. This is because the equality $H(n) = h(n)+1$ of (3.4a) holds only when $A_n \neq 0$. An example is $(m, p, d) = (7, 6, 3)$.

§6 $\Omega^q_{A/k}$ for $q \geq 3$.

The natural homomorphism $\pi : A \to A/\mathfrak{m}^2$ of k-algebras induces a homomorphism of A-modules $\Omega^q_{A/k} \to \Omega^q_{(A/\mathfrak{m}^2)/k}$ for all $q \geq 0$. In this section we show that if $q \geq 3$ then this map is an isomorphism. More generally we have

(6.1) Theorem. *Let K be a commutative ring in which 2 is invertible and let $R = K[X_0, \ldots, X_p]$ be the polynomial ring. Let $\mathfrak{a}$ be an ideal in R with $\mathfrak{a} \subset (X_0, \ldots, X_p)^2$ and $X_\alpha X_\beta - X_\gamma X_\delta \in \mathfrak{a}$ whenever $\alpha + \beta = \gamma + \delta$, $0 \leq \alpha, \beta, \gamma, \delta \leq p$. Let $C = R/\mathfrak{a} = K[x_0, \ldots, x_p]$ and let $\mathfrak{m}$ be the maximal ideal of C generated by $x_0, \ldots, x_p$. Then for $q \geq 0$ there is an isomorphism of K-modules $\Omega^q_{(C/\mathfrak{m}^2)/K} \xrightarrow{\cong} \Lambda^q(\mathfrak{m}/\mathfrak{m}^2) \oplus \Lambda^{q+1}(\mathfrak{m}/\mathfrak{m}^2)$ and for $q \geq 3$, the K-algebra homomorphism $\pi : C \longrightarrow C/\mathfrak{m}^2$ induces an isomorphism $\pi^*_q : \Omega^q_{C/K} \longrightarrow \Omega^q_{(C/\mathfrak{m}^2)/K}$ of C-modules.*

Proof. Note that $C/\mathfrak{m}^2$ is isomorphic to $K \oplus \mathfrak{m}/\mathfrak{m}^2$ as a K-algebra, where the multiplication in $K \oplus \mathfrak{m}/\mathfrak{m}^2$ is given by $(a, v) \cdot (b, w) = (ab, aw + bv)$, $a, b \in K$ and $v, w \in \mathfrak{m}/\mathfrak{m}^2$. Let $\mathcal{P}_q([0, p])$ be the set of subsets of $\{0, 1, \ldots, p\}$ of cardinality q and, for $I \in \mathcal{P}_q([0, p])$, let $\min(I)$ denote the smallest element of I. For $I \in \mathcal{P}_q([0, p])$, we write $x_I = x_{i_1} \wedge \cdots \wedge x_{i_q}$ ($\in \Lambda^q(\mathfrak{m}/\mathfrak{m}^2)$) and $dx_I = dx_{i_1} \wedge \cdots \wedge dx_{i_q}$ ($\in \Omega^q_{(C/\mathfrak{m}^2)/K}$), where $i_1 < i_2 < \cdots < i_q$ are the elements of I. If K is a field of characteristic $\neq 2$, then it was proved in [7 ; Theorem 1] that for all $q \geq 0$ there is an isomorphism $\theta : \Omega^q_{(C/\mathfrak{m}^2)/K} \to \Lambda^q(\mathfrak{m}/\mathfrak{m}^2) \oplus \Lambda^{q+1}(\mathfrak{m}/\mathfrak{m}^2)$ of K-modules such that $\theta(dx_I) = x_I$ and $\theta(x_{i_0} dx_I) = x_{i_0} \wedge x_I$. The same proof works in the case of any commutative ring K in which 2 is invertible. Since $\Omega^q_{C/K}$ is generated by $\{dx_I \mid I \in \mathcal{P}_q([0, p])\}$ as a C-module, it follows from (6.2) below that for $q \geq 3$ $\{dx_I \mid I \in \mathcal{P}_q([0, p])\} \cup \{x_{i_0} dx_I \mid I \in \mathcal{P}([0, p])$ and $0 \leq i_0 < \min(I)\}$ generates $\Omega^q_{C/K}$ as a K-module. Under the map $\theta \circ \pi^*_q$ this generating set is mapped onto the K-basis $\{x_I \mid I \in \mathcal{P}_q([0, p])\} \cup \{x_{i_0} x_I \mid I \in \mathcal{P}_q([0, p])$ and $0 \leq i_0 < \min(I)\}$ of

$\Lambda^q(\mathfrak{m}/\mathfrak{m}^2) \oplus \Lambda^{q+1}(\mathfrak{m}/\mathfrak{m}^2)$. Therefore the map $\theta \circ \pi_q^*$ is an isomorphism and hence so also is π_q^*. ∎

(6.2) Lemma. *With the same notation and assumptions as in* (6.1), *for integers* $0 \leq i, j, \alpha, \beta, \gamma, \delta \leq p$ *we have in* $\Omega^3_{C/K}$*:*

(a) *If* $\alpha < \beta < \gamma$ *then* $x_\alpha dx_\alpha \wedge dx_\beta \wedge dx_\gamma = x_\beta dx_\alpha \wedge dx_\beta \wedge dx_\gamma = x_\gamma dx_\alpha \wedge dx_\beta \wedge dx_\gamma = 0$.

(b) $x_\alpha dx_\beta \wedge dx_\gamma \wedge dx_\delta = -x_\beta dx_\alpha \wedge dx_\gamma \wedge dx_\delta = x_\gamma dx_\alpha \wedge dx_\beta \wedge dx_\delta = -x_\delta dx_\alpha \wedge dx_\beta \wedge dx_\gamma$.

(c) $x_i x_j dx_\alpha \wedge dx_\beta \wedge dx_\gamma = 0$.

Proof. (a) The assertion follows by using induction on $\gamma - \alpha$ and the same arguments as in [7 ; (1.2)].

(b) In view of (a), we may assume that α, β, γ, δ are distinct and $\alpha < \beta < \gamma < \delta$. The assertion follows by using the same arguments as in [7 ; (1.3)].

(c) In view of (a) and (b) we may assume that $i \leq j < \alpha < \beta < \gamma$. Then by (b) we have $x_i x_j dx_\alpha \wedge dx_\beta \wedge dx_\gamma = -x_i x_\alpha dx_j \wedge dx_\beta \wedge dx_\gamma = -x_\alpha x_i dx_j \wedge dx_\beta \wedge dx_\gamma = x_\alpha x_j dx_i \wedge dx_\beta \wedge dx_\gamma$ and $x_i x_j dx_\alpha \wedge dx_\beta \wedge dx_\gamma = x_j x_i dx_\alpha \wedge dx_\beta \wedge dx_\gamma = -x_j x_\alpha dx_i \wedge dx_\beta \wedge dx_\gamma$. Therefore $2 x_i x_j dx_\alpha \wedge dx_\beta \wedge dx_\gamma = 0$ and so $x_i x_j dx_\alpha \wedge dx_\beta \wedge dx_\gamma = 0$, since 2 is invertible in K. ∎

(6.3) Corollary. *Let* m, p, d *be positive integers with* $1 \leq p \leq m-1$, $\gcd(m, d) = 1$ *and let* $m_i = m + id$, $0 \leq i \leq p$. *Let* k *be a field of characteristic* $\neq 2$, $A = k[t^{m_0}, \ldots, t^{m_p}]$, *and let* $\mathfrak{m}$ *be the maximal ideal of* A *generated by* $t^{m_0}, \ldots, t^{m_p}$. *Then, for* $q \geq 0$ *there is an isomorphism of* k*-vector spaces* $\Omega^q_{(A/\mathfrak{m}^2)/k} \xrightarrow{\cong} \Lambda^q(\mathfrak{m}/\mathfrak{m}^2) \oplus \Lambda^{q+1}(\mathfrak{m}/\mathfrak{m}^2)$, *and, for* $q \geq 3$, *the* k*-algebra homomorphism* $\pi : A \longrightarrow A/\mathfrak{m}^2$ *induces an isomorphism* $\Omega^q_{A/k} \longrightarrow \Omega^q_{(A/\mathfrak{m}^2)/k}$ *of* A*-modules.*

Proof. We use the notation of § 1. Since $\mathfrak{p} \subset (X_0, \ldots, X_p)^2$ and $X_\alpha X_\beta - X_\gamma X_\delta \in \mathfrak{p}$ whenever $\alpha + \beta = \gamma + \delta$, $0 \leq \alpha, \beta, \gamma, \delta \leq p$, the corollary follows from (6.1). ∎

(6.4) Remark. One can apply (6.1) in situations other than monomial curves, for example, in the case of the coordinate axes, i.e., $C = K[X_0, \ldots, X_p]/\mathfrak{a}$ where $\mathfrak{a}$ is the ideal generated by $\{X_i X_j \mid 0 \leq i < j \leq p\}$.

(6.5) The deRham Complex. Recall that the deRham complex

$$0 \to A \xrightarrow{d} \Omega^1_{A/k} \xrightarrow{d} \Omega^2_{A/k} \xrightarrow{d} \cdots \xrightarrow{d} \Omega^q_{A/k} \xrightarrow{d} \Omega^{q+1}_{A/k} \xrightarrow{d} \cdots$$

of A/k is a complex of graded k-vector spaces (with degree of the differential d equal to 0) and is exact (characteristic of k is 0 is needed here) at each $q \geq 1$ by [6 ; Theorem (1.2)]. Combining this with the isomorphism in (6.3) we get a complex of graded k-vector spaces

$$0 \to A \xrightarrow{d} \Omega^1_{A/k} \xrightarrow{d} \Omega^2_{A/k} \xrightarrow{d} \Lambda^3(\mathfrak{m}/\mathfrak{m}^2) \oplus \Lambda^4(\mathfrak{m}/\mathfrak{m}^2) \xrightarrow{d} \Lambda^4(\mathfrak{m}/\mathfrak{m}^2) \oplus \Lambda^5(\mathfrak{m}/\mathfrak{m}^2) \cdots$$

where d maps $\Lambda^q(\mathfrak{m}/\mathfrak{m}^2)$ isomorphically onto $\Lambda^q(\mathfrak{m}/\mathfrak{m}^2)$ for $q \geq 4$. Therefore we have a short exact sequence of graded k-vector spaces

(6.6) $$0 \to \Omega^1_{A/k}/dA \xrightarrow{d} \Omega^2_{A/k} \xrightarrow{d} \Lambda^3(\mathfrak{m}/\mathfrak{m}^2) \longrightarrow 0$$

From the short exact sequence (6.6) we can determine the Hilbert function of $\Omega^2_{A/k}$ if we know that for $\Omega^1_{A/k}/dA$ and $\Lambda^3(\mathfrak{m}/\mathfrak{m}^2)$. The Hilbert function of $\Omega^1_{A/k}/dA$ was determined in (3.4) and the determination of the Hilbert function of $\Lambda^3(\mathfrak{m}/\mathfrak{m}^2)$ is described below.

(6.7) Lemma. *With notation and assumptions as in* (6.3)*, for non-negative integers* q, n *with* $q \leq p+1$, *and* $f = q(m + \frac{(q-1)}{2}\, d)$ *we have*

(a) $\dim_k \left(\Lambda^q(\mathfrak{m}/\mathfrak{m}^2)\right)_n$ *is the coefficient of* $T^{(n-f)/d}$ *in the Gaussian polynomial*

(6.7.1) $$\begin{bmatrix} p+1 \\ q \end{bmatrix}_T = \frac{(T^{p+1}-1)(T^p-1)\cdots(T^{p-q+2}-1)}{(T^q-1)(T^{q-1}-1)\cdots(T-1)}.$$

(b) *The largest weight* n *for which* $\dim_k \left(\Lambda^q(\mathfrak{m}/\mathfrak{m}^2)\right)_n \neq 0$ *is* $\sum_{i=p-q+1}^{p} m_i$ *and the smallest weight is* $\sum_{i=0}^{q-1} m_i$.

(c) *The largest weight* n *for which* $(\Omega^2_{A/k})_n \neq 0$ *is* $\max\{3m+3d(p-1), n_0-1\}$ *where* n_0 *is as in* (4.4).

Proof. (a) The k-vector space $\mathfrak{m}/\mathfrak{m}^2$ is graded with basis elements of weights $m = m_0, m_1, \ldots, m_p$, respectively and $\{x_I \mid I \in \mathcal{P}_q([0,p])\}$ (see the proof of (6.1) for this notation) is a k-basis of $\Lambda^q(\mathfrak{m}/\mathfrak{m}^2)$. Therefore $\dim_k(\Lambda^q\mathfrak{m}/\mathfrak{m}^2)_n$ is the number of partitions of n as the sum of q distinct elements of $\{m_0, \ldots, m_p\}$. As noted in [7], by subtracting m_0 from the first integer, m_1 from the second, $\ldots, m_{q-1}$ from the q^{th}, we see that this is the number of partitions of $(n-f)/d$ as the sum q non-negative integers, each at most $(p+1-q)$, where $f = \sum_{i=0}^{q-1} m_i = q(m + \frac{(q-1)}{2}\, d)$. Now the assertion follows from [1 ; pp33, 35].

(b) The elements $x_{p-q+1} \wedge x_{p-q+2} \wedge \cdots \wedge x_p$ and $x_0 \wedge x_1 \wedge \cdots \wedge x_{q-1} \in \Lambda^q(\mathfrak{m}/\mathfrak{m}^2)$ are of largest and smallest weight respectively.

(c) From (b) $3m + 3d(p-1)$ is the maximum n such that $(\Lambda^3(\mathfrak{m}/\mathfrak{m}^2))_n \neq 0$ and by definition $n_0 - 1$ is the maximum n such that $\dim_k(\Omega^1_{A/k}/dA)_n \neq 0$. Therefore the assertion follows from (6.6). ∎

The examples $(m,p,d) = (7,5,3)$ and $(7,4,3)$ show that either of the two numbers in (6.7c) can be the maximum, these pairs are $(57,53)$ and $(48,60)$ respectively.

The Gaussian polynomials have been much studied, with quite a large literature. The following is useful for the discussion of the Hilbert function of $\Omega^q_{A/k}$.

(6.8) Remark. Let p and q be any non-negative integers with $q \leq p$. Then the non-zero coefficients of $\begin{bmatrix} p \\ q \end{bmatrix}_T$ are symmetric and unimodal. The first part is easy and the second part is well known but deep. For the latter see [8][1].

(6.9) Example. For $(m,p,d) = (7,5,3)$, the following table illustrates the use of (6.6) to compute the Hilbert function of $\Omega^2_{A/k}$, where $h(n) = \dim_k(\Omega^1_{A/k}/dA)_n$, $H_2(n) = \dim_k(\Omega^2_{A/k})_n$ and $\lambda_3(n) = \dim_k(\Lambda^3(\mathfrak{m}/\mathfrak{m}^2))_n$. The row of $h(n)$ is from (5.2). The row of $\lambda_3(n)$ is computed using (6.7) as follows :

$$\begin{bmatrix} 6 \\ 3 \end{bmatrix}_T = \frac{(T^6-1)(T^5-1)(T^4-1)}{(T^3-1)(T^2-1)(T-1)} = 1+T+2T^2+3T^3+3T^4+3T^5+3T^6+2T^7+T^8+T^9$$

and the coefficient of T^i in $\begin{bmatrix} 6 \\ 3 \end{bmatrix}_T$ is $\lambda_3(3i+30)$, $0 \leq i \leq 9$. The $H_2(n)$ row is the sum of the other two rows by (6.6).

n	16-58
$h(n)$	0,1,0,0,1,0,0,2,1,0,2,1,0,3,1,1,2,1,1,2,1,1,2,1,1,2,0,1,1,0,1,1,0,0,1,0,0,1,0,0,0,0,0
$H_2(n)$	0,1,0,0,1,0,0,2,1,0,2,1,0,3,2,1,2,2,1,2,3,1,2,4,1,2,3,1,1,3,1,1,3,0,1,2,0,1,1,0,0,1,0
$\lambda_3(n)$	0,0,0,0,0,0,0,0,0,0,0,0,0,1,0,0,1,0,0,2,0,0,3,0,0,3,0,0,3,0,0,3,0,0,2,0,0,1,0,0,1,0

It is clear from (6.7.1) that the Gaussian polynomial is a product of the cyclotomic polynomials Φ_r. However, the question remains as to which cyclotomic polynomials occur. Because $\begin{bmatrix} p \\ q \end{bmatrix}_T = \begin{bmatrix} p \\ p-q \end{bmatrix}_T$, we can assume that $q \leq p/2$.

(6.10) Theorem. *Let Φ_r be the cyclotomic polynomial of primitive r^{th} roots of 1. Let p, q be positive integers with $q \leq p/2$. Then $\begin{bmatrix} p \\ q \end{bmatrix}_T$ is the product (without repetition) of the Φ_r such that r satisfies one of the following two conditions :*

(i) *$r > q$ and r divides one of the integers $p, p-1, \ldots, p-q+1$.*

(ii) *$2 \leq r < q$ and if $p \equiv s'_r \pmod r$, $0 \leq s'_r < r$, $q \equiv s_r \pmod r$, $0 \leq s_r < r$, then $0 \leq s'_r \leq s_r - 1$.*

Proof. For $1 \leq i \leq q$, let $F_i(T) = (T^{p-i+1} - 1)$ and $G_i = (T^i - 1)$. Then $F(T) = F_1 \cdots F_q$ is the numerator of (6.7.1) and $G(T) = G_1 \cdots G_q$ is the denominator of (6.7.1). Note that, since $q \leq p/2$, we have $F_i \neq G_j$ for all $1 \leq i, j \leq q$. Throughout the following proof we use the well-known fact :

(6.10.1) Φ_r is irreducible and divides $X^n - 1$ if and only if r divides n.

Case 1 : $r > q$: In this case Φ_r does not divide $G(T)$ and divides at most one of $F_1, \ldots, F_q$. Now, the assertion follows from (6.10.1).

[1] Thanks to Dom de Caen for telling us about this reference.

Case 2 : $r \le q$ **:** Since $X-1$ divides F_i and G_i for all $1 \le i \le q$, Φ_1 does not divide $\begin{bmatrix} p \\ q \end{bmatrix}_T$. Write $p = a'r + s'_r$ and $q = ar + s$ with $a', a \in \mathbb{Z}^+$, $0 \le s'_r, s_r < r$. Then $\mathrm{Floor}[q/r] = a$ and by (6.10.1) we have

(6.10.2) $$|\{G_i \mid \Phi_r \text{ divides } G_i,\ 1 \le i \le q\}| = |\{jr \mid 1 \le j \le a\}| = a\,.$$

Since $p - q + 1 = (a' - a)r + (s'_r - s_r) + 1 \le (a' - a + 1)r$, we have

$$\{p-i+1 \mid r \text{ divides } p-i+1, 1 \le i \le q\} = \begin{cases} \{(a'-j)r \mid 0 \le j \le a-1\}, & \text{if } s'_r \ge s_r, \\ \{(a'-j)r \mid 0 \le j \le a\}, & \text{if } s'_r < s_r, \end{cases}$$

and so by (6.10.1), we have

(6.10.3) $$|\{F_i \mid \Phi_r \text{ divides } F_i,\ 1 \le i \le q\}| = \begin{cases} a, & \text{if } s'_r \ge s_r\,, \\ a+1, & \text{if } s'_r < s_r\,. \end{cases}$$

From (6.10.2) and (6.10.3) it follows that Φ_r divides $\begin{bmatrix} p \\ q \end{bmatrix}_T$ if and only $0 \le s'_r < s_r$. ■

(6.11) Example. To illustrate (6.10) consider $q = 10$ and $p = 24$. Then we have $\{r \mid r \text{ satisfies (i) of (6.10) }\} = \{11, 12, [15, 24]\}$. For $r \in [2, 9]$ we successively have $(p, q) = (24, 10) \equiv \{(0,0), (0,1), (0,2), (4,0), (0,4), (3,3), (0,2), (6,1)\} \pmod r$. These are the pairs (s'_r, s_r) for $r \in [2, 9]$ and so $\{r \mid r \text{ satisfies (ii) of (6.10) }\} = \{3, 4, 6, 8\}$. Therefore $\begin{bmatrix} 24 \\ 10 \end{bmatrix}_T = \Phi_3\Phi_4\Phi_6\Phi_8\Phi_{11}\Phi_{12}\prod_{i=15}^{24}\Phi_i$ by (6.10).

---

§References

[1] Andrews, G. E. : *The Theory of Partitions,* Addison-Wesley, 1976.

[2] Cortinas, C. , Geller, S. C. and Weibel, C. : *The Artinian Berger Conjecture,* to appear in Math. Zeit.

[3] Kunz, E. : *Kähler Differentials,* Advanced Lectures Mathematics, Vieweg, Braunschweig-Wiesbaden, 1986.

[4] Patil, D. P. : *Generators for the Derivation Modules and the Defining Ideals of Certain Monomial Curves,* Ph.D. Thesis, University of Bombay, 1989.

[5] Patil, D. P. : *Minimal Sets of Generators for the Relation Ideals of Certain Monomial Curves,* Manuscripta Math., **80,** 239-248 (1993).

[6] Roberts, L. G. : *Kähler differentials and HC_1 of certain graded k-algebras,* in : J. F. Jardine and V. P. Snaith, eds., Algebraic K-Theory : Connections with Geometry and Topology, NATO ASI series, Series C, vol. **279**, Kluwer Academic Publishers, Dordrecht 389-424 (1989).

[7] Roberts, L. G. : *Kähler Differentials of Certain Cusps,* Proceedings of the Great Lakes K-Theory Conference, Fields Institute Communications, vol.**16**, 279-284 (1997).

[8] Zielberger, D. : *Kathy O'Hara's Constructive Proof of the Unimodality of the Gaussian Polynomials,* Amer. Math. Monthly, **96**, 590-602 (1989).