INSTITUTUL
DE
MATEMATICA

INSTITUTUL NATIONAL
PENTRU CREATIE
STIINTIFICA SI TEHNICA

ISSN 0250 3638

ALGEBRAIC SINGULARITIES DEFINED BY CICLIC GROUP ACTIONS

by

Serban BARCANESCU

PREPRINT SERIES IN MATHEMATICS
No.23/1985

BUCURESTI

ALGEBRAIC SINGULARITIES DEFINED BY CICLIC GROUP ACTIONS

by

Serban BARCANESCU[*)]

April, 1985

[*)] Department of Mathematics, The National Institute for Scientific and Technical Creation, Bd.Pacii 220, 79622 Bucharest, Romania.

ALGEBRAIC SINGULARITIES DEFINED BY CYCLIC GROUP ACTIONS

by

Şerban Bărcănescu

0. Introduction

The theory of the finite degree, complex linear representations of finite (cyclic) groups is particularly simple, due t the automatic fulfillment of Schur's Lemma and of the Theoren of Maschke. The parallel invariant theory for their symmetric extensions to polynomial rings is, in its general lines, finihed.

However, various problems appear when passing to particula classes of groups and to particular symmetric actions, in the attempt to characterize the algebraic singularities which so appear.

One of the simplest such particular case is considered in thi paper, namely the one of the arbitrary (up to similitude) actions on polynomials of finite cyclic groups.

Our main result (Thm.1, § 5) gives a partial answer in this direction, asserting the "linearity" of certain algebraic sigularities, which appear as invariant rings for cyclic group actions. Although it could be perhaps proven in a quicker wav we choosed, in reaching it, a path revealing the deep connection of the subject to the diophantine linear equations (over the positive integers) and to the classical ennumerative theo in combinatories.

This paper naturally extends [3], where only the simplest action of a cyclic group was considered (but where the "general" abelian case was also partially characterized).

The author expresses his gratitude to N.Manolache, L.Bădescu and D.Popescu for helpful talk.

1. Cyclic group actions on polynomials

Let G be a cyclic group of (finite) order $g>0$, realized as the unique subgroup of this order in $\mathbb{C}^*$ (the multiplicative group of the complex field), i.e. $G=\{\zeta^k / k=0,1,\dots,g-1\}$ with ζ a primitive g-root of 1. Let V be an arbitrary $\mathbb{C}$ - linear representation of G, of finite degree $n>0$. Up to similitude, V is diagonal (since G is abelian) and the homotety of the generator ζ uniquely defines the G-module structure on V.

Therefore, the algebraic extension of this linear representation to $R=\mathrm{Sym}(V)=\mathbb{C}[X_1,\dots,X_n]$, is given by a certain linear form in n variables, with coefficients from $\{0,1,\dots,g-1\}$. Precisely, if ζ acts on the variable X_j $(j=1,2,\dots,n)$ by: $(\zeta,X_j)\longmapsto\zeta^{a_j}X_j$, then ζ acts on every monomial $X^{\xi}=X_1^{\xi_1}X^{\xi_2}\dots\dots X_n^{\xi_n}$ (with $\xi=(\xi_1,\dots,\xi_n)\in\mathbb{Z}_+^n$) by: $(\zeta,X^{\xi})\mapsto\zeta^{L(\xi)}X^{\xi}$, with

$L(\xi)=a_1\xi_1+\dots+a_n\xi_n$.

We shall consider only non-degenerate actions, i.e. we impose from the very beginning the reasonable restriction: $a_j\neq 0$, $j=1,2,\dots,n$. This means we don't allow absolute invariants of G on linear forms, avoiding thus an unnecessary digression on Segre products (suited to actions of finite "general" abelian groups).

More than that, if $d=(a_1,\dots,a_n)$ is the greatest common divisor of the coefficients of L, then $L'=\sum_{j=1}^{n}(a_j/d)Y_j$ is the order g/gcd(d,g). However, since a Veronese selection (cf.§3) into the ring of invariants of G′ on R, re-establishes the ring of invariants of G on R, we do not loose generality by supposing that $a_1,\dots,a_n$ are coprime in ansamble.

With these cautions already taken, we consider the corresponding G-module structure on R.

Let $G^{*}=\{\chi_k/k=0,1,\dots,g-1\}$ be the dual of G, indexed by: $\chi_k(\zeta)=\zeta^k$, k=0,1,...,g-1. The isotypical component associated the irreducible character χ_k, is (in our special circumstance the module $R^{(k)}$ of all semi-invariants of weight χ_k, for k=0,1,...,g-1. In particular, $R^{(0)}$ is the ring of absolute invariants (of G on R) and every $R^{(k)}$ is an $R^{(0)}$-module, such that: $R=\bigoplus_{k=0}^{g-1}R^{(k)}$ this $R^{(0)}$-module decomposition of R being consistent with the total degree gradations. More, $R^{(k)}\neq(0)$ for k=0,1.., g-1, because G is finite. Thus, the G-module structure on R (given by the above action) coincides with the $R^{(0)}$-module structure of R.

Certain properties of this structure are known from the genera theory of invariants for finite groups. For instance, $R^{(0)}$ is a finitely generated $\mathbb{C}$-algebra and every $R^{(k)}$ is a finitely generated $R^{(0)}$-module (the Theorem of Hilbert -Noether), so the ring extension $R^{(0)}\hookrightarrow R$ is finite and $\dim(R^{(0)})=n$.

The ring $R^{(0)}$ is an algebraic singularity as soon as ζ doesn' act as a pseudo-reflection on V (Chevalley-Shephard-Todd).

This algebraic singularity is a always Cohen-Macaulay (a fact proved by Hochester for general toric actions) and every $R^{(k)}$ is a Cohen-Macaulay $R^{(0)}$-module, for k=1,...,g-1. The canonica module of the Cohen-Macaulay singularity $R^{(0)}$, is the isotypical component $R^{(k)}$, associated to the character $\det^{-1}$ of G (as a subgroup of $GL_{\mathbb{C}}(n)$), i.e. it is the discriminant of the action of G on R (Eisenbud). In particular, the singularity $R^{(0)}$ is Gorenstein iff ζ is identified to an element of $SL_{\mathbb{C}}(n)$, by its initial linear action on V (K.Watanabe).

Remark

The Theorem of Burnside-Chevalley-Serre shows that the knewledge of $R^{(0)}$ allows the recovering of the whole theory of the (finite degree) linear representations of G, because a certain non-zero multiple of the regular representation $\mathbb{C}[G]$ may be realized as a factorving of $R^{(0)}$.

Specific to our groups, is the following property of the G-module structure of R, obtained by mere translation of general definitions:

1. *Proposition*

In the above setting, let $M^{(k)}=\{\xi\in\mathbb{Z}_+^n / L(\xi)\equiv k \pmod{g}\}$, *for* k=0,1,...,g-1.

(i) $M^{(0)}$ *is a finitely generated submonoid of the free abelian monoid* $\mathbb{Z}_+^n$ *and every* $M^{(k)}$ *is a monoidal* $M^{(0)}$ - *submodule of* $\mathbb{Z}_+^n$ (i.e. $M^{(k)}+M^{(0)}\subseteq M^{(k)}$), *such that:*

$$\mathbb{Z}_+^n = \dot{\bigcup}_{k=0}^{g-1} M^{(k)} \text{ and } M^{(k)}\cap M^{(k')}=\phi, \text{ for } k\neq k'$$

(ii) $R^{(0)}$ *is the monoid* $\mathbb{C}$*-algebra of* $M^{(0)}$ *and every* $R^{(k)}$ *is is spanned over* $\mathbb{C}$ *by all monomials with exponents in* $M^{(k)}$, k=1,2,...,g-1. *In particular, the* $R^{(0)}$*-module structure on* $R^{(k)}$ *is given by the* $M^{(0)}$*-module structure on* $M^{(k)}$, k=1,2,..,g-1.

This property puts into light certain combinatorial structures, which we have to consider in order to characterize the singularity $R^{(0)}$. The next two sections are devoted to this. We turn back to invariants in §5.

2. Gradations on free abelian monoids

Let $n>2$ be an integer. We consider the free abelian group $\mathbb{Z}^n$ (the direct product of n copies of the additive grou $\mathbb{Z}$) and fix on it a partial order compatible with the group law. This comes to selecting a basis $E=\{e_1,\dots,e_n\}$ of $\mathbb{Z}^n$ (called "canonical" in the sequel) and order $\mathbb{Z}^n$ as the product-lattice of the linearly ordered abelian groups $\{\mathbb{Z}e_j/j=1,2,\dots\dots,n\}$, each having $\mathbb{Z}_+e_j=\{k.e_j/k=0,1,2,\dots\}$ as the set of positive elements ($j=1,2,\dots,r$).

The free abelian monoid $\mathbb{Z}_+^n=\bigoplus_{j=1}^{n}\mathbb{Z}_+e_j$, ordered by the restriction of the given order on $\mathbb{Z}^n$ (denoted by $\leq_E$, or simply by $\leq$ if no confusion may arise), becomes the poset of all positive elements in $\mathbb{Z}^n$ and the monoid embedding $\mathbb{Z}_+^n\subseteq\mathbb{Z}^n$ (given by the canonical structure of $\mathbb{Z}^n$ as the universal abelian group of the cancellative monoid $\mathbb{Z}_+^n$) enjoys the property: for $\xi,\xi'\in\mathbb{Z}_+^n$ and $\xi+\xi'=0$ in $\mathbb{Z}^n$, it follows $\xi=\xi'=0$ (cf. [4]).

By the universality property of $\mathbb{Z}^n$, every monoid homomorphism $f:\mathbb{Z}_+^n\longrightarrow\mathbb{Z}_+$ uniquely extends to a group homomorphism $\bar{f}:\mathbb{Z}^n\longrightarrow\mathbb{Z}$ (i.e. the dual of $\mathbb{Z}_+^n$ (as a monoid) is canonically embedded by means of E into the dual of $\mathbb{Z}^n$ (as a group)). The monoid homomorphism f is uniquely defined by its values on E: putting $a_j=f(e_j)$, $j=1,2,\dots,n$, the effect of f on any $\xi\in\mathbb{Z}_+^n$ is given by $f(\xi)=L_f(\xi)$, where L_f is the linear form in n variables:

$$L_f = a_1Y_1+\dots+a_nY_n.$$

We consider non-degenerate forms only, i.e. we suppose that $a_j\neq 0$ for $j=1,2,\dots,n$.

In this case, all fibers of f are non-empty, finite subset of $\mathbb{Z}_+^n$, giving a gradation compatible with the monoid structure on $\mathbb{Z}_+^n$.

Conversely, any fixed non-degenerate linear form $L=a_1Y_1+\dots$

fibers $f_L:\mathbb{Z}_+^n \longrightarrow \mathbb{Z}_+$, reffered to as "the L-gradation" on $\mathbb{Z}_+^n$. Its unique extension to $\mathbb{Z}^n$ yields a group homomorphism $\bar{f}_L:\mathbb{Z}^n \to \mathbb{Z}$, such that, denoting by $G_o(L)$ its kernel, the exact sequence:

$$0 \longrightarrow G_o(L) \longrightarrow \mathbb{Z}^n \xrightarrow{\bar{f}_L} \mathrm{Im}(\bar{f}_L) \longrightarrow 0$$

splits, $\mathrm{Im}(\bar{f}_L)$ being non-zero and free. Therefore $G_o(L)$ is free and $\mathrm{rk}G_o(L)=n-1$. Since $\mathrm{Im}(\bar{f}_L)$ is a subgroup of $\mathbb{Z}$, it is of the form $\mathbb{Z}.d$, with d equal to the greatest common divisor of the coefficients of L.

We may therefore "normalize" L, by working with $(1/d)L$, whose coefficients have the gcd equal to 1.

From now on, we fix a normalized, non-degenerate linear form in $n\geq 2$ variable over $\mathbb{Z}_+$, namely: $L=a_1Y_1+\ldots+a_nY_n$, calling it "basic" in the sequel. We study the associated L-gradation on $\mathbb{Z}_+^n$ (resp. on $\mathbb{Z}^n$).

Since $\mathrm{Im}(\bar{f}_L)=\mathbb{Z}$ for a basic L, the above exact sequence becomes:

$$0 \to G_o(L) \to \mathbb{Z}^n \to \mathbb{Z} \to 0,$$

splitted as well. The free abelian group $G_o(L)$ (of rank (n-1)) is here called "the directional group" of L.

The image of the L-gradation on $\mathbb{Z}_+^n$, is the submonoid of $\mathbb{Z}_+$, generated by the coefficients of L. It will be denoted by $\langle L \rangle$, its main property being the following well-known one (whose proof is left to the reader):

2. Proposition

Let L be a normalized, non-degenerate linear form in $n\geq 2$ variables over $\mathbb{Z}_+$. Then $\langle L\rangle$ is a numerical submonoid of $\mathbb{Z}_+$, generated by n elements.

Let us remind that a "numerical" submonoid $N\subseteq\mathbb{Z}_+$ is such that there is an integer $m\geq 0$ and $[m,\infty)=\{k\in\mathbb{Z}_+/k\geq m\}\subseteq N$. The least suc integer is denoted here by $p(N)$. The finite set $\mathbb{Z}_+\setminus N$ is called "the gap set" of N.

An "ideal" I of a numerical monoid N, is a subset $I\subseteq N$ such that $I+N\subseteq I$. An ideal of a numerical monoid obviously remains a numerical monoid.

For a basic linear form in n variables L, the integer $p(L)=$ $=p(\langle L\rangle)$ is not easyly computable, even in particular cases. Here is a sample:

Proposition (Herzog, [5])

Let $a_1,\dots,a_n\in\mathbb{Z}_+\setminus\{0\}$ generate in $\mathbb{Z}_+$ a numerical submonoid N (i.e. gcd $(a_1,\dots,a_n)=1$). Suppose N has the property:

$(\forall)$ $j\in\{1,2,\dots,n-1\}$, $h_j=\mathrm{lcm}(\gcd(a_1,\dots,a_j),a_{j+1})\in N$

Then $p(N)=\sum_{j=1}^{n}(h_j-a_j)+a_n+1$.

A numerical monoid N having the enounced property is necessarly "symmetric", i.e. $z\in N$ iff $p(N)-1-z\in N$ for any $z\in\mathbb{Z}_+$. (Monoid algebras of symmetric monoids are Gorenstein and monoid algebras of monoids as the one in the Proposition are complete intersections, cf. [5]).

Thus, for a "general" basic linear form L on $\mathbb{Z}_+^n$, the correspoding L-gradation has finite fiber over any $m\in\mathbb{Z}_+$, but this fiber is void as soon as m is a gap of $\langle L\rangle$.

The gap set of $\langle L\rangle$ being finite, the fibers of the L-gradation are non-void over all integers from $[p(L),\infty)$.

For a fixed basic form $L=a_1Y_1+\ldots+a_nY_n$, we denote by:

(1) $$F(m)=\{\xi\in\mathbb{Z}^n_+/\,|\xi|_L = m\}$$

the fiber of the L-gradation over $m\in\mathbb{Z}_+$.

Thus $F(0)=\{0\}$, $F(m)$ is finite for all $m\geq 1$ and $F(m)\neq\emptyset$ iff $m\in\langle L\rangle$.

Obviously $\mathbb{Z}^n_+ = \dot{\bigcup}_{m\in\langle L\rangle} F(m)$ and $F(m)\cap F(m')=\emptyset$ when $m\neq m'$. More: $F(m)+F(m')\subseteq F(m+m')$ for all $m,m'\in\mathbb{Z}_+$.

Now, having fixed an L-degree $m\in\langle L\rangle$, to any element $\xi\in F(m)$ we associate the following subset of the directional group of L:

(2) $$\Delta(\xi)=\{\alpha\in G_o(L)/\,\xi+\alpha\geq 0 \text{ in } \mathbb{Z}^n\},$$

where $\leq$ is the fixed partial order on $\mathbb{Z}^n$.

If $\mathcal{F}(G_o(L))$ denotes the set of all finite subsets in $G_o(L)$, (2) gives a function:

(2)' $$\Delta : \mathbb{Z}^n_+ \longrightarrow \mathcal{F}(G_o(L)).$$

3. *Proposition*

Let $m\in\langle L\rangle\setminus 0$ be an L-degree.

(i) *$F(m)=\xi+\Delta(\xi)$ for any $\xi\in F(m)$*

(ii) *$\Delta(\xi')=\Delta(\xi)+(\xi-\xi')$ for any $\xi, \xi'\in F(m)$*

(iii) *$\Delta(\xi)=\{\eta-\xi/\eta\in F(m)\}$ for any $\xi\in F(m)$*

(iv) *The function $\Delta:\mathbb{Z}^n_+\longrightarrow\mathcal{F}(G_o(L))$ is increasing, where $\mathbb{Z}^n_+$ has the lattice structure given by the restriction of $\leq$ from $\mathbb{Z}^n$ and $\mathcal{F}(G_o(L))$ is ordered by inclusion.*

Proof

(i) If $\alpha\in\Delta(\xi)$, then $\xi+\alpha\in\mathbb{Z}^n_+$ so $|\xi+\alpha|_L=|\xi|_L+|\alpha|_L=m+0=m$, giving $\xi+\alpha\in F(m)$. Conversely, for any $\eta\in F(m)$; $\alpha=\eta-\xi\in\Delta(\xi)$, because

$\eta=\xi+\alpha\geq 0$, so $\eta\in\xi+\Delta(\xi)$.

(ii) By (i): $F(m)=\xi+\Delta(\xi)=\xi'+\Delta(\xi')$ and the assertion follows.

(iii) By (i): $F(m)=\xi+\Delta(\xi)$, so $\Delta(\xi)=F(m)-\xi$ in $\mathbb{Z}^n$.

(iv) Let $\xi\leq\eta$ in $\mathbb{Z}_+^n$. Then $\alpha\in\Delta(\xi)\Rightarrow\xi+\alpha\geq 0$ so $\eta+\alpha\geq\xi+\alpha\geq 0$, showing that $\alpha\in\Delta(\eta)$. Therefore $\Delta(\xi)\subseteq\Delta(\eta)$.

Since $F(m)$ is finite (for $m\in\mathbb{Z}_+$), it follows from (i), Prop. that $\Delta(\xi)$ is finite for any $\xi\in F(m)$ and more: $\#\Delta(\xi)=\#F(m)$. On each fiber $F(m)$, the correspondence Δ(of (2)') takes $F(m)$ diferent values, therefore its restriction $\Delta|_{F(m)}$ is injective. More, Δ takes the clutter $(F(m),\leq)$ into the clutter $(\{\Delta(\xi)\}_{\xi\in F(m)},\subseteq)$.

In general, the monotonous correspondence Δ(of (2)') is not strict, i.e. $\xi\leq\eta$ in $\mathbb{Z}_+^n$ and $\Delta(\xi)=\Delta(\eta)$, doesn't imply $\xi=\eta$. However, it has the following useful property.

4. Proposition

Let $m\in\langle L\rangle\setminus 0$ be an L-degree and $\xi\in F(m)$ an element. The subgroup generated in $G_o(L)$ by $\Delta(\xi)$ depends only on m and not on ξ.

Proof

Let $\xi,\xi',\xi''\in F(m)$ be any elements. The identity:

$$\xi''-\xi=(\xi''-\xi')-(\xi-\xi'),$$

together with (iii) of Prop.3, shows that any element of $\Delta(\xi)$ belongs to the subgroup generated by $\Delta(\xi')$ inside $G_o(L)$. So $\langle\Delta(\xi)\rangle\subseteq\langle\Delta(\xi')\rangle$, where $\langle M\rangle$ denotes the subgroup generated by the set M.

The converse inclusion is a result of (iii), Prop.3 and of th identity $\xi''-\xi'=(\xi''-\xi)-(\xi'-\xi)$.

This result puts forward the groups:

(3) $$G_o(m)=\langle\Delta(\xi)\rangle\subseteq G_o(L),\ m>0 \text{ and } \xi\in F(m).$$

These groups are free subgroups of $G_o(L)$, therefore $\mathrm{rk}G_o(m)\leq$ $\leq n-1$ for any $m\in\langle L\rangle\setminus 0$.

They have the following remarkable properties.

5. Proposition

(i) For any L-degree $m\in\langle L\rangle\setminus 0$ there is an integer $g(m)>0$ such that:

(4) $$G_o(m)\subseteq G_o(2m)\subseteq\ldots\subseteq G_o(km)=G_o(L) \text{ for any } k\geq g(m)$$

and $g(m)$ is the least integer k, such that $G_o(km)=G_o(L)$

(ii) There is an integer $g(L)>0$, such that $g(m)=1$ for any $m\geq g(L)$.

Proof.

(i) By the definition (3) of $G_o(m)$, together with (iv) of Prop.3 it follows that $G_o(m)\subseteq G_o(2m)\subseteq\ldots\subseteq G_o(km)\subseteq\ldots\subseteq G_o(L)$ $(k\geq 1)$, since $\xi\leq 2\xi\leq\ldots\leq k\xi\leq\ldots$ $(k\geq 1)$ is an ascending chain in $\mathbb{Z}^n_+$. This sequence of groups must stabilize, $G_o(L)$ being a noetherian $\mathbb{Z}$-module. So, let $g(m)$ be its least stabilization index i.e.:

(*) $$G_o(m)\subseteq\ldots\subseteq G_o(g(m).m)\subseteq G_o(L) \text{ and } G_o(km)=G_o(g(m)m),$$

for $k\geq g(m)$.

Let $\alpha\in G_o(L)$ be an arbitrary element and consider its coordinates in the canonical basis E of $\mathbb{Z}^n$: $\alpha=(\alpha_1,\ldots,\alpha_n)$. Put $\bar{\alpha}=(|\alpha_1|,\ldots,|\alpha_n|)$ (where $|\alpha_i|$ means the absolute value of α_i,

$j=1,2,\dots,n$). Then $\overline{\alpha}\geq 0$ and more $\alpha+\overline{\alpha}\geq 0$ in $\mathbb{Z}^n$, so $\alpha\in\Delta(\overline{\alpha})$. Put $k=|\overline{\alpha}|_L$, the L-degree of $\overline{\alpha}$. Then $\alpha\in\Delta(\overline{\alpha})\subseteq\Delta(m.\overline{\alpha})\subseteq G_o(km)$, so $\alpha\in\bigcup_{k\geq 1} G_o(km)=G_o(g(m)m)$, by (*).

Therefore $G_o(L)\subseteq G_o(g(m)m)$, this giving (4).

(ii) Let $I=\{m\in\langle L\rangle / g(m)=1\}$. We show that I is a non-void idea of $\langle L\rangle$, this yielding the conclusion via the property of $\langle L\rangle$ of being a numerical monoid. So, we prove the assertions:

(a) $I\neq\emptyset$ and (b) $I+\langle L\rangle\subseteq I$.

Proof of (a)

Let $\mathcal{B}=\{\varepsilon_1,\dots,\varepsilon_{n-1}\}$ be any basis of the free abelian group $G_o(L)$. Consider the coordinates of the vectors $\varepsilon_1,\dots,\varepsilon_{n-1}$ in the canonical basis E of $\mathbb{Z}^n$, namely: $\varepsilon_j=(\varepsilon_{j1},\dots,\varepsilon_{jn})$, $j=1,2,\dots,n-1$, with $\varepsilon_{ij}\in\mathbb{Z}$. We construct the element of $\mathbb{Z}^n$, having the coordinates:

$$w_B=(\max_{1\leq j\leq n-1}|\varepsilon_{j1}|,\dots,\max_{1\leq j\leq n-1}|\varepsilon_{jn}|),$$

where $|\varepsilon_{ji}|$ is the absolute value of the integer ε_{ji}, for all j,i. Then $w_B\geq 0$ in $\mathbb{Z}^n$ and, by its very definition, $w_B+\varepsilon_j\geq 0$ in $\mathbb{Z}^n$ for $j=1,2,\dots,n-1$. Therefore, by (2), $\varepsilon_j\in\Delta(w_B)$ for $j=1,2,\dots,n-1$, so $B\subseteq\Delta(w_B)$, which by (3) gives $G_o(L)\subseteq G_o($ with $m=|w_B|_L$ such that $G_o(L)=G_o(m)$ and $m\in I$.

Proof of (b)

Let $m\in I$ and $h\in\langle L\rangle$ and pick $\xi\in F(m)$, $\eta\in F(h)$.

Then $\Delta(\xi)\subseteq\Delta(\xi+\eta)$ by (iv) of Prop.2, so $G_o(L)=G_o(m)$ is contained in $G_o(m+h)$ $(=\langle\Delta(\xi+\eta)\rangle$, by Prop.4). This gives $G_o(L)=$ $=G_o(m+h)$, i.e. $m+h\in I$ and the proof is finished.

The interpretation of the integers $\{g(m)/m\in\langle L\rangle\}$, defined at (i) Proposition 5, will be given in the next section.

Now, we go into more detail in describing the fibers of the L-gradation on $\mathbb{Z}_+^n$, i.e. the finite sets $\Delta(\xi), \xi\in\mathbb{Z}_+^n$, introduced at (2) above. To this end, we first remark (cf. (ii) of Prop.5) that if $m\geq g(L)$, then $\Delta(\xi)$ generates the directional group $G_o(L)$, for any $\xi\in F(m)$. Then $\Delta(\xi)$ also generates the $\mathbb{Q}$-vector space $G_o(L)\otimes_{\mathbb{Z}}\mathbb{Q}$, which means that $\Delta(\xi)$ contains a $\mathbb{Q}$-basis of the free abelian group $G_o(L)$.

Conversely, if $m\in\langle L\rangle\setminus 0$ and $\xi\in F(m)$ are such that $\Delta(\xi)$ contains a $\mathbb{Q}$-basis of $G_o(L)$, then any $\alpha\in G_o(L)$ has a natural multiplier p, such that $p\alpha\in G_o(m)$. This p may be taken the same for all $\alpha\in G_o(L)$, because this group is finitely generated. This means $p\cdot G_o(L)\subseteq G_o(m)$, i.e. $G_o(L)/G_o(m)$ is finite, of exponent p. In particular $p\Delta(\xi)\subseteq\Delta(p\xi)$ generates $G_o(L)$, so $g(m)\leq p$. Thus, at least for $m\geq g(L)$, we may represent all elements of $\Delta(\xi)$, ξ $F(m)$, in a certain $\mathbb{Q}$-basis $B\subseteq\Delta(\xi)$ of $G_o(L)$. This is, however, too general for our purposes and at this point we force enter into play the coefficients of the basic form L.

6. Proposition

Let $L=a_1Y_1+\ldots+a_nY_n$ be a basic linear form in $n\geq 2$ variables. Let $m\in\langle L\rangle - 0$ be an L-degree with the property:

(5) $(\exists)j\in\{1,2,\ldots,n\}$ and $m=k.a_j$ with $k\geq\max\{a_i/i\neq j\}$.

Then there are: an element $\xi=\xi(m)\in F(m)$ and a $\mathbb{Q}$-basis $B_m=\{\varepsilon_i/i\in\{1,\ldots,n-1\}\setminus j\}$ of $G_o(L)$, such that:

(i) $B_m\subseteq\Delta(\xi)$

(ii) $\Delta(\xi)=\{a_j^{-1}(\sum_{i\neq j}x_i\varepsilon_i)/x_i\in\mathbb{Z}_+$ for all i and $\sum_{i\neq j}a_ix_i\leq m\}$.

Proof

For convenience, suppose j=1, such that $m=k.a_1$, with $k\geq\max\{a_i/i=2,3,\ldots,n\}$.

We choose the element $\xi(m)=\xi\in F(m)$, having in the canonical basis of $\mathbb{Z}^n$, the coordinates:

$$\xi = (k,0,0,\dots,0).$$

In $G_o(L)$ we consider the natural $\mathbb{Q}$-basis B, made - up by the vectors $\varepsilon_2,\dots,\varepsilon_n$, whose coordinates in the canonical basis o $\mathbb{Z}^n$ are:

$$\varepsilon_2=(-a_2,a_1,0,\dots,0),\ \varepsilon_3=(-a_3,0,a_1,0,\dots,0),\dots.$$
$$\dots,\varepsilon_n=(-a_n,0,\dots,0,a_1).$$

Our assumption on k shows that $\varepsilon_2,\dots,\varepsilon_n\in\Delta(\xi)$, for the above chosen ξ, so $B\subseteq\Delta(\xi)$ and (i) is fulfilled.

Now, any element $\alpha\in\Delta(\xi)$ may be uniquely written:

$$\alpha = \frac{1}{a_1}x_2\varepsilon_2+\frac{1}{a_1}x_3\varepsilon_3+\dots+\frac{1}{a_1}x_n\varepsilon_n,$$

with $x_2,\dots,x_n\in\mathbb{Z}$.

In the canonical basis of $\mathbb{Z}^n$, every such α has the coordinate

$$\alpha = \Big(-\frac{1}{a_1}\Big(\sum_{i=2}^{n} x_i a_i\Big),\ x_2,x_3,\dots,x_n\Big).$$

Thus, the definition (3) of $\Delta(\xi)$ gives: $\alpha\in\Delta(\xi)$ iff $\alpha+\xi\geq 0$ in $\mathbb{Z}^n \Leftrightarrow k-\frac{1}{a_1}\Big(\sum_{i=2}^{n} x_i a_i\Big)\geq 0$ and $x_j\geq 0$ for $j=2,3,\dots,n$.

This is precisely what (ii) says.

The representation (ii) of Proposition 6 is important, becau- se it identifies $\Delta(\xi)$ with a homotethical image of a certain order-ideal in a monoidal poset, provided (5) is fulfilled. This identification is meaningful in the study of the monoids considered at § 2.

In view of future application, we give a name to the condition (5) of Proposition 6, saying that: "m is standard for L, in direction j" as soon as (5) takes place.

Let us remark that any $m \geq \max\{a_i / i \neq j\}$ is standard in direction j for L, if $a_j=1$.

As Proposition 6 shows, there are many integers m, which are standard in direction j for L, for each $j \in \{1,2,\ldots,n\}$.

If $m \in \langle L \rangle$ is standard for L in every direction $j \in \{1,2,\ldots,n\}$, we say that "(L,m) is a standard pair". This obviously comes to: $m \equiv 0 \pmod{\operatorname{lcm}_{1 \leq j \leq n}(a_j)}$, where "lcm" is "the lowest common multiple".

In order to give the announced interpretation for $\Delta(\xi)$ ($\xi \in F(m)$ and m standard in some direction j for L), let us consider the subgroup of $G_o(L)$, generated by the special $\mathbb{Q}$-basis $B_m \subseteq \Delta(\xi)$. Let $\langle B_m \rangle$ be this subgroup. In it , B_m becomes an integral basis, so B_m canonically defines a partial order on $\langle B_m \rangle$, having $\langle B_n \rangle_+ = \{\sum_{i \neq j} x_i \varepsilon_i / x_i \in \mathbb{Z}_+\}$ as the set of all positive elements. An "order ideal" in a poset is a subset which, together with an element, contains all elements below it (i.e. a subset which is "filtered below"). Now, in $\langle B_m \rangle_+$, the set: $\Theta(\xi) = \{\sum_{i \neq j} x_i \varepsilon_i / \sum_{i \neq j} a_i x_i \leq m\}$ is obviously an order-ideal, connected to our set $\Delta(\xi)$ by:

$$(6) \qquad a_j \, \Delta(\xi) = \Theta(\xi),$$

(cf.Prop.6, (ii)), where $a_j \Delta(\xi) = \{a_j \alpha / \alpha \in \Delta(\xi)\}$.

Since $\Theta(\xi)$ is finite, it is finitely generated (a "generator" of an order ideal being one of its maximal elements) and (6) allows on $\Delta(\xi)$ several conclusions valid for $\Theta(\xi)$ (see below, §3).

Now, we consider a standard pair (L,m) and prove its main property, under the following form.

7. Proposition

Let $L=a_1Y_1+\ldots+a_nY_n$ be a basic linear form in $n\geq 2$ variables and let $m>0$ be an integer such that $m\equiv 0 \pmod{\operatorname{lcm}_{1\leq j\leq n}(a_j)}$. For any integer $k\geq 1$, consider the linear equation:

$(\mathcal{E}_k)$ $L(Y_1,\ldots,Y_n)=km$.

Then any solution from $\mathbb{Z}_+^n$ to $(\mathcal{E}_k)$ is a sum of k solutions from $\mathbb{Z}_+^n$ to $(\mathcal{E}_1)$.

Proof.

We proceed by induction on k, the case $k=1$ being trivial.

Thus, we suppose the assertion true for any $1\leq k'<k$ and prove it for k. The main tool in our proof is the following decomposition theorem for latticially ordered abelian groups (cf. [4], § 1, 10):

(DT) let $(x_i)_{1\leq i\leq p}$ and $(y_j)_{1\leq j\leq q}$ be two finite sequences of positive elements in the latticially ordered abelian group G such that: $\sum_{i=1}^{p}x_i=\sum_{j=1}^{q}y_j$.

Then there is a double sequence $(z_{ij})_{1\leq i\leq p,\ 1\leq j\leq q}$ of positive elements in G, such that:

$$x_i=\sum_{j=1}^{q}z_{ij} \text{ for all } i \text{ and } y_j=\sum_{i=1}^{p}z_{ij} \text{ for all } j.$$

Coming back to our proof, let $(x_1,\ldots,x_n)$ be a solution from $\mathbb{Z}_+^n$ to $(\mathcal{E}_k)$. Since (L,m) is a standard pair, $m/a_j\in\mathbb{Z}_+$ for every $j\in\{1,2,\ldots,n\}$, so there are non-negative integers $y_1,\ldots,y_n$ and $r_1,\ldots,r_n$ such that:

$$(*) \qquad x_j=(m/a_j)y_j+r_j,\ 0\leq r_j<m/a_j \quad \text{for } j=1,2,\ldots,m.$$

But $(x_1,\ldots,x_n)$ is a solution to $(\mathcal{E}_k)$, so we get that $(r_1,\ldots,r_n)$ is a solution from $\mathbb{Z}_+^n$ to $(\mathcal{E}_{k'})$, with $k'=k-(\sum_{j=1}^{n}y_j)$. If $k'=0$, then $r_1=r_2=\ldots=r_n=0$ and $x_j=(m/a_j)y_j$, $j=1,\ldots,n$. We apply to $\sum_{j=1}^{n}y_j=1+\ldots+1$ (k times) the decomposition theorem (DT) for $G=\mathbb{Z}$, thus decomposing each y_j in

$_1,\ldots,x_n)$ into a sum of k solutions from $\mathbb{Z}^n$ to $(\mathcal{E}_1)$.

If $k'\neq 0$, then $k'<k$ and the induction hypothesis applied to $(\mathcal{E}_{k'})$ shows that there are k' solutions from $\mathbb{Z}^n_+$ to $(\mathcal{E}_1)$, say: $(r_{11},\ldots,r_{1n}),\ldots,(r_{k'1},\ldots,r_{k'n})$, such that

$$(**) \qquad r_j=\sum_{i=1}^{k'} r_{ij}, \quad \text{for } j=1,2,\ldots,n$$

Now, applying the (DT) for $\mathbb{Z}$ to $\sum_{j=1}^{n} y_j+k'=1+\ldots+1$ (k times), we find two families of non-negative integers $(z_{ji})_{1\leq j\leq n,\ 1\leq i\leq k}$ and $(t_i)_{1\leq i\leq k}$, such that:

(a) $y_j=\sum_{i=1}^{k} z_{ji}$ for all j

(b) $k'=\sum_{i=1}^{k} t_i$

(c) $t_i+\sum_{j=1}^{n} z_{ji}=1$, for all i.

The relation (c) shows that there is a partition of $\{1,2,\ldots,k\}$ with two non-void blocks: A,B, such that: $\#A=k-k'$, $\#B=k'$ and: $(z_{ji})_{1\leq j\leq n}=(0,\ldots,0)$ iff $i\in B$, $\sum_{j=1}^{n} z_{ji}=1$ iff $i\in A$, respectively $t_i=0$ iff $i\in A$ and $t_i=1$ iff $i\in B$.

Using (a), it follows that $y_j=\sum_{i\in A} z_{ji}$ for all j, so (*) becomes:

$$x_j=\sum_{i\in A}(m/a_j)z_{ji}+r_j,\ j=1,2,\ldots,n.$$

Also, (b) becomes: $k'=\sum_{i\in B} t_i$, which allows us to write (**) under the form:

$$(**)' \qquad r_j=\sum_{i\in B} r_{ij}, \text{ for } j=1,2,\ldots,n.$$

Therefore we obtain the following decomposition into k vectors from $\mathbb{Z}_+^n$ of $(x_1,\dots,x_n)$:

$$(***)\quad x_j=\sum_{i\in A}(m/a_j)z_{ji}+\sum_{i\in B}r_{ij},\ \text{for } j=1,2,\dots,n.$$

The definition of A shows that $((m/a_j)z_{ji})_{1\leq j\leq n}$ is a solutio to $(\mathcal{E}_1)$ for $i\in A$ and the definition of B (together with the i duction hypothesis) shows that $(r_{ij})_{1\leq j\leq n}$ is a solution to $(\mathcal{E}_1)$ for $i\in B$.

Thus (***) is a decomposition of $(x_j)_{1\leq j\leq n}$ into a sum of k solutions from $\mathbb{Z}_+^n$ to $(\mathcal{E}_1)$ and the proof is finished.

One easily verifies that $m\not\equiv 0 \pmod{a_j}$ for some $j\in\{1,\dots,n\}$, even when m is standard for L in some other direction $j'\neq j$, makes untrue the assertion of Proposition 7, inforcing the seemingly true fact that the converse to Proposition 7 also holds. We close this section with the remark that little is known, in general, about the cardinalities of the fibers $\{F(m)/m>0\}$, in terms of the coefficients of the basic form L. One may give an upper bound to every $\#F(m)$, $m>0$, in these terms, provided such upper bounds are given for the component (in the canonical basis of $\mathbb{Z}^n$) of every $\xi\in F(m)$ (cf.A.O.Gel' fond and Yu.V.Linnik, Elementary Methods in the Analytic Theory of Numbers, Pergamon Press (1966), ch.2, § 3). The Hilbert series technique (see below) perhaps allows further information, but we won't stop doing this here, since our interes grows into qualitative algebraic properties of the objects described into the next section.

3. Veronese submonoids of free abelian monoids

We keep into force the definition and notations of § 2.

Let $L=a_1Y_1+\ldots+a_nY_n$ be a basic linear form over $\mathbb{Z}_+$, in $n\geq 2$ variables.

For any L-degree $g\in\langle L\rangle\setminus 0$, we consider the principal submonoid $\mathbb{Z}_+g$ of $\mathbb{Z}_+$. Its pre-image by the L-gradation on $\mathbb{Z}_+^n$, is a submonoid of $\mathbb{Z}_+^n$, denoted by V(L,g) and called "the Veronese monoid, associated to the pair (L,g)". As a submonoid of $\mathbb{Z}_+^n$, V(L,g) is "the g-th Veronese selection into the L-gradation on $\mathbb{Z}_+^n$ ". The Veronese monoid V(L,sg), for s>0, is called "the s-th Veronese selection" into V(L,g) and is denoted here by $V^{(s)}(L,g)$. The monoid V(L,g) is naturally graded by L, namely:

$$(7)\quad V(L,g)=\dot{\bigcup}_{m\geq 0}V_m(L,g),\ \text{with } V_m(L,g)=F(mg)\ \text{(cf. (1))}.$$

We reffer to (7) as "the inner gradation" on $V_m(L,g)$. The main algebraic "invariant" of the graded monoid V(L,g), is its Hilbert series, defined by:

$$(8)\quad H_{L,g}(z)=\sum_{m\geq 0}(\#V_m(L.g))z^m\in\mathbb{Z}[[z]].$$

(It represents a rational function with integral coefficients, since the monoid algebra V(L,g) , whose usual Hilbert series is (8) (when graded by (7)), is finitely generated over $\mathbb{C}$).
For any s>0, the Hilbert series of $V^{(s)}(L,g)$ is connected to (8) by:

$$(9)\quad H^{(s)}_{L,g}(z)=1/s\sum_{j=0}^{s-1}H_{L,g}(\omega^j z^{1/s}),$$

ω being a primitive s-root of 1 in $\mathbb{C}^*$.

In order to clarify how V(L,g) embedds into $\mathbb{Z}_+^n$, let us shortly remind an important notion, essentially due to Hochster ([6]

On any abelian, cancellative monoid $(M,+)$ (with unit 0) ther is a natural poset structure $\le_M$, compatible with the algebra structure, namely: for $x,y\in M$, $x\le_M y$ iff $(\exists)$ $z\in M$ and $x+z=y$.

If $x+y=0$ in M implies $x=y=0$, then $\le_M$ uniquely extends to the universal abelian group $G(M)$ of M, such that $G_+(M)=\{z\in G(M)/ /z\ge_M 0\}$ is identified to M.

If $N\subseteq M$ is a submonoid, then it carries two poset structures: the inner one $\le_N$ and the restriction of $\le_M$.

We say that "N is normal in M" if these two poset structures coincide on N.

This comes to $N=G(N)\cap M$, where $G(N)$ is the universal abelian group of N (canonically embedded in $G(M)$). In general, $\tilde{N}=G(N)\wedge M$ is the least normal submonoid of M, containing N. $\tilde{N}$ is called "the normalization" of N.

The importance of this notion may be underlined by quoting the following result of Hochster (loc.cit):

"*If* M *is a finitely generated, normal submonoid of a free abelian monoid* $\mathbb{Z}_+^n$, *then its monoid algebra* $\mathbb{C}[M]$ *is a Cohen-Macaulay domain*".

Now, coming back to Veronese monoids, we may prove the following

8. *Proposition*

With L,g *as above, the Veronese monoid* V(L,g) *is a finitely generated, normal submonoid of* $\mathbb{Z}_+^n$.

Proof.

Let $\xi,\eta\in V(L,g)$ and $\xi\ge\eta$ in $\mathbb{Z}_+^n$ (i.e. in $\mathbb{Z}^n$, cf.§2). Then $\xi-\eta\in\mathbb{Z}_+^n$ and $|\xi-\eta|_L=|\xi|_L-|\eta|_L\equiv 0-0\equiv 0 \pmod g$, such that $\xi-\eta\in V(L,g)$, which means $\xi\ge\eta$ in $V(L,g)$. The finite generatedness of V(L,g) is seen by identifying its monoid algebra of a finite (cyclic) group on $\mathbb{C}[\mathbb{Z}_+^n] = \mathbb{C}[X_1,\ldots,X_n]$ (cf.§1), then applying the Hilbert-Noether theorem.

This result shows that the canonical poset structure on V(L,g) is precisely the one induced by the lattice $(\mathbb{Z}_+^n,\leq)$, so the notation $\leq$ for the partial order on V(L,g) may produce no confusion.

Let G(L,g) be the universal abelian group of V(L,g). Then G(L,g) is canonically identified to an ordered subgroup of $\mathbb{Z}^n$, such that $G_+(L,g)=V(L,g)$ (where $G_+(L,g)$ is defined as $G(L,g)\cap\mathbb{Z}_+^n$), because of the normality asserted by Prop.8.

Remark

The normality of V(L,g) into $\mathbb{Z}_+^n$ is essentially the consequence of two facts: firstly, that the coefficients of L are all positive and secondly, that V(L,g) consists of all solutions from $\mathbb{Z}_+^n$ to $L(Y)\equiv 0$ (mod g).

Having seen how the natural poset structure extends from V(L,g) to G(L,g), we must further clarify how the inner gradation (7) does the same.

Since G(L,g) is the universal abelian group of V(L,g), the inner gradation (7), considered as a surjective monoid homomorphism $V(L,g) \xrightarrow{f_{L,g}} \mathbb{Z}_+$ (we remind that $g\in\langle L\rangle$ is not a gap of $\langle L\rangle$), uniquely extends to a surjective group homomorphism $\bar{f}_{L,g}:G(L,g)\longrightarrow\mathbb{Z}$. If $G_o(L,g)=\ker(\bar{f}_{L,g})$, then the following exact sequence:

$$(10) \qquad 0\to G_o(L,g)\to G(L,g) \xrightarrow{\bar{f}_{L,g}} \mathbb{Z}\to 0,$$

splits, $\mathbb{Z}$ being free. Therefore, rk $G(L,g)=1+\mathrm{rk}G_o(L,g)$.

9. Proposition

(i) $G(L,g)=\{\xi\in\mathbb{Z}^n / |\xi|_L\equiv 0 \pmod g\}$

(ii) $G_o(L,g)$ coincides with the directional group $G_o(L)$.

Proof

(i) If $\omega\in G(L,g)$, then $\omega=\xi-\xi'$ for some $\xi,\xi'\in V(L,g)$. This means $|\xi|_L\equiv|\xi'|_L\equiv 0 \pmod g$, so $|\omega|_L = |\xi|_L - |\xi'|_L\equiv 0 \pmod g$.

Conversely, let $\omega\in\mathbb{Z}^n$ be such that $|\omega|_L\equiv 0 \pmod g$.

As $\mathbb{Z}^n$ is the universal abelian group of $\mathbb{Z}^n_+$, we can write: $\omega=\eta-\eta'$, for some $\eta,\eta'\in\mathbb{Z}^n_+$. From $|\omega|_L\equiv 0 \pmod g$ we get $|\eta|_L\equiv|\eta'|_L\equiv k \pmod g$, with $k\in\{0,1,\dots,g-1\}$. From Prop.2, 2, we get an element $\mu\in\mathbb{Z}^n_+$, such that $|\mu|_L\equiv g-k \pmod g$ (for instance, $|\mu|_L\equiv mg+g-k$, for $m\geq p(L)$).

Then $\eta+\mu$, $\eta'+\mu$ both belong to $\mathbb{Z}^n_+$ and $|\eta+\mu|_L\equiv|\eta'+\mu|_L\equiv k+g-k\equiv 0 \pmod g$. Therefore $\eta+\mu$ and $\eta'+\mu$ both belong to $V(L,g)$. Since $\omega=\eta-\eta'=(\eta+\mu)-(\eta'+\mu)$, it follows that $\omega\in G(L,g)$.

(ii) By the very definition of $G_o(L,g)$ it follows that $G_o(L,g)=\{\omega\in G(L,g) / |\omega|_L=0\}\subseteq\{\theta\in\mathbb{Z}^n / |\theta|_L=0\}=G_o(L)$.

By (i), we see that $\Delta(\xi)\subseteq G_o(L,g)$ for any $\xi\in V(L,g)$ (cf. (2), §2), i.e. $G_o(kg)\subseteq G_o(L,g)$ for any $k\geq 1$ (cf. (3), §2), giving by (4), Prop.5, §2: $G_o(L)=\bigcup_{k\geq 1} G_o(kg)\subseteq G_o(L,g)$.

We shall be further concerned with an important property appertaining to graded structures, namely their standardness.

Let us remind that a graded monoid $M=\dot{\bigcup}_{m\geq 0} M_m$ is called "standard" iff it is generated by its first degree component M_1. This means: $M_m=M_1+\dots+M_1$ (m times) in M, for any $m>0$ and $M_o=\{0\}$. Denoting by $\langle M_1\rangle$ the submonoid generated in M by the first degree component M_1, the standardness of the given gradation obviously comes to: $M=\langle M_1\rangle$.

In particular, this trivially implies that M is the normalization of $\langle M_1\rangle$ inside M. When only this weaker condition holds (i.e. M coincides with the normalization $\widetilde{\langle M_1\rangle}$ of $\langle M_1\rangle$ inside ven gradation. Now, coming to our particular case, the following facts may be proven.

10. *Proposition*

Let L be a basic linear form in $n\geq 2$ variables.

Then there is an integer $g(L)$ (precisely the one defined at (ii), Prop.5, § 2) *such that $V(L,g)$ is quasi-standard in its inner gradation, for any $g\geq g(L)$.*

Proof

We use (ii), Prop.5, § 2 and reduce the assertion in the enounce to the proof of the following equivalence:

(a) *$V(L,g)$ has quasi-standard inner gradation*

(b) *$G_o(L,g)=G_o(g)$.*

Proof of (a) $\Rightarrow$ (b)

(a) means that $V(L,g)$ is the normalization inside itself of the submonoid $\langle V_1(L,g)\rangle$, generated by its first degree component.

However, the monoid $\langle V_1(L,g)\rangle$ has $G_o(g)\oplus\mathbb{Z}.\xi$ as its universal abelian group, $\xi\in F(g)=V_1(L,g)$ being an arbitrary element. (Indeed, the universal abelian group of $\langle V_1(L,g)\rangle$ consists of all differences (inside $\mathbb{Z}^n$) of elements from $\langle V_1(L,g)\rangle$. But $\langle V_1(L,g)\rangle$ is itself standard in the induced inner gradation of $V(L,g)$, so, fixing an element $\xi\in V_1(L,g)$, we see that any $\eta\in\langle V_1(L,g)\rangle$ is of the form: $\eta=m\xi+\beta$, with $m\geq 0$ and $\beta\in\Delta(m\xi)=m\Delta(\xi)$. So, any difference $\eta-\eta'$ of elements from $\langle V_1(L,g)\rangle$, is of the form: $\eta-\eta'=(m-m')\xi+(\beta-\beta')$, with $m,m'\in\mathbb{Z}_+$ and $\beta\in m\Delta(\xi)$, $\beta'\in m'\Delta(\xi)$. This yields the conclusion).

Then $V(L,g)=\widetilde{\langle V_1(L,g)\rangle}=(G_o(g)\oplus\mathbb{Z}\xi)\cap V(L,g)$, so $V(L,g)\subsetneq$ $\subsetneq G_o(g)\oplus\mathbb{Z}\xi$. By the definition of the universal abelian group, it then follows that: $G(L,g)\subseteq G_o(g)\oplus\mathbb{Z}(\xi)\subsetneq G(L,g)$ (the last inclusion coming from $\langle V_1(L,g)\rangle \subseteq V(L,g)$), so that: $G(L,g)=G_o(g)\oplus\mathbb{Z}\xi$.

The exact sequence (10) readily gives: $G(L,g)=G_o(L,g)\oplus\mathbb{Z}\xi$, so $G_o(L,g)\oplus\mathbb{Z}\xi=G_o(g)\oplus\mathbb{Z}\xi$. But $G_o(g)\subseteq G_o(L)$ (cf. (3)) and $G_o(L)=G_o(L,g)$ (cf. (ii), Prop.9), so $G_o(g)\subseteq G_o(L,g)$. Together with $G_o(L,g)\oplus\mathbb{Z}\xi=G_o(g)\oplus\mathbb{Z}\xi$, this last inclusion gives (b).

Proof of (b) $\Rightarrow$ (a)

Reversing the implications, we deduce from (b) that $G(L,g)$ ($=G_o(L,g)\oplus\mathbb{Z}\xi$, for any fixed $\xi\in F(g)=V_1(L,g)$) is the universal abelian group of $\langle V_1(L,g)\rangle$. Then $\langle \widetilde{V_1(L,g)}\rangle=G(L,g)\cap V(L,g)$ $=V(L,g)$, i.e. (a) holds.

This result shows that, for a fixed gradation L on $\mathbb{Z}_+^n$, "almost all" Veronese selections $V(L,g)$ are quasi-standard in their inner gradation (7).

Remark

The integer $g(m)$ of (i), Prop.5, § 2 may now be interpreted as "the deviation from quasi-standardness" of the Veronese monoid $V(L,m)$.

About the actual standardness of the inner gradation of a Veronese monoid $V(L,g)$, the following simple criterium clarifies the situation.

11. Proposition

Let L be a basic form is $n\geq 2$ variables and $g\in\langle L\rangle\setminus 0$ an L-degree. The following are equivalent:

(i) $V(L,g)$ has standard inner gradation

(ii) $V(L,g)$ has quasi-standard inner gradation and $\langle V_1(L,g)\rangle$ is normal in $V(L,g)$.

(iii) For any $\xi\in V_1(L,g)$ and any integer $m\geq 1$, $\Delta(m\xi)=m\Delta(\xi)$ in $G_o(L)$

(i) $\Rightarrow$(ii). Indeed, $V(L,g)$ quasi-standard means that $V(L,g)= =\widetilde{\langle V_1(L,g)\rangle}$ and $\langle V_1(L,g)\rangle$ normal in $V(L,g)$ means that $\langle \widetilde{V_1(L,g)}\rangle=\langle V_1(L,g)\rangle$.

(i) $\Rightarrow$ (iii). $V(L,g)$ standard means: $V_m(L,g)=\sum_1^m V_1(L,g)$, for any $m\geq 1$, i.e. $F(mg)=\sum_1^m F(g)$ for $m\geq 1$. For any $\xi\in F(g)$, we know that: $F(mg)=m\xi+\Delta(m\xi)$, $m\geq 1$ (cf. (i), Prop.3, §2), so $m\xi+\Delta(m\xi)= =\sum_1^m(\xi+\Delta(\xi))=m\xi+m\Delta(\xi)$ and the cancellation property for $\mathbb{Z}_+^n$ yields the desired conclusion.

Remark

The explicit connection between (ii) and (iii) of Proposition 11, is the following. First, remark that (ii) splits into:

(a) $V(L,g)$ is quasi-standard iff $\Delta(\xi)$ generates $G_o(L)$ for any $\xi\in F(g)$

(b) $\langle V_1(L,g)\rangle$ is normal inside $V(L,g)$ iff $\Delta((p-q)\xi)\subseteq p\Delta(\xi)- -q\Delta(\xi)$, for any $p\geq q>0$.

By (ii) of Prop.5 (a) is covered by (iii) of Prop.11 and obviously the same is true for (b).

The above general considerations on the standardness of the inner gradation (7) of a Veronese monoid $V(L,g)$, do not give yet positive examples, but rather provide quick possibilities for counterexamples.

For instance, $V(L,g)$ cannot be standard when g is a gap of $\langle L\rangle$ (which is obvious), or when $g\in\langle L\rangle$ but $G_o(g)\neq G_o(L)$ (as the case of $L=3Y_1+5Y_2+6Y_3$, $g=8$ immediately shows).

More, even when g is standard in some direction j for L (see §2), the standardness of $V(L;g)$ may fail, as it is the case for $L=7Y_1+2Y_2+3Y_3$, $g=14$.

A positive answer to this question is contained into the next

12. Proposition

Let (L,g) be a standard pair (cf. § 2). Then the Veronese monoid V(L,g) has standard inner gradation.

Proof

The assertion is a mere translation of Proposition 7, § 2.

The next step we are taking, is the characterization of the homogeneous systems of parameters in Veronese monoids. They may not exist in general, however we are able to construct such systems in "sufficiently many" cases, the method giving the expected systems in many relevant particular cases.

Let us first remind that a "monomial system of parameters" in a Veronese monoid V(L,g) is a family of n=rk G(L,g) eleme $\xi_1,\dots,\xi_n$ from V(L,g), such that the submonoid $\langle\xi_1,\dots,\xi_n\rangle$ they generate in V(L,g), has the property:

(11) $(\forall)\ \eta\in V(L,g)$,$(\exists)\ p\in\mathbb{Z}_+\setminus\{0\}$ and $p\cdot\eta\in\langle\xi_1,\dots,\xi_n\rangle$.

When $\xi_1,\dots,\xi_n\in V_d(L,g)$, for some $d\geq 1$, such a system is calle "homogeneous", of degree d.

13. Proposition

Let $V(L,g)\in\mathbb{Z}_+^n$ be a Veronese monoid.

If g is standard in some direction j for L, then V(L,g) has an homogeneous monomial system of parameters.

Such a system may be chosen of degree $d\equiv 0 \pmod{\operatorname{lcm}_{1\leq i\leq n,\, i\neq j}(a_i)}$

$a_1,\dots,a_n$ being the coefficients of L.

Proof

We may take g standard in direction n for L, so an element $\xi\in F(g)$, and a Q-basis $B=\{\varepsilon_1,\dots,\varepsilon_{n-1}\}$ for $G_o(L)$ may be foun such that:

$$\Delta(\xi)=\Big\{a_n^{-1}\big(\sum_{j=1}^{n-1}x_j\varepsilon_j\big)/x_j\in\mathbb{Z}_+ \text{ for all } j \text{ and } \sum_{j=1}^{n-1}a_jx_j\leq g\Big\}.$$

Precisely the same argument as the one in Prop.6, §2 shows that, for any integer $m \geq 1$:

(a) $\Delta(m\xi)=\left\{a_n^{-1}(\sum_{j=1}^{n-1}x_j\xi_j)/x_j\in\mathbb{Z}_+ \text{ for all } j \text{ and } \sum_{j=1}^{n-1}a_jx_j\leq mg\right\}.$

For every $m \geq 1$, we define the integers:

(b) $r_j(m)=\max\left\{x_j\in\mathbb{Z}_+/(\exists)\alpha\in\Delta(m\xi) \text{ and } pr_{\varepsilon_j}(\alpha)=x_j\right\},$

where pr_{ε_j} is the projection on the ε_j-axis of $G_o(L)$.

We search for a system of parameters for $V(L,g)$, of the following form:

(c) $\xi_o=d\xi,\ \xi_1=d\xi+a_n^{-1}r_1(d)\varepsilon_1,\dots,\xi_{n-1}=d\xi+a_n^{-1}r_{n-1}(d)\varepsilon_{n-1},$

where $d>0$ is an integer to be found.

In order that (c) be a system of parameters, there must exis for any $\eta\in V(L,g)$, integers $p,\alpha_o,\alpha_1,\dots,\alpha_{n-1}\in\mathbb{Z}_+$, such that $p>0$ and:

(*.1) $p\eta=\alpha_o\xi_o+\alpha_1\xi_1+\dots+\alpha_{n-1}\xi_{n-1}.$

Let $k>0$ be the (inner) degree of η in $V(L,g)$. Then (a) gives $(n-1)$ non-negative integers $x_1,\dots,x_{n-1}$, uniquely dete mined by:

(*.2) $\eta=k\xi+a_n^{-1}(\sum_{j=1}^{n-1}x_j\alpha_j)$ and $\sum_{j=1}^{n-1}a_jx_j\leq kg.$

Replacing (c) and (*.2) into (x.1), we obtain:

$$pk\xi+a_n^{-1}(\sum_{j=1}^{n-1}px_j\varepsilon_j)=d(\sum_{i=0}^{n-1}\alpha_i)\xi+a_n^{-1}(\sum_{j=1}^{n-1}{}_jr_j(d)\varepsilon_j).$$

Taking the L-degrees and remembering that B is a $\mathbb{Q}$-basis in $G_o(L)$, we obtain from here:

$$pk=d\Big(\sum_{i=0}^{n-1}\alpha_i\Big) \text{ and } px_j=\alpha_j r_j(d), \text{ for } j=1,2,\ldots,n-1.$$

Choosing $p\equiv 0 \pmod{d\prod_{j=1}^{n-1} r_j(d)}$, there results: $\alpha_j=p.r_j(d)^{-1}.x_j\in\mathbb{Z}_+$ for $j=1,2,\ldots,n-1$ (because $p>0$). More: $\alpha_o= pd^{-1}k - \sum_{j=1}^{n-1}\alpha_j\in\mathbb{Z}$. We also need $\alpha_o\geq 0$, i.e. $\sum_{j=1}^{n-1}\alpha_j\leq pd^{-1}k$. Using the already found values of $\alpha_1,\ldots,\alpha_{n-1}$, this gives:

$$\sum_{j=1}^{n-1}pr_j(d)^{-1}x_j\leq pd^{-1}k,$$

equivalent to:

$$(**)\qquad \sum_{j=1}^{n-1}r_j(d)^{-1}x_j\leq d^{-1}k,$$

for any $(x_1,\ldots,x_{n-1})\in\mathbb{Z}_+^{n-1}$, verifying: $\sum_{j=1}^{n-1}a_jx_j\leq gk$.
If we can choose d such that: $dg\leq a_jr_j(d)$ for all $j\in\{1,\ldots\ldots,n-1\}$, then it will follow:

$$gr_j(d)^{-1}\leq d^{-1}a_j\Rightarrow gr_j(d)^{-1}x_j\leq d^{-1}a_jx_j \text{ for all } j,$$

such that $g\sum_{j=1}^{n-1}r_j(d)x_j\leq d^{-1}\sum_{j=1}^{n-1}a_jx_j\leq gd^{-1}k$, giving (**) after division by g.

So, we are left with the problem of finding $d>0$, such that $dg\leq a_jr_j(d)$, for $j=1,2,\ldots,n-1$.

But $a_n^{-1}r_j(d)\varepsilon_j\in\Delta(d\xi)$ by (b) and (a)(remember that $\Delta(d\xi)$ is essentially an order ideal), which means, again by (a):

$$a_jr_j(d)\leq dg.$$

Therefore, if such d exists, it has to verify:

(***) $\qquad a_j r_j(d)=dg, \qquad$ for $j=1,2,\dots,n-1$.

A natural choice for d would be: $d\equiv 0 \,(\text{mod} \operatorname*{lcm}_{1\leq i\leq n-1}(a_i))$, giving: $r_j(d)=(d/a_j)g$ for $j=1,2,\dots,n-1$, so the only problem is to show that this agrees with the definition (b) of the integers $\{r_j(m)\}_{m\geq 1}$.

Or, for such d, we obtain: $a_j r_j(d)=a_j(d/a_j)g=dg$, so (a) shows that $a_n^{-1}(d/a_j)g\varepsilon_j$ certainly belongs to $\Delta(d\xi)$ (for all j). If this is not the maximum along the ε_j-axis, then the actual max $r_j(d)$ should satisfy: $(d/a_j)g\lneqq r_j(d)$. Since $a_n^{-1}r_j(d)\varepsilon_j\in\Delta(d\xi)$, we would then obtain: $dg=(d/a_j)g.a_j \lneqq r_j(d)a$ $\leq gd$, a contradiction. Therefore (***) is fulfilled by the considered d and the proof is finished.

14. Corollary

If (L,g) is a standard pair, then the Veronese monoid V(L,g) has an homogeneous system of parameters of degree 1.

Proof

(L,g) being standard, g is in particular standard in direction n for L and more: $g\equiv 0 \;(\text{mod} \operatorname*{lcm}_{1\leq i\leq n-1}(a_i))$, where $a_1,\dots$ $\dots,a_n$ are the coefficients of L. Then already the choice d=1 satisfies the requirements (***) from the proof of Proposition 13.

Remark

Using the definition (b) from the proof of Proposition 13, explicit expressions may be found for the parameters of degre 1 in V(L,g), in the case of a standard pair $(L=\sum_{i=1}^{n} a_i Y_i, g)$. An easy computation shows that such a system of parameters is for instance, the following:

(12) $\xi_1=(g/a_1,0,\ldots,0)$, $\xi_2=(0,g/a_2,0,\ldots,0),\ldots\ldots$

$\ldots\ldots,\xi_n=(0,0,\ldots,0,g/a_n)$,

where the coordinates are taken in the canonical basis of $\mathbb{Z}^n$.

The next step in the study of the Veronese monoids, is the characterization of their defining relations. This cannot be done here in full generality, but we shall derive some useful information at least for the standard case.

To this end, we make some introductory considerations on quadratic monoidal relations, restricting ourselves to submonoids of free abelian monoids, in order to avoid unnecessary generalities. So, let $n\geq 1$ be an integer and let $F\subseteq\mathbb{Z}_+^n$ be a finite non-empty subset.

For any $m\geq 2$ and any sequence $f=(f_1,\ldots,f_m)$ over F, an "elementary quadratic transform" of f is a sequence $f'=(f'_1,\ldots,f'_m)$ (of precisely the same lenght) over F, defined by:

($\exists$) $i,k\in\{1,2,\ldots,m\}$, $i\neq k$ such that $f_i+f_k=f'_i+f'_k$ and $f_j=f'_j$ for $j\in\{1,2,\ldots,m\}\setminus\{i,k\}$.

We write this kind of connection between f and f' as: $f\sim f'$, since it is obviously reflexive and symmetrical. The transitive closure of this relation is therefore an equivalence, which we use in the sequel.

The finite set F is called "quadratic" if the following holds:

(13) for any $m\geq 2$ and any two sequences $f=(f_1,\ldots,f_m)$ and $h=(h_1,\ldots,h_m)$ over F, such that $\sum_{i=1}^m f_i=\sum_{i=1}^m h_i$, there is a family of $t\geq 2$ sequences $f^{(\alpha)}=(f_1^{(\alpha)},\ldots,f_m^{(\alpha)})$, $\alpha=1,2,\ldots,t$ over F, such that: $f=f^{(1)}\sim f^{(2)}\sim\ldots\sim f^{(t)}=h$.

15. Proposition

In the above setting, the following are equivalent:

(i) $F \subseteq \mathbb{Z}_+^n$ is a quadratic set

(ii) for any $m \geq 2$, any sequence $f=(f_1,\dots,f_m)$ over F and any element $x \in F$, which appears in some decomposition with m terms of $\sum_{j=1}^m f_j$ over F, there are $t \geq 1$ sequences: $(f^{(\alpha)})_{1 \leq \alpha \leq t}$ of m elements over F, with the property: $f=f^{(1)} \sim f^{(2)} \sim \dots \sim f^{(t)}$ and $x=f_k^{(t)}$ for some $k \in \{1,\dots,m\}$.

Proof

(i) $\Rightarrow$ (ii) is obvious by (13) and (ii) $\Rightarrow$ (i) follows by induction on m, using the cancellation property of $\mathbb{Z}_+^n$.

16. Proposition

Let $n_1, n_2 \geq 1$ be integers and $F_1 \subseteq \mathbb{Z}_+^{n_1}$; $F_2 \subseteq \mathbb{Z}_+^{n_2}$ be finite, non-empty quadratic subsets. Then $F_1 \times F_2$ is a quadratic subset in $\mathbb{Z}_+^{n_1+n_2}$.

Proof.

The assertion immediately follows from Proposition 15, whose condition (ii) is consistent with cartesian products, since the monoid law on $\mathbb{Z}_+^{n_1} \times \mathbb{Z}_+^{n_2}$ is the direct product of the monoi laws on the factors and the elementary quadratic transforms may be performed on each factor separately.

17. Proposition

For any integer $k \geq 1$, the interval $[0,k] = \{0,1,\dots,k\}$ is a quadratic subset of $\mathbb{Z}_+$.

Proof

Let $m \geq 2$ be any integer and $(i_1,\dots,i_m)$ a sequence with m terms from $[0,k]$. Any $x\in[0,k]$ appearing in some decomposition with m terms of $\Sigma_{=1}^{m} i$, should be reacked through a finite number of elementary quadratic transforms over $[0,k]$, starting from $(i)=(i_1,\dots,i_m)$. In order to prove this, we first remark that any transposition on $(i_1,\dots,i_m)$ certainly gives an elementary quadratic transform of this sequence, thus we may from the very beginning suppose that $k\geq i_1\geq i_2\geq\dots\geq i_m\geq 0$. We now look at the position of $x\in[0,k]$ with respect to (i), distinguishing three possible cases.

I) $k\geq x\geq i_1\geq i_2\geq\dots\geq i_m\geq 0$.

If $i_1+i_2\geq x$, then $(i_1,i_2,i_3,\dots,i_m)\sim(x,\ i_1+i_2-x,\ i_3,\dots,i_m)$ is enough, because $0\leq x\leq k$ and $0\leq i_1+i_2-x\leq i_2\leq k$.

If $i_1+i_2+i_3\geq x\geq i_1+i_2$, then the following two steps are enough: $(i_1,i_2,i_3,i_4,\dots,i_m)\sim(i_1+i_2,0,i_3,i_4,\dots,i_m)\sim(x,0,i_1+i_2+i_3-x,i_4,\dots,i_m)$, because $0\leq x\leq k$ and $0\leq i_1+i_2+i_3-x\leq i_3\leq k$.

If $i_1+i_2+i_3+i_4\geq x\geq i_1+i_2+i_3$, then the following three steps are enough:

$$(i_1,i_2,i_3,i_4,i_5,\dots,i_m)\sim(i_1+i_2,0,i_3,i_4,i_5,\dots,i_m)\sim(i_1+i_2+i_3,0,0,i_4,i_5,\dots,i_m)\sim(x,0,0,i_1+i_2+i_3+i_4-x,\ i_5,\dots,i_m).$$

We continue like this, the procedure eventually giving the desired conclusion, because $i_1+i_2+\dots+i_m\geq x$ by hypothesis.

II) $k\geq i_1\geq i_2\geq\dots\geq i_\alpha\geq x\geq i_{\alpha+1}\geq\dots\geq i_m$, for some $\alpha\in\{1,2,\dots,m-1\}$.

Then a single elementary quadratic transform is enough, namely:

$$(i_1,\dots,i_\alpha,i_{\alpha+1},\dots,i_m)\sim(i_1,\dots,x,\ i_\alpha+i_{\alpha+1}-x,\dots,i_m),$$

because $0\leq x\leq k$ and $0\leq i_\alpha+i_{\alpha+1}-x\leq i_\alpha\leq k$.

III) $k\geq i_1\geq\ldots\geq i_m\geq x\geq 0$

Here also a single elementary transform is enough, namely:

$$(i_1,\ldots,i_{m-1},i_m)\sim(i_1,\ldots,\ ,\ i_{m-1}+i_m-x),$$

because $0\leq x\leq k$ and $0\leq i_{m-1}+i_m-x\leq i_{m-1}\leq k$.

This ends the proof of the Proposition.

Remark

Proposition 17 is also true in the trivial case k=0.

We remind, now, that a "principal order ideal" in a poset $(P,\leq)$ is a subposet of the type $O(x)=\{y\in P/y\leq x\}$, for $x\in P$ (called "the generator" of $O(x)$).

A "finitely generated" order ideal $O(x_1,\ldots,x_n)$ in P, is the union of the principal order ideals $O(x_1),\ldots,O(x_n)$, $n\geq 1$.

18. Proposition

For any $n\geq 1$, a principal order ideal in $(\mathbb{Z}_+^n,\leq)$ is a quadrati subset.

(the order on $\mathbb{Z}_+^n$ being the monoidal one).

Proof

Let $O(x)$ be the order ideal generated by $x=(x_1,\ldots,x_n)\in\mathbb{Z}_+^n$.

Then $O(x)$ is the parallelotope $[0,x_1]\times[0,x_2]\times\ldots\times[0,x_n]\subseteq\mathbb{Z}_+^n$ such that the assertion follows from the Proposition 16 and 17.

The next natural step would be the checking of the quadratic property for finitely generated order ideals in $\mathbb{Z}_+^n$. However, it is not true that they are all quadratic for $n\geq 2$, unless i

19. Proposition

Let $F \subseteq \mathbb{Z}_+^n$ be a (finitely generated) order ideal, having the following property:

(D) for any integer $m \geq 2$ and for any $d \in mF$ and $\alpha, \beta \in F$, satisfying: $d+\alpha \in mF$ and $d+\beta \in mF$, there are elements $d' \in (m-1)F$ and $\alpha', \beta' \in F$ such that: $d'+\alpha' = d+\alpha$ and $d'+\beta' = d+\beta$.

Then F is a quadratic set.

(Here $mF = F+\ldots+F$ (m times) in $\mathbb{Z}_+^n$).

Proof

We shall proceed by induction on the number of terms in decompositions over F, using (ii) of Proposition 15, the case m=2 being trivial.

So, let $(a_1,\ldots,a_m)$ and $(b_1,\ldots,b_m)$ be two m-terms families over F, where $m \geq 2$, such that:

$$(*) \qquad a_1+a_2+\ldots+a_m = b_1+b_2+\ldots+b_m \qquad (\text{in } \mathbb{Z}_+^n)$$

We must show that $(a_1,\ldots,a_m)$ and $(b_1,\ldots,b_m)$ are then quadratically connected, if (D) takes place and if this is true for any $m' < m$. From $(*)$, we obtain an element:

$$r = -b_1+a_2+\ldots+a_m = -a_1+b_2+\ldots+b_m \in \mathbb{Z}^n.$$

Let: $d = \sup(r,0)$, "sup" being the usual lattice operation in $\mathbb{Z}^n$. Then : $d \in \mathbb{Z}_+^n$, $d \leq a_2+\ldots+a_n$, $d \leq b_2+\ldots+b_n$, so there are elements $\alpha, \beta \in \mathbb{Z}_+^n$, such that:

$$(\#1) \qquad d+\alpha = a_2+\ldots+a_n, \quad d+\beta = b_2+\ldots+b_n.$$

Then, the definition of r gives:

$$(\#2) \qquad d+\alpha = r+b_1 \; ; \quad d+\beta = r+a_1,$$

But F is an order ideal and $a_1,b_1\in F$, so $\alpha,\beta\in F$.

Now, from the Decompostion Theorem in latticially ordered abelian groups (cf.Bourbaki, [4]- see also the proof of Prop.7, §2), from $d\leq a_2+\dots+a_m$ and $d,a_2,\dots,a_m\in\mathbb{Z}^n_+$, it follows the existence of positive elements $a'_2,\dots,a'_m\in\mathbb{Z}^n_+$, such that $d=a'_2+\dots+a'_m$ and $a'_j\leq a_j$ in $\mathbb{Z}^n_+$, for $j=2,\dots,m$. Since F is an order-ideal and $a_2,\dots,a_m\in F$, we derive from here that: $d\in(m-1)$ (with $m-1\geq 2$, because $m>2$).

Then (#2) shows that d,α,β satisfy the hypothesis of (D) in the enounce, so there are elements $d'\in(m-2)F$ and $\alpha',\beta'\in F$ and $d+\alpha=d'+\alpha'$, $d+\beta=d'+\beta'$.

From (*) and (#1) we deduce:

(3) $\alpha+a_1=\beta+b_1$ (in $\mathbb{Z}^n_+$),

and more:

$$d'+\alpha'=a_2+\dots+a_m \quad , \quad d'+\beta'=b_2+\dots+b_n.$$

By the choosing of d',α',β', these last equalities are (m-1) terms decompositions over F, therefore the induction hypothesis shows that there are (finitely many) elementary quadratic transforms, connecting $(a_2,\dots,a_m)$ to (α',d') and $(b_2,\dots,b_m)$ to (β',d'). Then, by finitely many elementary quadratic transforms, we may connect $(a_1,a_2,\dots,a_m)$ to (a_1,α',d') and $(b_1,b_2,\dots,b_m)$ to (b_1,α',d'). But then $a_1+\alpha'+d'=b_1+\alpha'+d'$ in $\mathbb{Z}^n_+$, and (3) shows that a single more elementary quadratic transform connects (a_1,α',d') to (b_1,α',d').

Therefore, starting from $(a_1,\dots,a_m)$, we can perform (finitely may) elementary quadratic transforms on this sequence, obtaining $(b_1,\dots,b_m)$.

This ends the proof of the Proposition.

Remark

The whole monoid $\mathbb{Z}_+^n$ $(n\geq 1)$ is a quadratic set, as the Decomposition Theorem immediately shows.

Indeed, if $(a_1,\ldots,a_m)$, $(b_1,\ldots,b_m)$ are families over $\mathbb{Z}_+^n$ $(m\geq 2)$ and $a_1+\ldots+a_m=b_1+\ldots+b_m$, then the Decomposition Theorem gives a double family: $(z_{ij})_{1\leq i\leq m,\ 1\leq j\leq m}$ of elements from $\mathbb{Z}_+^n$, such that: $a_i=\sum_{j=1}^m z_{ij}$ for every i and $b_j=\sum_{i=1}^m z_{ij}$ for every j.

Then $(a_1,\ldots,a_m)$ may be quadratically connected to $(b_1,\ldots,b_m)$ by simply interchanging z_{ij} with z_{jk} in an elementary quadratic transform and thus succesively recapturing $b_1,b_2,\ldots,b_m$ from $a_1,a_2,\ldots,a_m$.

Such transfer may be performed step by step, because no restriction is put on the a_i's or b_j's (the Decomposition Theorem simply saying that every relation: $a_1+\ldots+a_m=b_1+\ldots+b_m$ may be obtained by rearranging the terms in convenient decompositions of $(a_i)_i$ and $(b_j)_j$). This is equivalent, of course, to the factoriality of the monoid algebra $\mathbb{C}[\mathbb{Z}_+^n]=\mathbb{C}[X_1,\ldots,X_n]$.

A similar Decomposition Theorem is not valid, however, over an arbitrary order ideal $F\subseteq\mathbb{Z}_+^n$, so convenient restrictions (as, for instance (D) of Prop.19) have to be put on F in order to assure at least its quadratic feature.

Now, we return to Veronese monoids and consider a (basic) linear form $L=a_1Y_1+\ldots+a_pY_p$, $p\geq 1$, which defines, together with any L-degree $g\in\langle L\rangle$, and order ideal, namely:

$$(14)\qquad \mathcal{O}(L,g)=\{\lambda\in\mathbb{Z}_+^p/L(\lambda)\leq g\}.$$

As we have seen before, for any integer $m\geq 1$:

$$(15)\qquad mO(L,g)\subseteq O(L,mg)\ \ (\text{with } mO(L,g)=\textstyle\sum_1^m O(L,g) \text{ in } \mathbb{Z}_+^n),$$

the equality (for all m) being assured if (L,g) is a standar pair.

20. Proposition

Let $L=\sum_{j=1}^{p} a_j Y_j$ be a form in $p\geq 1$ variables, such that $\langle L\rangle$ has no gaps in $\mathbb{Z}_+$ (equivalently, $a_j=1$ for some $j\in\{1,\ldots,p\}$). Then $O(L,g)$ is a quadratic set in $\mathbb{Z}_+^p$, for any $g\in\mathbb{Z}_+$.

Proof.

We have only to check condition (D) of Proposition 19, since $O(L,g)$ is an order ideal already.

Let $m\geq 2$ be an integer, $d\in mO(L,g)$, $\alpha,\beta\in O(L,g)$ such that: $d+\alpha\in mO(L,g)$, $d+\beta\in mO(L,g)$.

We search for elements $d'\in(m-1)O(L,g)$, $\alpha',\beta'\in O(L,g)$ verifyin $d'+\alpha'=d+\alpha$, $d'+\beta'=d+\beta$.

Then $d'\leq d+\alpha$ and $d'\leq d+\beta$ in $\mathbb{Z}_+^n$, so $d'\leq \inf(d+\alpha,\ d+\beta)=$ $=d+\inf(\alpha,\beta)$ (where "inf" is the usual lattice operation on $\mathbb{Z}_+^n$). Therefore, we may write: $d'=d-\xi+\inf(\alpha,\beta)$, where $\xi\geq 0$ is a convenient element from $\mathbb{Z}_+^n$.

Then $\alpha'=d-d'+\alpha=\xi+\alpha-\inf(\alpha,\beta)\geq 0$ and $\beta'=d-d'+\beta=\xi+\beta-\inf(\alpha,\beta)\geq 0$ are uniquely determined by the same ξ. Thus, we only have to find an element $\xi\geq 0$, such that:

(*1) $\quad d-\xi+\inf(\alpha,\beta)\in(m-1)O(L,g)$

(*2) $\quad \xi+\alpha-\inf(\alpha,\beta)\in O(L,g)$ and $\xi+\beta-\inf(\alpha,\beta)\in O(L,g)$,

and (D) will be fulfilled.

Thus, $O(L,g)$ verifies (D) iff for d,α,β as above, there is an element $\xi\geq 0$ satisfying (*1) and (*2).

According to (14) and (15), the conditions (*1) and (*2) lea to:

$$(\#) \qquad L(\xi)\in \left[L(d)-(m-1)g,\ g-\sup(L\ (\alpha),\ L(\beta))\right] + L(\inf(\alpha,\beta))$$

Now, $L(d)$ may be supposed not less than $(m-1)g$ (or else $d'=d$, $\alpha'=\alpha$ and $\beta'=\beta$ will be sufficient), so $L(d)-(m-1)g\geq 0$.

From $(\#)$ we see that ξ exists iff the intersection:

$$(I=\left[L(d)-(m-1)g,\ \ g-\sup(L(\alpha),L(\beta))\right])\cap\langle L\rangle$$

is non void, i.e. iff I is not entirely contained in the gap set of $\langle L\rangle$. Since $\langle L\rangle$ has no gaps, the proof is finished.

21.Proposition

Let L be a basic form in $n\geq 2$ variables and let $g\in\langle L\rangle$ be an L-degree,such that (L,g) is a standard pair.

Suppose further that $\langle L\rangle$ has no gaps in $\mathbb{Z}_+$.

Then the Veronese monoid $V(L,g)$ has quadratic defining relations.

Proof.

Indeed, suppose $a_1=1$, where $\{a_j| j=1,\ldots,n\}$ are the coefficients of L. We take the representation of $V_1(L,g)=F(L,g)$ as an homotethnical image of an order ideal in some $\mathbb{Z}_+^{n-1}$, with respect to another coefficient a_j, $j\neq 1$, of L (cf.Prop.6,§2). Since the quadratic nature of a finite set doesn't change by an homotothy, we may suppose that $V_1(L,g)=\theta(\xi)+\xi$, for some $\xi\in V_1(L,g)$, where $\theta(\xi)$ is an order ideal in $\mathbb{Z}_+^{n-1}$ (this free abelian monoid being identified to the set of all positive elements in some ordering of $G_o(L)\cong\mathbb{Z}^{n-1}$). Now, the definition (13) obviously resists to translations, therefore $V_1(L,g)$ is quadratic simultaneously with $\theta(\xi)$. But $\theta(\xi)$ is of the form (14) (cf.(6), §2) and more, it is in the conditions of Proposition 20, by our hypothesis and our choosing of ξ. Thus $\theta(\xi)$ is quadratic, implying the same for $V_1(L,g)$. But $V(L,g)$ is standard, so it defining relations are precisely those over $V_1(L,g)$.

22. Proposition

Let (L,g) be a standard pair, such that $\langle L\rangle$ has no gaps in $\mathbb{Z}$ Then the Veronese selection $V^{(s)}(L,g)$ has standard inner gradation and quadratic defining relations, for every integer $s\geq 1$.

Proof

The assertion about the inner gradation follows follows from the fact that $V^{(s)}(L,g)=V(L,sg)$ and (L,sg) is a standard pair if (L,g) is such.

The assertion about the defining relations follows from the remark that (using the notation (14)) $O(L,g)$ quadratic (and standard), implies the same for $s.O(L,g)=O(L,g)+...+O(L,g)$ (s times)$=O(L,sg)$, as the definition (13) readily shows.

Remarks

(i) In the above setting, let us remark that the property of $\langle L\rangle$ of not having gaps in $\mathbb{Z}_+$, already implies that L is a basic linear form.

By multiplication with an arbitrary positive integer, one immediately obtains a result similar to Proposition 22, namely:

" if $L=\sum_{j=1}^{n} a_jY_j$ has positive integral coefficients such that one of them divides every other one, then Proposition 22' remains valid for $V^{(s)}(L,g)$, with $g\equiv 0$ (mod $\mathop{\mathrm{lcm}}_{1\leq j\leq n}(a_j)$) and $s\geq 1$"

This is true because the quadratic property of a finite set is preserved by homotety (with a positive rational number) and the same holds for the standardness (cf. Prop.7).

(ii) As we have already observed (see the proof of Proposition 21), the quadratic property of a finite subset $F\subseteq\mathbb{Z}_+^n (n\geq 1)$ is not affected by translation (with a vector $\alpha\in\mathbb{Z}_+^n$) and by homotethy (with a positive integral (or rational) number). Thus F quadratic $\Rightarrow$ ${}^pF+\alpha$ quadratic, for $p>0$ in $\mathbb{Z}$ and $\alpha\in\mathbb{Z}_+^n$ (where ${}^pF=\{p\cdot\xi/\xi\in F\}$).

In particular, for n=1, it follows from Proposition 17 that the submonoid of $\mathbb{Z}_+$, *generated by any finite arithmetic progression*, has quadratic defining relations.

This particular case is "generic" in the sense that, in order to actually find the (defining) relations between the elements of a quadratic set $F\subseteq\mathbb{Z}_+^n (n\geq 1)$, one has to look for all arithmetic progressions inside F, but having their ratios in $\mathbb{Z}^n$.

4. Veronese monoid algebras

We consider the monoid algebras over $\mathbb{C}$ of the Veronese monoids defined at §3. The above terminology and notations are kept in what follows. So, let $L=\sum_{j=1}^n a_jY_j$ be a basic linear form in $n\geq 2$ variables and let $g\in\langle L\rangle$ be an L-degree.

We denote by $R(L,g)=\mathbb{C}[V(L,g)]$ the monoid algebra of V(L,g). From the definition of V(L,g) it follows that $R(L,g)\subseteq\mathbb{C}[\mathbb{Z}_+^n]=\mathbb{C}[X_1,\dots,X_n]$ and, as a $\mathbb{C}$-vector space, R(L,g) is spanned by the monomials $\{X^\xi/\xi\in V(L,g)\}$ (where $X^\xi=X_1^{\xi_1},\dots$ $\dots,X_n^{\xi_n}$, for $\xi=(\xi_1,\dots,\xi_n)$).

R(L,g) is graded by the inner gradation (7) of V(L,g), namely:

$$(16) \qquad R(L,g)=\bigoplus_{m\geq 0} R_m(L,g),$$

with $R_o(L,g)=\mathbb{C}$ and $R_m(L,g)=\bigoplus_{\xi\in V_m(L,g)}\mathbb{C}\cdot X^\xi$.

Putting toghether the informations derived above for Veronese monoids, we can formulate the following

23. Proposition

Let $V(L,g)\subseteq \mathbb{Z}_+^n$ be a Veronese monoid (L,g as above)

(i) $R(L,g)$ is a finitely generated $\mathbb{C}$- subalgebra of $\mathbb{C}[X_1,\ldots$ $\ldots\ldots,X_n]$, such that the ring extension $R(L,g)\subseteq \mathbb{C}[X_1,\ldots,X_n]$ is finite (hence $\dim R(L,g)=n$).

(ii) $R(L,g)$ is a Cohen-Macaulay ring

(iii) The gradation (16) on $R(L,g)$ is standard when (L,g) is a standard pair. If, moreover, $\langle L\rangle$ has no gaps in $\mathbb{Z}_+$, then $R(L,g)$ has quadratic defining relations.

(iv) If g is standard in some direction for L, then $R(L,g)$ has a system of parameters, consisting of monomials of the same L-degree. When the pair (L,g) itself is standard, then $R(L,g)$ has a monomial system of parameters of L-degree 1.

Proof

(i) comes from Prop. 8 and the remark that $X_j^g\in R(L,g)$, for ever $j\in\{1,2,\ldots\ldots,n\}$.

(ii) comes from the normality of the monoid embedding $R(L,g)$ $\mathbb{Z}_+^n$, together with Hochster's result [6]

(iii) is a mere translation of Proposition 12 and 21, while

(iv) results from Proposition 13 and its Corollary 14.

Remark

Interpreting $R(L,g)$ as a ring of invariants of a cyclic grou of order g acting on $\mathbb{C}[X_1,\ldots,X_n]$, the result of Watanabe (quoted at §1), shows that $R(L,g)$ is Gorenstein iff $\|L\| = \sum_{j=1}^n a_j\equiv 0$ (mod g), where $a_1,\ldots,a_n$ are the coefficients of L.

Important information about the singularity $R(L,g)$, is contained in a minimal resolution of $R(L,g)/_{R_+(L,g)}\cong\mathbb{C}$ ov $R(L,g)$ (where $R_+(L,g)=\bigoplus_{m>0} R_m(L,g)$).

$$(17)\quad \ldots \to S_p \xrightarrow{d_p} S_{p-1} \quad \ldots \quad S_1 \xrightarrow{d_1} S_o = R(L,g) \xrightarrow{\gamma} \mathbb{C} \to 0$$

be such a resolution (γ being the canonical homomorphism), where every S_p is a finitely generated, free $R(L,g)$-module. The gradation (16) of $R(L,g)$ canonically gives a gradation on each term S_p $(p>0)$, such that a fixed basis of S_p consists of elements of degree zero in this extended gradation.
We grade in this manner the resolution (17), its minimality meaning: $d_p(S_p) \subseteq R_+(L,g)S_{p-1}$, for $p \geq 1$.
The integer: $b_p(L,g) = \mathrm{rk}_{R(L,g)} S_p$, $p \geq 0$, are called "the Betti numbers" of the singularity $R(L,g)$. They are equal to the coefficients of the "Poincaré of $R(L,g)$, defined by:

$$(18)\qquad P_{L,g}(z) = \sum_{p \geq 0} (\dim \mathrm{Tor}^p_{R(L,g)}(\mathbb{C},\mathbb{C}))z^p \in \mathbb{Z}[[z]] .$$

$P_{L,g}(z)$ contains the simplest ennumerative information about the singularity $R(L,g)$, with respect to the "internal" resolution (17) (here "internal" means that (17) unties $R(L,g)$ over itself, contrary to the "external" resolution of $R(L,g)$ over its minimal regular embedding, which compares $R(L,g)$ to a non-singularity; the "internal" resolution is infinite (except when $R(L,g)$ itself is regular), while the "external" one is always finite).
The ennumerative invariant $P_{L,g}(z)$ is computable in particular nice situations, when it can be algebraically connected to the usual Hilbert series of the gradation (16) on $R(L,g)$, namely:

$$(19)\qquad H_{L,g}(z) = \sum_{m \geq 0} (\dim R_m(L,g))z^m \in \mathbb{Z}[[z]].$$

Such a particular situation arises, for instance, when (17) is a linear resolution, i.e. when every differential d_p $(p \geq 1)$ is homogeneous (with respect to the inner gradation on every

S_p) of degree +1.

This comes to the fact that R(L,g) is a "Fröberg ring", i.e. its ennumerative invariants $H_{L,g}(z)$ and $P_{L,g}(z)$ are connected by the relation:

$$(20) \qquad P_{L,g}(z)H_{L,g}(-z)=1.$$

We shall check this property on the graded structures studie here and to this end we first remind the general behaviour of the Poincaré and Hilbert series after factoring out regular sequences in graded noetherian algebras over $\mathbb{C}$ (or any field).

Lemmȧ

Let $A=\bigoplus_{m\geq 0}A_m$ be a noetherian graded algebra over $\mathbb{C}=A_0$, wit irrelevant maximal ideal $A_+=\bigoplus_{m\geq 0}A_m$ and let $x\in A_+$ be a homoge neous non-zero divizor, of degre $d\geq 1$.

Then:

(i) $H_{A/XA}(z)=(1-z^d)H_A(z)$

(ii) $P_{A/XA}(z)=(1+z)^{-1}P_A(z)$ when d=1 and $P_{A/XA}(z)=(1-z^2)^{-1}P_A($ when d 1.

(The proof of (i) is immediate, while (ii) (essentially due to Tate) may be found in: T.H.Gulliksen & G.Levin, Homology of Local Rings, Queen's Papers in P. and Appl.Math., No.20 (19 for instance).

In particular, the following result may be derived from here

24. Proposition

Let A be as in the enounce of the above Lemma and let $\{X_1,X_2,\ldots,X_n\}$ be a regular sequence in A, such that every X is homogeneous, of degree 1.

The following are equivalent:

(i) $P_A(z).H_A(-z)=1$

(ii) $P_{A/(X_1,\dots,X_n)A}.H_{A/(X_1,\dots,X_n)A}(-z)=1.$

Proof

Indeed, from the above Lemma, if follows that $P_{A/(X_1,\dots,X_n)A}(z)$ $=(1+z)^{-n}P_A(z)$ and $H_{A/(X_1,\dots,X_n)A}(z)=(1-z)^nH_A(z)$.

This proposition says, in particular, that for a Cohen-Macaulay graded algebra A, with dim A=n, the checking of the Fröberg property (20) for A comes to the checking of the same for the artinian graded algebra $A/(X_1,\dots,X_n)A$, $\{X_1,\dots,X_n\}$ being a maximal regular sequence, consisting of homogeneous elements of degree 1.

Now, coming back to our particular situation, we prove the following result about certain Veronese monoid algebras.

25. Proposition

Let L be a basic linear from in $n\geq 2$ variables and let $g\in\langle L\rangle$ be an L-degree, such that the pair (L,g) is standard and L has no gaps in $\mathbb{Z}_+$.

Then the Veronese monoid algebra R(L,g) is a Fröberg ring (i.e. (20) takes place).

Proof

Using Proposition 23, we select a particular system of parameters of degree one in R(L,g), namely the one given by (12), §3:

$p_1=X$,...,$p_n=X$, $\pi_j=g/a_j(\delta_{ji})_{1\le i\le n}$,

$a_1,\dots,a_n$ being the coefficients of L.

Factoring-out R(L,g) by this system of parameters (which is a regular sequence), we obtain an artinian graded algebra:

$$A(L,g)=R(L,g)/(p_1,\dots,p_n)R(L,g).$$

In virtue of Prop.24, we only have to check the Fröberg property for this artinian ring.

Because R(L,g) is standard (in its inner gradation (16)), the same is true for A(L,g). R(L,g) has quadratic defining relations (cf. (iii), Prop.23), so the defining relations of A(L,g) will split into the following two classes:

(I) monomial relations of the kind: $X^{\xi}X^{\eta}$, where $\xi,\eta\in V_1(L,g)$ and $\xi+\eta\ge\pi_j$ in $\mathbb{Z}_+^n$, for some $j\in\{1,2,\dots,n\}$

(II) binomial quadratic relations of the kind: $X^{\xi}X^{\eta}-X^{\xi'}X^{\eta'}$ where $\xi,\xi',\eta,\eta'\in V_1(L,g)$ and $\xi+\eta=\xi'+\eta'$ in $\mathbb{Z}_+^n$, but $\xi+\eta$ is not greater than any of $\pi_1,\dots,\pi_n$, in the monoidal order relation on $\mathbb{Z}_+^n$.

Let $U=\{(\xi,\eta)/\xi,\eta\in V_1(L,g)$ and give relations of type I$\}$ and $T=\{(\xi,\eta)/\xi,\eta\in V_1(L,g)$ and give relations of type II$\}$.

Then /U/T/ is a partition of $V_1(L,g)\times V_1(L,g)$ and each block U,T is symmetric about the diagonal of this cartesian product. Moreover, this partition of the defining relations for A(L,g) satisfies the following property:

(*) there is an element $(\xi,\eta)\in U$ such that $T\cap(V_1(L,g)\times\{\xi\})\neq\emptyset$ and $T\cap(V_1(L,g)\times\{\eta\})\neq\emptyset$.

To see this, we choose, for instance:

$$\xi=(i,0,0,\dots,0),\ \eta=(j,0,0,\dots,0),$$

where $i,j\in\{1,2,\dots$

then we choose $\xi'=(0,i_2,\ldots,i_n)$, $\eta'=(0,j_2,\ldots,j_p)$, with $i_k<g/a_k$, $j_k<g/a_k$ for $k=2,3,\ldots,n$ (such that $(\xi',\xi)\in T$ and $(\eta',\eta)\in T$). Such elements always exist, by our conditions on L.

Now, this presentation of $A(L,g)$ is enough to assure its Fröberg property, according to a result of Kobayashi (cf. [7]). This ends the proof of the Proposition.

The linearity of the (internal) resolution (17) of $R(L,g)$, asserted by Proposition 25 (under the circumstances that (L,g) is a standard pair and $\langle L\rangle$ has no gaps in $\mathbb{Z}_+$) allows one to explicitly compute the free bases of the components $(S_p)_{p\geq 1}$ in (17).

Using the notations introduced above, we simply indicate the result of such computations (for a monoid algebra $R(L,g)$ which satisfies the requirements of Proposition 25), in the following list:

(21.1) S_1 has free basis $(E_\xi)_{\xi\in V_1(L,g)}$, consisting of elements of degree zero in the inner gradation

(21.2) S_2 has free basis $\left\{[\xi,\xi']^*/\xi,\xi'\ V_1(L,g)xV_1(L,g)\right\}$, where $[\xi,\xi']^*$ is the "perturbated" determinantal linear expression:

$$[\xi,\xi']^*=X^\lambda(X^\xi E_{\xi'}-X^{\xi'}E_\xi),$$

with $\lambda\in G_o(L,g)$ and $\lambda+\xi\geq 0$ in $\mathbb{Z}_+^n$, $\lambda+\xi'\geq 0$ in $\mathbb{Z}_+^n$ (hence X^λ belongs to the fractions field of $R(L,g)$, but $X^{\lambda+\xi}$, $X^{\lambda+\xi'}$ actually belong to $R(L,g)$.

The basis of S_2 consistis of all such "perturbed" determinants which are linearly independent over $\mathbb{C}$ in the first degree component of S_1.

(21.3) S_3 has free basis consisting of all $\mathbb{C}$- linearly independent (in the first degree component of S_2) "perturbed" determinants of the kind:

$[\xi,\xi',\xi'']^*$, where $(\xi,\xi',\xi'')\in V_1(L,g)xV_1(L,g)xV_1(L,g)$ and $[\xi,\xi',\xi'']^* = X^{\lambda_1}[\xi,\xi']^* + X^{\lambda_2}[\xi',\xi'']^* + X^{\lambda_3}[\xi'',\xi]^*$, for $\lambda_1,\lambda_2,\lambda_3\in G_o(L,g)$ such that, if λ perturbas ξ,ξ' to give $[\xi,\xi']^*$, then $\lambda_1+\lambda+\xi\geq 0$ and $\lambda_1+\lambda+\xi'\geq 0$ in $\mathbb{Z}_+^n$, and so on.

....

(21.m) S_m has free basis consisting of all $\mathbb{C}$-linearly independent (in the first degree component of S_{m-1}) "perturbed" determinants of the kind:

$$[\xi_1,\dots,\xi_m]^*=X^{\lambda_1}[\xi_2,\dots,\xi_m]^*+X^{\lambda_2}[\xi_1,\xi_3,\dots,\xi_m]^*+\dots\dots+X^{\lambda_m}[\xi_1,\dots,\xi_{m-1}]^*,$$

where $\lambda_1,\dots,\lambda_m\in G_o(L,g)$ are allowable perturbations of the determinants $[\xi_1,\dots,\hat{\xi}_j,\dots,\xi_m]^*$, $j=1,2,\dots,m$, respectively.

<u>Remark</u>

Roughly speaking, a "perturbed" determinant $[\xi_1,\dots,\xi_m]^*$ (m≥2 is obtained as follows: one takes infinitely many copies of the variables $\{Y_\xi/\xi\in V_1(L,g)\}$, namely $\{Y_\xi^{(m)}/\xi\in V_1(L,g),m\geq 1\}$ completing them with $Y_\xi^{(0)}=X^\xi$ for $\xi\in V_1(L,g)$.
These (infinitely many) new variables lay inside the polynomial ring $R(L,g)[Y_\xi^{(m)}]_{\xi\in(V_1(L,g),\ m\geq 1}$, where we define:

$$[\xi_1,\dots,\xi_m]^*=\det(Y_{\xi_{ik}}^{(k)})_{1\leq i,k\leq m},$$

where $\xi_{1k}=\xi_k$ for $k=1,2,\dots,m$ and $\{\xi_{ik}/i\geq 2,\ 1\leq k\leq m$ are so chosen, that each two-by-two minor $\det\begin{bmatrix} X_{\xi_{ik}} & X_{\xi_{jk}} \\ X_{\xi_{ik'}} & X_{\xi_{jk'}} \end{bmatrix}$, be zero in R(L,g)

because the first line $(\xi_1,\ldots,\xi_m)$ is not uniquely extendible (by quadratic connections) to a determinant like the one above. We gave it only in order to keep track of the procedure and the underline its "monoidal" antisymmetric nature.
The differential $d_m : S_m \longrightarrow S_{m-1}$ acts on such determinants by simply lowering by one the upper index of each variable $Y^{(m)}_{\xi_{ij}}$, replacing $Y^{(0)}_{\xi_{ij}}$ by $X^{\xi_{ij}}$ wherever it is the case, then developping the resulting determinant by the minors of its first line.

The connection between $P_{L,g}(z)$ and $H_{L,g}(z)$, in case $R(L,g)$ is a Fröberg ring, becomes efficient only if $H_{L,g}(z)$ may be explicitely computed (or, at least, conveniently characterized). For the very simple case of trivial basic forms (i.e. the ones having all coefficients equal to 1), this was done in [3] and [1]. In general, the Cohen-Macaulayness of $R(L,g)$ allows us to describe $H_{L,g}(z)$ as a rational function of the type:

$$(22) \qquad H_{L,g}(z) = \frac{Q_{L,g}(z)}{\prod_{j=1}^{n}(1-z^{d_j})} ,$$

where $d_1,\ldots,d_n$ are the degrees of the elements in a homogeneous system of parameters for $R(L,g)$ and $Q_{L,g}(z)$ is a polynomial with positive integral coefficients (cf.[2]).
Of course, by (iv) of Proposition 25, we may take $d_1=\ldots=d_n=1$ in case (L,g) is a standard pair, or $d_1=\ldots=d_n=d\geq 1$ if g is at least standard in some direction for L.
The polynomial $Q_{L,g}(z)$ in the numerator of $H_{L,g}(z)$ is nothing else than the Hilbert series of the resulting artinian graded algebra, after dividing-out $R(L,g)$ by the corresponding homogeneous system of parameters.
This is why $Q_{L,g}(z)$ (hence $H_{L,g}(z)$) may be explicitely computed only after carefully choosing homogeneous systems of pa-

rameters in each particular case separatedly (cf. [1]). Starting from very general ennumerative principles, we can d ve another expression for $H_{L,g}(z)$. Namely, let $a_1, a_2, \dots, a_n$ be the coefficients of the form L, which is not necessarily basic, now. Then, since $H_{L,g}(z) = \sum_{m\geq 1} \#(V_m(L,g))\, z^m$, directly from the de finition (7), §2 , of the inner gradation on V(L,g), it follows that:

$\# V_m(L,g)$=the coefficient of z^{mg} in the power series

$$\sum_{\xi \in \mathbb{Z}^n_+} z^{L(\xi)} = \sum_{(\xi_1,\dots,\xi_n)} z^{a_1\xi_1+\dots+a_n\xi_n}$$

However, it is clear that:

$$\sum_{(\xi_1,\dots,\xi_n)} z^{a_1\xi_1+\dots+a_n\xi_n} = \prod_{1\leq j\leq n} (1-z^{a_j})^{-1}$$

In order to select here the powers of z, which are multiples of g, we only have to average about the cyclic group of orde g, this last expression. This yields the following form of $H_{L,g}$:

$$H_{L,g}(z) = g^{-1} \sum_{j=0}^{g-1} \prod_{k=1}^{n} (1-\zeta^{ja_k} z^{a_k/g})^{-1}, \tag{23}$$

where ζ is a primitive root of order g of 1.

Remarks

(i) Of course, (23) is not easy to handle even for small values of g. However, (22) and (23) may lead together to valuable numerical conclusions, in some particular cases.

(ii) (23) is reminiscent of Molien's formula for the Hilbert series of rings of invariants of finite groups acting on poly

Molien's formula itself, is but a very particular case of the general ennumeration principle known to combinatorists under the name of "Mac Mahon's Master Theorem".

5. Conclusions

Let G be a cyclic group of order $g>0$, indentified to the group of all g-roots of 1 in $\mathbb{C}^*$, i.e. $G=\{\zeta^k/k=0,1,\ldots,g-1\}$, ζ being a primitive such root.

For any $n\geq 2$, we put G to diagonally act on $\mathbb{C}[X_1,\ldots,X_n]$, by $(\zeta,X^\xi)\mapsto \zeta^{L(\xi)}X^\xi$, for $\xi\in\mathbb{Z}_+^n$, $L=\sum_{j=1}^n a_jY_j$ being a linear form with positive integral coefficients (not necessarily basic).

As we have remarked at § 1 (Proposition 1), the invariant algebra of G on $\mathbb{C}[X_1,\ldots,X_n]$, is a monoid algebra, namely the Veronese one R(L,g) (cf. § 4).

We are now going to translate our previous results into invariant-theoretic terms, using the following terminology. When the form L (giving the action of G) has equal coefficients, i.e. $a_1=a_2=\ldots=a_n=p\in\{1,2,\ldots,g-1\}$, we say that "G homogeneously acts on $\mathbb{C}[X_1,\ldots,X_n]$".

Remark

Would it be true that any diagonal action of G on $\mathbb{C}[X_1,\ldots$ $\ldots,X_n]$ is a Segre product of homogeneous ones, then our next result (Thm.1) would be immediately proved by means of general results of Fröberg and Backelin, together with [3]. Although we did not check this, the above presented method has some advantages by itself.

The invariant algebra R(L,g) of an homogeneous action $L=p(Y_1+\ldots+Y_n)$ of G on $\mathbb{C}[X_1,\ldots,X_n]$, is isomorphic to the invariant algebra R(L′,g′) of the homogeneous action $L'=Y_1+\ldots+Y_n$ of the cyclic group G′ of order g/gcd(p,g) on

$\mathbb{C}\left[X_1,\ldots,X_n\right]$.

However, such algebraic singularities are known to be Fröber by [3]. Therefore, the initial R(L,g) is Fröberg, by the remark that any Veronese selection into a graded algebra over a field, preserves the Fröberg property (cf. I. Backelin, R.F berg, Reports of the Univ. Stockholm, 2(1983)).

Adding this remark to Proposition 27 of § 4, we may formulat our main result, namely:

1. Theorem

Let G be a cyclic group of order $g>1$, diagonally acting on $\mathbb{C}\left[X_1,\ldots,X_n\right]$ by means of a linear form $L=a_1Y_1+\ldots+a_nY_n$, (wit positive integral coefficients).

Let R(L,g) be the invariant algebra of this action, canonically graded by L (if. (16), § 4).

Suppose further that one of the following holds:

(A) the action L is homogeneous, of some degree $p\in\{1,2,\ldots\ldots,g-1\}$

(B) the pair (L,g) is standard and $\langle L\rangle$ has no gaps in $\mathbb{Z}_+$

Then the algebraic singularity R(L,g) is a Fröberg ring.

We remark that a non-standard pair (L,g) seems not to yield a Fröberg singularity R(L,g), since it has not quadratic defining relations.

It also seems (as particular cases show) that the condition on $\langle L\rangle$ of not having gaps, may be retired form (B) without changing the conclusion of Theorem 1.

March, 11, 1985

Bibliography

[1] Ș.Bărcănescu, Preprint Series in Math., INCREST, 67(1981

[2] Ș.Bărcănescu, Rev.Roumanie Math.P. et Appl., 9(1982), 919-926.

Appl., 4(1981), 549-565.

[4] N.Bourbaki, Algèbre, ch.VI, Hermann, Paris (1965).

[5] I.Herzog, Manuscripta Math., 3(1975), 175-193.

[6] M.Hochster, Annals of Math., 96(1972), 318-337.

[7] Y.Kobayashi, Math.Scand., 42(1978), 19-33.