ANNALES

DE

L'INSTITUT FOURIER

David RYDH

A minimal Set of Generators for the Ring of multisymmetric Functions

Tome 57, nº 6 (2007), p. 1741-1769.

<http://aif.cedram.org/item?id=AIF_2007__57_6_1741_0>

Ann. Inst. Fourier, Grenoble
57, 6 (2007) 1741-1769

A MINIMAL SET OF GENERATORS FOR THE RING OF MULTISYMMETRIC FUNCTIONS

by David RYDH

Abstract. — The purpose of this article is to give, for any (commutative) ring A, an explicit minimal set of generators for the ring of multisymmetric functions $\mathrm{T}S^d_A(A[x_1,\dots,x_r]) = \bigl(A[x_1,\dots,x_r]^{\otimes_A d}\bigr)^{\mathfrak{S}_d}$ as an A-algebra. In characteristic zero, i.e. when A is a $\mathbb{Q}$-algebra, a minimal set of generators has been known since the 19^{th} century. A rather small generating set in the general case has also recently been given by Vaccarino but it is not minimal in general. We also give a sharp degree bound on the generators, improving the degree bound previously obtained by Fleischmann.

As $\Gamma^d_A(A[x_1,\dots,x_r]) = \mathrm{T}S^d_A(A[x_1,\dots,x_r])$ we also obtain generators for divided powers algebras: If B is a finitely generated A-algebra with a given surjection $A[x_1,x_2,\dots,x_r] \to B$ then using the corresponding surjection $\Gamma^d_A(A[x_1,\dots,x_r]) \to \Gamma^d_A(B)$ we get generators for $\Gamma^d_A(B)$.

Résumé. — Soit A un anneau commutatif arbitraire. Nous exhibons un ensemble minimal et explicite de générateurs de l'anneau des fonctions multisymétriques $\mathrm{T}S^d_A(A[x_1,\dots,x_r])$ et obtenons, par conséquent, une borne stricte sur le degré des générateurs. Dans le cas où la caractéristique de A est égale à zéro, un tel ensemble est connu depuis le $19^{\text{ème}}$ siècle. Dans le cas général par contre, il n'existait jusque-là qu'une borne, généralement non stricte, sur le degré des générateurs, et un ensemble, généralement non minimal, de générateurs.

1. Introduction

Let k be a field of characteristic zero. Explicit generators for the ring of multisymmetric functions $\bigl(k[x_1,\dots,x_r]^{\otimes_k d}\bigr)^{\mathfrak{S}_d}$ have been known since the nineteenth century, cf. [22, 10]. At the end of the same century nonconstructive methods began to appear, in particular Hilbert's basis theorem [8]. An easy consequence of this theorem is that if a finite group G

Keywords: Symmetric functions, generators, divided powers, vector invariants.
Math. classification: 13A50, 05E05, 14L30, 14C05.

acts linearly on a polynomial ring over a field k and $|G|$ is invertible in k, then the invariant ring is finitely generated, cf. [24, §57]. In particular, we may deduce that $\big(k[x_1,\dots,x_r]^{\otimes_k d}\big)^{\mathfrak{S}_d}$ is finitely generated without finding explicit generators.

The first result on the finiteness of the invariant ring of a group action in characteristic p was given by Noether [16]. Her argument is essentially the following: Let A be a noetherian ring and $G=\{g_1,g_2,\dots,g_m\}$ a finite group acting on $B=A[x_1,\dots,x_n]$. Let $C=A[e_{11},e_{12},\dots,e_{nm}]\subseteq B$ where e_{ij} is the j^{th} elementary symmetric function in $g_1(x_i),g_2(x_i),\dots,g_m(x_i)$. The A-algebra C is finitely generated and hence noetherian. As B is finite over C and $C\subseteq B^G\subseteq B$ it follows that B^G is finite over C and thus finitely generated as an A-algebra. In particular $\big(A[x_1,\dots,x_r]^{\otimes_A d}\big)^{\mathfrak{S}_d}$ is finitely generated for any noetherian ring A.

The abstract methods partly removed the need for explicit generators. However, interest in effective answers reappeared in the end of the twentieth century. One of the first results in this direction was given by Campbell, Hughes and Pollack [2] who showed that the ring of multisymmetric functions can be generated by elements of degree $\leqslant \max\big(d, rd(d-1)/2\big)$. In characteristic 0, the explicit generators have degree $\leqslant d$.

Some years later Fleischmann [5, Thm. 4.6] improved this degree bound to $\leqslant \max\big(d, r(d-1)\big)$ and also showed [5, Thm. 4.7] that this was the best possible if $A=\mathbb{F}_p$ and $d=p^s$, cf. Corollary 8.7. Vaccarino [23, Thm. 1] then used this result to give explicit generators, cf. Theorem 7.9. Fleischmann's degree bound is, however, not always sharp and the corresponding generating set is not minimal.

For any positive integer n and prime p we let

$$Q_p(n)(t)=a_st^s+a_{s-1}t^{s-1}+\dots+a_0\in\mathbb{N}[t]$$

where $a_sa_{s-1}\dots a_0$ is the representation of n in base p. We will prove the following theorem, cf. Theorem 7.19:

Theorem. — *Let A be any ring and $r,d\geqslant 1$ positive integers. The ring of multisymmetric functions $\big(A[x_1,\dots,x_r]^{\otimes_A d}\big)^{\mathfrak{S}_d}$ is* minimally *generated as an A-algebra by the elements*

$$e_k(x^\alpha)=(x^\alpha)^{\otimes k}\otimes 1^{\otimes d-k}+\dots+1^{\otimes d-k}\otimes(x^\alpha)^{\otimes k}$$

where e_k is the k^{th} elementary symmetric function on d variables and $(k,\alpha)\in\{1,2,\dots,d\}\times(\mathbb{N}^r\setminus 0)$ are such that $\gcd(\alpha)=1$ and either $k|\alpha|\leqslant d$ or there is a prime p, not invertible in A, such that

$$Q_p(k\alpha_1)+Q_p(k\alpha_2)+\dots+Q_p(k\alpha_r)\leqslant Q_p(d).$$

It is then easy to obtain the following sharp degree bound, cf. Corollary 8.8:

Corollary. — *Let A be any ring and $r, d \geqslant 1$ positive integers. For any prime p we let a_p and b_p be defined by $Q_p(d)(t) = a_p t^{b_p} + \dots$. The ring of multisymmetric functions is then generated by the elements of degree at most*

$$\max\left\{d, \max_p \big((a_p + r - 1)p^{b_p} - r\big)\right\}$$

where the maximum is taken over every prime p not invertible in A. Further, every generating set contains an element attaining this bound.

The ring of multisymmetric functions is usually described as the symmetric tensors of the polynomial ring in r variables

$$\mathrm{TS}^d_A(A[x_1, \dots, x_r]) := \big(A[x_1, \dots, x_r]^{\otimes_A d}\big)^{\mathfrak{S}_d}.$$

Another, functorially more well-behaved, description of the multisymmetric functions is given by the ring of divided powers $\Gamma^d_A(A[x_1, \dots, x_r])$ which is canonically isomorphic with the ring of multisymmetric functions. For any A-algebra B there is a canonical homomorphism $\Gamma^d_A(B) \to \mathrm{TS}^d_A(B)$ which is an isomorphism when A is of characteristic 0 or B is a free A-module but not in general [12]. If $B \to C$ is surjective then $\Gamma^d_A(B) \to \Gamma^d_A(C)$ is surjective but $\mathrm{TS}^d_A(B) \to \mathrm{TS}^d_A(C)$ need not be [12]. Thus, a set of generators for $\Gamma^d_A(A[x_1, \dots, x_r]) = \mathrm{TS}^d_A(A[x_1, \dots, x_r])$ will give a set of generators for $\Gamma^d_A(B)$ for any finitely generated A-algebra B but not for $\mathrm{TS}^d_A(B)$ in general. These issues are also discussed in [21].

From yet another slightly different viewpoint we can describe the multisymmetric functions as follows: Let V be a vector space over a field k and G a group acting linearly on V. Then G also acts on the dual space V^* and on the functions on V, i.e. the ring $k[V] = \mathrm{S}(V^*)$. The invariants of G are the invariant elements of $k[V]$, i.e. the subring $k[V]^G$. The set of *vector invariants* [25] of G is the invariant subring $k[V^r]^G \subseteq k[V^r]$ where G acts on $V^r = V \oplus V \oplus \dots \oplus V$ by $\sigma(v_1, v_2, \dots, v_r) = (\sigma v_1, \sigma v_2, \dots, \sigma v_r)$. The symmetric functions are the invariants of the symmetric group on d letters $\mathfrak{S}_d$ acting by permutations on $V = k^d$. The multisymmetric functions are the vector invariants of the same action.

Closely related to the question of generators of the ring of multisymmetric functions is the question of which relations these generators satisfy. In characteristic 0 the relations between the generators were thoroughly studied by Junker [9, 10, 11] in the nineteenth century. More recently, Vaccarino gave in [23, Thm. 2] relations for his set of generators mentioned above. In this article however, we will not discuss the relations that the generators satisfy.

We begin with some notation in §2 and a somewhat technical combinatorial result, Main Lemma 2.10, which will be used in the proof of the main theorem in the last section. We recall the definition of polynomial laws in §3, the algebra of divided powers $\Gamma_A(M)$ in §4, and the multiplicative structure of $\Gamma^d_A(B)$ in §5. In the rest of the article we will only consider $\Gamma^d_A(B)$ for B free over A and as mentioned above, in this case $\Gamma^d_A(B)$ coincides with the symmetric tensors $\mathrm{TS}^d_A(B)$, see 5.2. The reader, if inclined so, may replace $\Gamma^d_A(B)$ with $\mathrm{TS}^d_A(B)$, $\gamma^k_A(x)$ with $x^{\otimes_A k}$, interpret × as the shuffle product and forget about divided powers altogether. The important results of §§4-5 used in the sequel are Formula 5.3 describing the multiplication in $\Gamma^d_A(B)$ and the surjective homomorphism $\rho^e_d : \Gamma^e_A(B) \twoheadrightarrow \Gamma^d_A(B)$ for $e \geqslant d$ defined in paragraph 5.5. The homomorphism ρ^e_d allows us to lift relations in $\Gamma^d_A(B)$ to relations in $\Gamma^e_A(B)$ which will be useful in §7. We also use the convenient shorthand notation $\mathbf{1}^k$ for $\gamma^k_A(1)$ or $1^{\otimes_A k}$.

In §6 we establish some notation and well known facts about the multisymmetric functions $\Gamma^d_A(A[x_1, x_2, \dots, x_r]) = \mathrm{TS}^d_A(A[x_1, x_2, \dots, x_r])$. In the central section §7 a *minimal* set of generators for the ring of multisymmetric functions $\Gamma^d_A(A[x_1, x_2, \dots, x_r])$ is found in Theorem 7.19 for an arbitrary ring A. Several applications of this theorem is then given in §8. A sharp bound on the total degree of any generating set is given in Corollary 8.8, improving [5, Thm. 4.6]. In Corollary 8.10, the cases when $\Gamma^d_A(A[x_1, x_2, \dots, x_r])$ is generated by the elementary multisymmetric polynomials is determined as has previously been done by Briand [1, Thm. 1].

Finally we briefly discuss the relation between the generators of the ring of multisymmetric polynomials and the Chow scheme in Remark 8.11.

Acknowledgement. — I would like to thank D. Laksov for introducing me to divided powers and for many suggestions and comments. Thanks also to F. Vaccarino for reading an early manuscript and pointing out some references. Finally I thank the referee for several valuable comments.

2. Multi-indices, multinomials and a combinatorial result

Notation 2.1. — We let $\mathbb{N}$ be the set of non-negative integers $0, 1, 2, \dots$

Notation 2.2. — For a multi-index $\nu \in \mathbb{N}^{(\mathcal{I})}$ we let

$$((\nu)) = \binom{|\nu|}{\nu} = \frac{(\sum_\alpha \nu_\alpha)!}{\prod_\alpha (\nu_\alpha!)}$$

be the multinomial coefficient of ν. In particular $((a,b)) = \binom{a+b}{a}$.

Notation 2.3. — For $i \in \mathcal{I}$ we let $\mathbf{e}_i \in \mathbb{N}^{(\mathcal{I})}$ be the multi-index such that

$$(\mathbf{e}_i)_\alpha = \begin{cases} 0 & \text{if } \alpha \neq i \\ 1 & \text{if } \alpha = i. \end{cases}$$

Definition 2.4. — *For $n \in \mathbb{Q}$ and p a prime we let $\operatorname{ord}_p(n)$ be the order of n at p, i.e. $\operatorname{ord}_p(n)$ is defined by $n = \pm \prod_{p \text{ prime}} p^{\operatorname{ord}_p(n)}$.*

Definition 2.5. — *For $n \in \mathbb{N}$ we let $Q_p(n)(t) = a_s t^s + a_{s-1}t^{s-1} + \cdots + a_0 \in \mathbb{Z}[t]$ be the polynomial with coefficients $0 \leqslant a_k \leqslant p-1$ such that $Q_p(n)(p) = n$, i.e. $a_s a_{s-1} \dots a_0$ is the presentation of n in base p. If $\alpha \in \mathbb{N}^n$ then we let $Q_p(\alpha) = \sum_{k=1}^n Q_p(\alpha_k)$.*

Definition 2.6. — *If $P(t), Q(t) \in \mathbb{Z}[t]$ are polynomials then $P > Q$ means that $P(n) > Q(n)$ for all sufficiently large n.*

Lemma 2.7. — *Let $n \in \mathbb{N}$ and $\alpha \in \mathbb{N}^{(\mathcal{I})}$. We have that*

(i) $\operatorname{ord}_p(n!) = \frac{1}{p-1}\big(n - Q_p(n)(1)\big)$.
(ii) $\operatorname{ord}_p\,((\alpha)) = \frac{1}{p-1}\big(Q_p(\alpha)(1) - Q_p\big(|\alpha|\big)(1)\big)$.
(iii) $\operatorname{ord}_p\,((p^s\alpha)) = \operatorname{ord}_p\,((\alpha))$.

Proof. — (i) is easily verified, (ii) is an immediate consequence of (i) and (iii) follows from (ii). □

Lemma 2.8. — *Let $\alpha \in \mathbb{N}^{(\mathcal{I})}$. We have three inequalities*

$$\operatorname{ord}_p\,((\alpha)) \geqslant 0 \qquad Q_p(\alpha)(1) \geqslant Q_p\big(|\alpha|\big)(1) \qquad Q_p(|\alpha|) \geqslant Q_p(\alpha)$$

and equality in any of these inequalities holds if and only if the sum $\sum_{i\in\mathcal{I}} \alpha_i$ can be computed in base p without carrying, i.e if and only if $Q_p(|\alpha|) = Q_p(\alpha)$.

Proof. — The first inequality is obvious as $((\alpha))$ is a positive integer. It is further easily seen that the two last inequalities hold and with equality if and only if the sum $\sum_{i\in\mathcal{I}} \alpha_i$ can be computed in base p without carrying. The second inequality is a multiple of the first by Lemma 2.7 (ii) and thus $\operatorname{ord}_p\,((\alpha)) = 0$ if and only if $Q_p(|\alpha|) = Q_p(\alpha)$. □

Definition 2.9. — *Fix a positive integer r and let $\mathcal{M}^* = \mathbb{N}^r \setminus \{0\}$. We will identify $\beta \in \mathcal{M}^*$ with the monomial $x^\beta = x_1^{\beta_1} x_2^{\beta_2} \dots x_r^{\beta_r}$. In particular, we identify $\mathbf{e}_i \in \mathcal{M}^*$ with x_i. Given a multi-index $\alpha \in \mathcal{M}^*$ and an integer $d < |\alpha|$ we let $\mathcal{S}_{\alpha,d}$ be the set of $\nu \in \mathbb{N}^{(\mathcal{M}^*)}$ such that there is a decomposition $x^\alpha = \prod_{\beta \in \mathcal{M}^*} \left(x^\beta\right)^{\nu_\beta}$ and such that $|\nu| > d$. That is, the elements of $\mathcal{S}_{\alpha,d}$ are factorizations of x^α in at least $d+1$, not necessarily different, non-trivial monomials.*

Main Lemma 2.10. — *Given a multi-index $\alpha \in \mathcal{M}^*$, an integer $d < |\alpha|$ and a prime p, we let $s = \operatorname{ord}_p \gcd(\alpha)$. Then there exists a $\nu \in \mathcal{S}_{\alpha,d}$ such that*

$$\operatorname{ord}_p \frac{p^s((\nu))}{|\nu|} = 0$$

if and only if $Q_p(\alpha) > Q_p(d)$.

Proof. — First note that $\operatorname{ord}_p\big(p^s((\nu))/|\nu|\big)$ is always non-negative. In fact, there exists a $\beta \in \mathcal{M}^*$ such that $\nu_\beta > 0$ and $\operatorname{ord}_p \nu_\beta \leqslant s$, and $((\nu))/|\nu| = ((\nu - \mathbf{e}_\beta))/\nu_\beta$. We will prove the lemma in several steps:

I) *Reduction to the case where $s = 0$.* Assume that $s > 0$ and let $\nu \in \mathcal{S}_{\alpha,d}$. If p does not divide ν then define $\nu', \nu'', \widetilde{\nu} \in \mathbb{N}^{(\mathcal{M}^*)}$ by

$$\nu'_\beta = \left\lfloor \frac{\nu_\beta}{p} \right\rfloor \quad \text{and} \quad \widetilde{\nu} = p(\nu' + \nu'')$$

where ν'' is chosen such that

$$|\widetilde{\nu}| = p \left\lceil \frac{|\nu|}{p} \right\rceil \quad \text{and} \quad \sum_{\beta \in \mathcal{M}^*} \widetilde{\nu}_\beta \beta = \sum_{\beta \in \mathcal{M}^*} \nu_\beta \beta = \alpha.$$

Then $\widetilde{\nu} \in \mathcal{S}_{\alpha,d}$ since $|\widetilde{\nu}| \geqslant |\nu| \geqslant d+1$. To see that such a ν'' exists, let $\alpha'' = \alpha/p - \sum_{\beta \in \mathcal{M}^*} \nu'_\beta \beta$ and $q = \lceil (|\nu| - p|\nu'|)/p \rceil \leqslant |\alpha''|$. Then choose $\beta_1, \beta_2, \dots, \beta_q \in \mathcal{M}^*$ such that $\alpha'' = \beta_1 + \beta_2 + \dots + \beta_q$ and let $\nu'' = \sum_i \mathbf{e}_{\beta_i}$. Now as $\operatorname{ord}_p\big(|\nu|!/|\nu|\big) = \operatorname{ord}_p\big(|\widetilde{\nu}|!/|\widetilde{\nu}|\big)$ and $\operatorname{ord}_p(\nu!) = \operatorname{ord}_p\big((p\nu')!\big) \leqslant \operatorname{ord}_p(\widetilde{\nu}!)$ we obtain that

$$\operatorname{ord}_p \frac{((\nu))}{|\nu|} = \operatorname{ord}_p \frac{|\nu|!}{|\nu|\nu!} \geqslant \operatorname{ord}_p \frac{|\widetilde{\nu}|!}{|\widetilde{\nu}|\widetilde{\nu}!} = \operatorname{ord}_p \frac{((\widetilde{\nu}))}{|\widetilde{\nu}|}$$

and thus

$$\min_{\nu \in \mathcal{S}_{\alpha,d}} \operatorname{ord}_p \frac{p^s((\nu))}{|\nu|} = \min_{p\mu \in \mathcal{S}_{\alpha,d}} \operatorname{ord}_p \frac{p^s((p\mu))}{|p\mu|} = \min_{p\mu \in \mathcal{S}_{\alpha,d}} \operatorname{ord}_p \frac{p^{s-1}((\mu))}{|\mu|}$$

by Lemma 2.7 (iii). Let $p\mu \in \mathcal{S}_{\alpha,d}$. If we let $\alpha' = \alpha/p$ and $d' = \lfloor d/p \rfloor$ then $\mu \in \mathcal{S}_{\alpha',d'}$ as $p|\mu| \geqslant d+1$ implies that $|\mu| \geqslant \lceil (d+1)/p \rceil = d'+1$. Thus

$$\min_{p\mu\in\mathcal{S}_{\alpha,d}} \operatorname{ord}_p \frac{p^{s-1}((\mu))}{|\mu|} = \min_{\mu\in\mathcal{S}_{\alpha',d'}} \operatorname{ord}_p \frac{p^{s-1}((\mu))}{|\mu|}.$$

Finally $Q_p(\alpha) > Q_p(d)$ if and only if $Q_p(\alpha') > Q_p(d')$ and we conclude step I) by induction on s.

II) *Reduction to the case where $\nu = \sum_{i=1}^r \delta_i \mathbf{e}_{x_i} + \mathbf{e}_{x^\gamma}$ with $\delta \in \mathbb{N}^r$ and $\gamma \in \mathcal{M}^*$.* From step I) we can assume that $p \nmid \alpha$ and hence $p \nmid \nu$. If we choose β_0 such that $p \nmid \nu_{\beta_0}$ then

$$\operatorname{ord}_p \frac{((\nu))}{|\nu|} = \operatorname{ord}_p\ ((\nu - \mathbf{e}_{x^{\beta_0}})).$$

For every $\beta \in \mathcal{M}^*$ choose $i(\beta) \in \{1,2,\dots,r\}$ such that $\beta_{i(\beta)} > 0$ and let

$$\nu' = \sum_{\beta\in\mathcal{M}^*} \nu_\beta \mathbf{e}_{x_{i(\beta)}} - \mathbf{e}_{x_{i(\beta_0)}}.$$

Then $|\nu'| = |\nu| - 1$ and $\operatorname{ord}_p\ ((\nu')) \leqslant \operatorname{ord}_p\ ((\nu - \mathbf{e}_{x^{\beta_0}}))$. Finally if we let $\nu'' = \nu' + \mathbf{e}_{x^\gamma}$ with $x^\gamma \in \mathcal{M}^*$ such that $\sum_{\beta\in\mathcal{M}^*} \nu''_\beta \beta = \sum_{\beta\in\mathcal{M}^*} \nu_\beta \beta = \alpha$ then $|\nu''| = |\nu|$ and

$$\operatorname{ord}_p \frac{((\nu''))}{|\nu''|} = \operatorname{ord}_p \frac{((\nu'' - \mathbf{e}_{x^\gamma}))}{\nu''_\gamma} \leqslant \operatorname{ord}_p\ ((\nu')) \leqslant \operatorname{ord}_p \frac{((\nu))}{|\nu|}.$$

Let $\mathcal{T}_{\alpha,d} = \{\delta \in \mathbb{N}^r\ :\ \delta < \alpha,\ |\delta| \geqslant d\}$.

III) $\operatorname{ord}_p\ ((\nu))/|\nu| = \operatorname{ord}_p\ ((\delta))$ *for some $\delta \in \mathcal{T}_{\alpha,d}$.* From the previous step we can assume that $\nu = \sum_{i=1}^r \delta_i \mathbf{e}_{x_i} + \mathbf{e}_{x^\gamma}$. If $|\gamma| \geqslant 2$, i.e. $x^\gamma \neq x_j$ for some j then

$$\frac{((\nu))}{|\nu|} = \frac{((\delta_1, \delta_2, \dots, \delta_r, 1))}{\delta_1 + \delta_2 + \dots + \delta_r + 1} = ((\delta)).$$

Otherwise $x^\gamma = x_j$ and $\nu = \sum_{i=1}^r \alpha_i \mathbf{e}_{x_i}$. As $p \nmid \alpha$ by step I), there is an k such that $p \nmid \alpha_k$ and we can write $\nu = \sum_{i=1}^r \delta'_i \mathbf{e}_{x_i} + \mathbf{e}_{x_k}$ where $\delta' = \alpha - \mathbf{e}_k$. Then

$$\operatorname{ord}_p \frac{((\nu))}{|\nu|} = \operatorname{ord}_p\ ((\nu - \mathbf{e}_{x_k})) = \operatorname{ord}_p\ ((\delta')).$$

IV) $\min_{\nu\in\mathcal{S}_{\alpha,d}} \operatorname{ord}_p\ ((\nu))/|\nu| = \min_{\delta\in\mathcal{T}_{\alpha,d}} \operatorname{ord}_p\ ((\delta))$. From step III) it follows that

$$\min_{\nu\in\mathcal{S}_{\alpha,d}} \operatorname{ord}_p \frac{((\nu))}{|\nu|} \geqslant \min_{\delta\in\mathcal{T}_{\alpha,d}} \operatorname{ord}_p\ ((\delta)).$$

For any $\delta \in \mathcal{T}_{\alpha,d}$ we let $\gamma = \alpha - \delta$ and $\nu = \sum_i \delta_i \mathbf{e}_{x_i} + \mathbf{e}_{x^\gamma} \in \mathcal{S}_{\alpha,d}$. As $\operatorname{ord}_p\ ((\nu))/|\nu| = \operatorname{ord}_p\ ((\delta)) - \operatorname{ord}_p(\nu_\gamma) \leqslant \operatorname{ord}_p\ ((\delta))$ this concludes step IV).

V) *The minimum of* $\left\{\operatorname{ord}_p\left((\delta)\right)\right\}_{\delta\in\mathcal{T}_{\alpha,d}}$ *is attained for a* δ *with* $|\delta|=d$. This follows immediately from the fact that $\operatorname{ord}_p\left((\delta)\right)\geqslant\operatorname{ord}_p\left((\delta-\mathbf{e}_i)\right)$ if i is chosen such that $\operatorname{ord}_p(\delta_i)$ is minimal.

VI) *Conclusion.* Let $\delta\in\mathbb{N}^r$ such that $|\delta|=d$ and $\delta<\alpha$. Lemma 2.8 shows that $\operatorname{ord}_p\left((\delta)\right)=0$ if and only if $Q_p(\delta)=Q_p\big(|\delta|\big)=Q_p(d)$. It is then easily seen that there exists a $\delta<\alpha$ such that $Q_p(\delta)=Q_p(d)$ if and only if $Q_p(\alpha)>Q_p(d)$. □

3. Polynomial laws and symmetric tensors

We recall the definition of a polynomial law [18, 19].

Definition 3.1. — *Let M and N be A-modules. We denote by $\mathcal{F}_M$ the functor*

$$\mathcal{F}_M\ :\ A\text{–}\mathbf{Alg}\to\mathbf{Sets},\qquad A'\mapsto M\otimes_A A'.$$

A polynomial law *from M to N is a natural transformation $f\ :\ \mathcal{F}_M\to\mathcal{F}_N$. More concretely, a polynomial law is a* map $f_{A'}\ :\ M\otimes_A A'\to N\otimes_A A'$ *for every A-algebra A' such that for any homomorphism of A-algebras $g\ :\ A'\to A''$ the diagram*

$$\begin{tikzcd}
M\otimes_A A' \arrow[r, "f_{A'}"] \arrow[d, "\mathrm{id}_M\otimes g"'] \arrow[dr, phantom, "\circ"] & N\otimes_A A' \arrow[d, "\mathrm{id}_N\otimes g"] \\
M\otimes_A A'' \arrow[r, "f_{A''}"] & N\otimes_A A''
\end{tikzcd}$$

commutes. The polynomial law f is homogeneous of degree d *if for any A-algebra A', the corresponding map $f_{A'}\ :\ M\otimes_A A'\to N\otimes_A A'$ is such that $f_{A'}(ax)=a^d f_{A'}(x)$ for any $a\in A'$ and $x\in M\otimes_A A'$. If B and C are A-algebras then a polynomial law from B to C is* multiplicative *if for any A-algebra A', the corresponding map $f_{A'}\ :\ B\otimes_A A'\to C\otimes_A A'$ is such that $f_{A'}(xy)=f_{A'}(x)f_{A'}(y)$ for any $x,y\in B\otimes_A A'$.*

Notation 3.2. — Let A be a ring and M and N be A-modules (resp. A-algebras). We let $\operatorname{Pol}^d(M,N)$ (resp. $\operatorname{Pol}^d_{\mathrm{mult}}(M,N)$) denote the polynomial laws (resp. multiplicative polynomial laws) $M\to N$ which are homogeneous of degree d.

Notation 3.3. — Let A be a ring and M an A-algebra. We denote the d^{th} tensor product of M over A by $\mathrm{T}^d_A(M)$. We have an action of the symmetric group $\mathfrak{S}_d$ on $\mathrm{T}^d_A(M)$ permuting the factors. The invariant ring of this action is the set of symmetric tensors and is denoted $\mathrm{TS}^d_A(M)$. By

$\mathrm{T}_A(M)$ and $\mathrm{TS}_A(M)$ we denote the graded A-modules $\bigoplus_{d\geqslant 0}\mathrm{T}^d_A(M)$ and $\bigoplus_{d\geqslant 0}\mathrm{TS}^d_A(M)$ respectively.

3.4 Shuffle product. — When B is an A-algebra, then $\mathrm{TS}^d_A(B)$ has a natural A-algebra structure induced from the A-algebra structure of $\mathrm{T}^d_A(B)$. The multiplication on $\mathrm{TS}^d_A(B)$ will be written as juxtaposition. For any A-module M, we can equip $\mathrm{T}_A(M)$ and $\mathrm{TS}_A(M)$ with A-algebra structures compatible with the grading. The multiplication on $\mathrm{T}_A(M)$ is the ordinary tensor product and the multiplication on $\mathrm{TS}_A(M)$ is called the *shuffle product* and is denoted by ×. If $x\in\mathrm{TS}^d_A(M)$ and $y\in\mathrm{TS}^e_A(M)$ then

$$x\times y=\sum_{\sigma\in\mathfrak{S}_{d,e}}\sigma\left(x\otimes_A y\right)$$

where $\mathfrak{S}_{d,e}$ is the subset of $\mathfrak{S}_{d+e}$ such that $\sigma(1)<\sigma(2)<\cdots<\sigma(d)$ and $\sigma(d+1)<\sigma(d+2)<\dots\sigma(d+e)$.

4. Divided powers

All of the material in this section can be found in [18] and a good exposition is [4, §2].

4.1. — Let A be a ring and M an A-module. Then there exists a graded A-algebra, the algebra of divided powers, denoted $\Gamma_A(M)=\bigoplus_{d\geqslant 0}\Gamma^d_A(M)$ equipped with maps $\gamma^d : M\to\Gamma^d_A(M)$ such that, denoting the multiplication with × as in [4], we have that for every $x,y\in M$, $a\in A$ and $d,e\in\mathbb{N}$

$$\Gamma^0_A(M)=A,\quad\text{and}\quad\gamma^0(x)=1 \tag{4.1}$$

$$\Gamma^1_A(M)=M,\quad\text{and}\quad\gamma^1(x)=x \tag{4.2}$$

$$\gamma^d(ax)=a^d\gamma^d(x) \tag{4.3}$$

$$\gamma^d(x+y)=\textstyle\sum_{d_1+d_2=d}\gamma^{d_1}(x)\times\gamma^{d_2}(y) \tag{4.4}$$

$$\gamma^d(x)\times\gamma^e(x)=((d,e))\gamma^{d+e}(x). \tag{4.5}$$

Using (4.1) and (4.2) we will identify A with $\Gamma^0_A(M)$ and M with $\Gamma^1_A(M)$. If $(x_\alpha)_{\alpha\in\mathcal{I}}$ is a family of elements of M and $\nu\in\mathbb{N}^{(\mathcal{I})}$ then we let

$$\gamma^\nu(x)=\mathop{\times}_{\alpha\in\mathcal{I}}\gamma^{\nu_\alpha}(x_\alpha)$$

which is an element of $\Gamma^d_A(M)$ with $d=|\nu|=\sum_{\alpha\in\mathcal{I}}\nu_\alpha$.

4.2 Functoriality. — $\Gamma_A(\cdot)$ is a covariant functor from the category of A-modules to the category of graded A-algebras [18, Ch. III §4, p. 251].

4.3 Base change. — For any A-algebra A' there is a natural isomorphism $\Gamma_{A'}(M\otimes_A A')\to\Gamma_A(M)\otimes_A A'$ taking $\gamma^d(x\otimes_A 1)$ to $\gamma^d(x)\otimes_A 1$ [18, Thm. III.3, p. 262]. This shows that γ^d is a homogeneous polynomial law of degree d.

4.4 Universal property. — The map $\operatorname{Hom}_A\bigl(\Gamma^d_A(M),N\bigr)\to\operatorname{Pol}^d(M,N)$ given by $f\mapsto f\circ\gamma^d$ is an isomorphism [18, Thm. IV.1, p. 266].

4.5 Basis. — If $(x_\alpha)_{\alpha\in\mathcal{I}}$ is a family of elements of M which generates M, then the family $\bigl(\gamma^\nu(x)\bigr)_{\nu\in\mathbb{N}^{(\mathcal{I})}}$ generates $\Gamma_A(M)$. If $(x_\alpha)_{\alpha\in\mathcal{I}}$ is a basis of M then $\bigl(\gamma^\nu(x)\bigr)_{\nu\in\mathbb{N}^{(\mathcal{I})}}$ is a basis of $\Gamma_A(M)$ [18, Thm. IV.2, p. 272].

4.6 Exactness. — The functor $\Gamma_A(\cdot)$ is a left adjoint [18, Thm. III.1, p. 257] and thus commutes with any (small) direct limit. It is thus *right exact* [7, Def. 2.4.1] but note that $\Gamma_A(\cdot)$ is a functor from the category of A-modules to the category of graded A-algebras and that the latter category is not abelian. By [7, Rem. 2.4.2] a functor is right exact if and only if it takes the initial object onto the initial object and commutes with finite coproducts and coequalizers. Thus $\Gamma_A(0)=A$ and given an exact diagram of A-modules

$$\begin{tikzcd} M' \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & M \arrow[r, "h"] & M'' \end{tikzcd}$$

the diagram

$$\begin{tikzcd} \Gamma_A(M') \arrow[r, shift left, "\Gamma f"] \arrow[r, shift right, "\Gamma g"'] & \Gamma_A(M) \arrow[r, "\Gamma h"] & \Gamma_A(M'') \end{tikzcd}$$

is an exact sequence of A-algebras and

$$\Gamma_A(M\oplus M')=\Gamma_A(M)\otimes_A\Gamma_A(M').$$

The latter identification can be made explicit [18, Thm. III.4, p. 262] as

$$\begin{aligned}\Gamma^d_A(M\oplus M')&=\bigoplus_{a+b=d}\bigl(\Gamma^a_A(M)\otimes_A\Gamma^b_A(M')\bigr)\\ \gamma^d(x+y)&=\sum_{a+b=d}\gamma^a(x)\otimes\gamma^b(y).\end{aligned}$$

This makes $\Gamma_A(M\oplus M')=\bigoplus_{a,b\geqslant 0}\Gamma^{a,b}_A(M\oplus M')$ into a bigraded algebra where $\Gamma^{a,b}_A(M\oplus M')=\Gamma^a_A(M)\otimes_A\Gamma^b_A(M')$.

4.7 Exactness of $\Gamma^d_A(\cdot)$. — If $M\twoheadrightarrow N$ is a surjection then it is easily seen from the explicit generators of $\Gamma^d(N)$ in 4.5 that $\Gamma^d_A(M)\twoheadrightarrow\Gamma^d_A(N)$ is surjective. This does, however, not imply that $\Gamma^d_A(\cdot)$ is right exact. In fact, in general it is not since we have that $\Gamma^d_A(M\oplus M')\neq\ \Gamma^d_A(M)\oplus\Gamma^d_A(M')$.

4.8 Filtered direct limits. — The functor $\Gamma_A^d(\cdot)$ commutes with *filtered* direct limits. In fact, if (M_α) is a directed filtered system of A-modules then

$$\bigoplus_{d\geqslant 0}\Gamma_A^d(\varinjlim_{A-\mathbf{Mod}} M_\alpha) = \varinjlim_{A-\mathbf{Alg}}\bigoplus_{d\geqslant 0}\Gamma_A^d(M_\alpha) = \\ = \varinjlim_{A-\mathbf{Mod}}\bigoplus_{d\geqslant 0}\Gamma_A^d(M_\alpha) = \bigoplus_{d\geqslant 0}\varinjlim_{A-\mathbf{Mod}}\Gamma_A^d(M_\alpha).$$

The first equality follows from the exactness of Γ described in paragraph 4.6 and the second from the fact that a filtered direct limit in the category of A-algebras coincides with the corresponding filtered direct limit in the category of A-modules [7, Cor. 2.9].

4.9 Γ *and* TS. — The homogeneous polynomial law $M \to \mathrm{TS}_A^d(M)$ of degree d given by $x \mapsto x^{\otimes_A d} = x \otimes_A \cdots \otimes_A x$ corresponds by the universal property 4.4 to an A-module homomorphism $\Gamma_A^d(M) \to \mathrm{TS}_A^d(M)$. This extends to an A-algebra homomorphism $\Gamma_A(M) \to \mathrm{TS}_A(M)$, where the multiplication in $\mathrm{TS}_A(M)$ is the shuffle product defined in paragraph 3.4, cf. [18, Prop. III.1, p.254].

When M is a free A-module the homomorphisms $\Gamma_A^d(M) \to \mathrm{TS}_A^d(M)$ and $\Gamma_A(M) \to \mathrm{TS}_A(M)$ are isomorphisms of A-modules respectively A-algebras [18, Prop. IV.5, p. 272]. More generally, these homomorphisms are isomorphisms when M is a *flat* A-module, see [3, 5.5.2.5, p. 123], or when A is a $\mathbb{Q}$-algebra, see [18, Ch. III, Cor., p. 256]. This is also discussed in [21].

4.10. — Let $d_1, d_2 \in \mathbb{N}$. There is a canonical homomorphism

$$\rho_{d_1,d_2}^{d_1+d_2} : \Gamma_A^{d_1+d_2}(M) \to \Gamma_A^{d_1}(M) \otimes_A \Gamma_A^{d_2}(M)$$

given by the homogeneous polynomial law $x \mapsto \gamma^{d_1}(x) \otimes \gamma^{d_2}(x)$ of degree $d_1 + d_2$ and the universal property 4.4. In particular

$$\rho_{d_1,d_2}^{d_1+d_2}\big(\gamma^\nu(x)\big) = \sum_{\substack{\nu^{(1)}+\nu^{(2)}=\nu \\ |\nu^{(i)}|=d_i}} \gamma^{\nu^{(1)}}(x) \otimes \gamma^{\nu^{(2)}}(x).$$

5. Multiplicative structure of $\Gamma_A^d(B)$

When B is a not necessarily commutative and unitary A-algebra then the multiplication of B induces a multiplication on $\Gamma_A^d(B)$ which we will denote by juxtaposition [19, (II)]. In particular $\gamma^d(x)\gamma^d(y) = \gamma^d(xy)$ and this makes γ^d into a multiplicative polynomial law homogeneous of degree d. Unless otherwise stated we will assume that B is a (commutative and unitary) A-algebra. The unit in $\Gamma^d_A(B)$ is $\gamma^d(1)$ and will be denoted by $\mathbf{1}^d$ in the sequel.

5.1 Universal property. — Let B and C be A-algebras. Then the map $\operatorname{Hom}_{A\text{-}\mathbf{Alg}}\bigl(\Gamma^d_A(B), C\bigr) \to \operatorname{Pol}^d_{\mathrm{mult}}(B, C)$ given by $f \to f \circ \gamma^d$ is an isomorphism [19, Thm.]. Also see [4, Prop. 2.5.1].

5.2 Γ *and* TS. — The homogeneous polynomial law $B \to \mathrm{TS}^d_A(B)$ of degree d given by $x \mapsto x^{\otimes_A d} = x \otimes_A \cdots \otimes_A x$ is multiplicative. The homomorphism $\varphi : \Gamma^d_A(B) \to \mathrm{TS}^d_A(B)$ in paragraph 4.9 is thus an A-algebra homomorphism. It is an isomorphism when B is a free A-module, or more generally when B is flat over A, since it is then an isomorphism of A-modules by 4.9.

This A-algebra homomorphism is studied in [21] and need neither be injective nor surjective. In particular it is shown that if $x \in \ker\varphi$ then $x^{d!} = 0$ and if $y \in \mathrm{TS}^d_A(B)$ then $y^{d!} \in \operatorname{im}\varphi$. Further, the corresponding morphism of schemes

$$\operatorname{Sym}^d_{\operatorname{Spec}(A)}\bigl(\operatorname{Spec}(B)\bigr) := \operatorname{Spec}\bigl(\mathrm{TS}^d_A(B)\bigr) \to \operatorname{Spec}\bigl(\Gamma^d_A(B)\bigr)$$

is a universal homeomorphism. An example due to Lundkvist [12] shows that $\bigl(\Gamma^d_A(B)\bigr)_{\mathrm{red}} \to \bigl(\mathrm{TS}^d_A(B)\bigr)_{\mathrm{red}}$ is not always an isomorphism. The induced morphism between *seminormalizations* $\bigl(\Gamma^d_A(B)\bigr)_{\mathrm{sn}} \to \bigl(\mathrm{TS}^d_A(B)\bigr)_{\mathrm{sn}}$, however, is an isomorphism as shown in [21].

Formula 5.3 (Multiplication formula [19, Eq. (3)]). — *Let $(x_\alpha)_{\alpha\in\mathcal{I}}$ be a family of elements in B and let $\mu, \nu \in \mathbb{N}^{(\mathcal{I})}$ with $d = |\mu| = |\nu|$. Then we have the following identity in $\Gamma^d_A(B)$*

$$\gamma^\mu(x)\gamma^\nu(x) = \sum_{\xi\in N_{\mu,\nu}} \gamma^\xi(x_{(1)}x_{(2)}) = \sum_{\xi\in N_{\mu,\nu}} \mathop{\times}_{(\alpha,\beta)\in\mathcal{I}\times\mathcal{I}} \gamma^{\xi_{\alpha\beta}}(x_\alpha x_\beta)$$

where $N_{\mu,\nu}$ is the set of multi-indices $\xi \in \mathbb{N}^{(\mathcal{I}\times\mathcal{I})}$ such that $\sum_{\beta\in\mathcal{I}} \xi_{\alpha\beta} = \mu_\alpha$ for every $\alpha \in \mathcal{I}$ and $\sum_{\alpha\in\mathcal{I}} \xi_{\alpha\beta} = \nu_\beta$ for every $\beta \in \mathcal{I}$.

5.4. — The homomorphism $\rho^{d_1+d_2}_{d_1,d_2}$ of 4.10 was given by the homogeneous polynomial law $B \to \Gamma^{d_1}_A(B) \otimes_A \Gamma^{d_2}_A(B)$ defined by $x \mapsto \gamma^{d_1}(x) \otimes \gamma^{d_2}(x)$. As this is a multiplicative law we get a homomorphism of A-algebras

$$\rho^{d_1+d_2}_{d_1,d_2} : \Gamma^{d_1+d_2}_A(B) \to \Gamma^{d_1}_A(B) \otimes_A \Gamma^{d_2}_A(B).$$

Further, given an A-algebra retraction $\epsilon : B \to A$ of the structure homomorphism $A \to B$ we get a homomorphism

$$\Gamma^{d_1+d_2}_A(B) \to \Gamma^{d_1}_A(B) \otimes_A \Gamma^{d_2}_A(B) \to \Gamma^{d_1}_A(B) \otimes_A \Gamma^{d_2}_A(A) \cong \Gamma^{d_1}_A(B)$$

which we will denote $\rho^{d_1+d_2}_{d_1,\epsilon}$.

5.5. — If $B=\bigoplus_{k\geqslant 0} B_k$ is a graded A-algebra with $B_0=A$ then we have a canonical augmentation $B\to B_0=A$. The corresponding homomorphism $\Gamma^{d_1+d_2}_A(B)\to\Gamma^{d_1}_A(B)$ given by 5.4 will be denoted $\rho^{d_1+d_2}_{d_1}$. If $(x_\alpha)_{\alpha\in\mathcal{I}}$ is a family of generators of $B_+=\bigoplus_{k\geqslant 1} B_k$ as an A-module, then by 4.5 the family $\bigl(\gamma^\nu(x)\times\mathbf{1}^{d-|\nu|}\bigr)_{\nu\in\mathbb{N}^{(\mathcal{I})},|\nu|\leqslant d}$ generates $\Gamma^d_A(B)$. If $e\geqslant d$

$$\rho^e_d\bigl(\gamma^\nu(x)\times\mathbf{1}^{e-|\nu|}\bigr)=\begin{cases}\gamma^\nu(x)\times\mathbf{1}^{d-|\nu|} & \text{if } |\nu|\leqslant d\\ 0 & \text{if } |\nu|>d.\end{cases}$$

Thus ρ^e_d is surjective.

Remark 5.6 (Geometrical interpretation of ρ). — If $A=k$ is an algebraically closed field, then the k-points of $\operatorname{Spec}\bigl(\Gamma^d_k(B)\bigr)=\operatorname{Sym}^d_k\bigl(\operatorname{Spec}(B)\bigr)$ correspond to the zero-cycles of degree d on $\operatorname{Spec}(B)$. Similarly, for any reduced A' it is possible to describe the A'-points of $\operatorname{Spec}\bigl(\Gamma^d_A(B)\bigr)$ as families of zero-cycles of degree d on $\operatorname{Spec}(B)$ parameterized by $\operatorname{Spec}(A')$ [20]. The homomorphism $\rho^{d_1+d_2}_{d_1,d_2}$ defined in 5.4 corresponds to a morphism of schemes

$$\operatorname{Spec}\bigl(\Gamma^{d_1}_A(B)\bigr)\times_A\operatorname{Spec}\bigl(\Gamma^{d_2}_A(B)\bigr)\to\operatorname{Spec}\bigl(\Gamma^{d_1+d_2}_A(B)\bigr)$$

describable as the addition of two families of cycles of degrees d_1 and d_2 respectively.

A retraction $\epsilon\,:\,\Gamma^1_A(B)=B\to A$ gives a family of zero-cycles of degree 1. The homomorphism $\rho^e_{d,\epsilon}$ corresponds to the addition of a family of cycles of degree d with $e-d$ times the family of cycles corresponding to ϵ. When $B=A[x_1,x_2,\dots,x_n]$ with its natural grading, then the canonical retraction on the zeroth graded part corresponds to the constant family of zero-cycles which is the origin in every fiber. The homomorphism ρ^e_d is the addition of a family of cycles of degree d with $e-d$ times this constant family.

6. Elementary symmetric polynomials and power sums

6.1. — If $B=A[x]$ is the polynomial ring in one variable, then $\Gamma^d_A(B)\cong\mathrm{TS}^d_A(B)$ is isomorphic to the ring of symmetric polynomials in d variables $A[x_1,x_2,\dots,x_d]^{\mathfrak{S}_d}$. It is well known that the ring of symmetric polynomials in d variables is the polynomial ring over A in the elementary symmetric functions $e_1,e_2,\dots,e_d$. The elementary symmetric functions correspond to the elements $e_k=\gamma^k(x)\times\mathbf{1}^{d-k}$ in $\Gamma^d_A(B)$. We also let $e_0=1=\mathbf{1}^d$ and $e_k=0$ for all $k>d$.

6.2. — We have another distinguished set of symmetric polynomials in d variables, the power sums. Let $p_k = x_1^k + x_2^k + \cdots + x_d^k$ for $k \in \mathbb{N}$. This corresponds to the element $p_k = x^k \times \mathbf{1}^{d-1}$. Note that

$$p_0 = \mathbf{1}^1 \times \mathbf{1}^{d-1} = ((1, d-1))\mathbf{1}^d = d.$$

Expressed in $\Gamma_A^d(B)$, the Newton identities relating e_k and p_k become

$$\sum_{\substack{a+b=k \\ a>0, b\geqslant 0}} (-1)^b p_a e_b + (-1)^k k e_k = 0, \quad k = 1, 2, \dots. \tag{6.1}$$

By induction these give the Waring formula, expressing p_k as a polynomial in $e_1, e_2, \dots, e_k$. Conversely, if $k!$ is invertible we obtain a formula expressing e_k in $p_1, p_2, \dots, p_k$. Thus if A is purely of characteristic 0, i.e. a $\mathbb{Q}$-algebra, then $\Gamma_A^d(B) = A[e_1, e_2, \dots, e_d] = A[p_1, p_2, \dots, p_d]$.

6.3. — Fix an integer $r \geqslant 1$ once and for all and let $B = A[x_1, x_2, \dots, x_r]$ be the polynomial ring in r variables. The rest of the paper will be devoted to the study of the ring of multisymmetric polynomials $\Gamma_A^d(B) = \mathrm{TS}_A^d(B)$.

6.4. — The analogues of the elementary symmetric polynomials are the elementary multisymmetric polynomials e_α given by

$$e_\alpha = \gamma^\alpha(x) \times \mathbf{1}^{d-|\alpha|} = \left(\mathop{\times}_{i=1}^{r} \gamma^{\alpha_i}(x_i) \right) \times \mathbf{1}^{d-|\alpha|}$$

for $\alpha \in \mathbb{N}^r$ such that $|\alpha| \leqslant d$ and $e_\alpha = 0$ otherwise. The elementary multisymmetric polynomials which only depend on one set of variables, i.e. such that $\alpha_i = k$ for some i and zero otherwise with $1 \leqslant k \leqslant d$, are called *primitive*.

6.5. — Similarly as in the 1-dimensional case, we define the multisymmetric power sum p_α as

$$p_\alpha = x^\alpha \times \mathbf{1}^{d-1} = \left(\prod_{i=1}^{r} x_i^{\alpha_i} \right) \times \mathbf{1}^{d-1}$$

with $\alpha \in \mathbb{N}^r$. As before, the p_α's with $\alpha_i = k$ for some i and zero otherwise with $1 \leqslant k \leqslant d$, are called *primitive*.

6.6. — When $r > 1$ it is no longer true that $\Gamma_A^d(B)$ is a polynomial ring. It is however easily seen that $\Gamma_A^d(B) = \mathrm{TS}_A^d(B)$ has relative dimension rd over A, i.e. $\mathrm{Sym}^d_{\mathrm{Spec}(A)}\big(\mathrm{Spec}(B)\big) := \mathrm{Spec}\big(\mathrm{TS}_A^d(B)\big)$ is equidimensional of relative dimension rd over $\mathrm{Spec}(A)$, cf. [6, Def. 13.3.2, Err. 35]. In fact $\mathrm{TS}_A^d(B) \hookrightarrow \mathrm{T}_A^d(B)$ is finite and the latter ring has relative dimension rd. A transcendence basis for $\Gamma_A^d(B)$ over A is given either by the primitive elementary multisymmetric functions or the primitive multisymmetric power sums.

It is well known and often (falsely) attributed to Weyl [25] that when A is purely of characteristic 0 then $\Gamma^d_A(B)$ is generated by the p_α's (or the e_α's) with $|\alpha| \leqslant d$. This result will also follow from Theorem 7.19 which gives generators for $\Gamma^d_A(B)$ for arbitrary A, cf. Corollary 8.4. For a brief outline of the classical proofs, see paragraph 7.1.

The Newton identities have a generalization to the multisymmetric case which has long been known, cf. [10, §4]. Recall that $e_\alpha = 0$ if $|\alpha| > d$.

Proposition 6.7 (Multisymmetric Newton identities). — *Let $\delta \in \mathbb{N}^r$ then*

$$\sum_{\substack{\alpha+\beta=\delta \\ \alpha\in\mathbb{N}^r\setminus 0,\ \beta\in\mathbb{N}^r}} (-1)^{|\beta|}((\alpha))p_\alpha e_\beta + (-1)^{|\delta|}|\delta|e_\delta = 0.$$

Proof. — The multisymmetric identities easily follow from the usual Newton identities by *polarization* : Let $A' = A[u_1, u_2, \dots, u_r]$. In $\Gamma^d_{A'}(A'[t])$ we have the usual Newton identities. Using the homomorphism $A'[t] \to A'[x_1, x_2, \dots, x_r]$ defined by $t \mapsto u_1x_1 + u_2x_2 + \cdots + u_rx_r$ we obtain identities in $\Gamma^d_{A'}(A'[x_1, x_2, \dots, x_r])$. Equating the coefficients of u^δ will then give the requested identity. For details see [25, Ch. II §3]. □

Corollary 6.8. — *If $d!$ is invertible in A then the two subrings of $\Gamma^d_A(B)$, generated by $(p_\alpha)_{|\alpha|\leqslant d}$ and $(e_\alpha)_{|\alpha|\leqslant d}$ respectively, coincide.*

Proof. — Repeated use of Proposition 6.7 with $|\delta| \leqslant d$ allows us to express p_β with $|\beta| \leqslant d$ as a polynomial in $(e_\alpha)_{\alpha\leqslant\beta}$ and e_β as a polynomial in $(p_\alpha)_{\alpha\leqslant\beta}$. In fact, all coefficients of the involved identities are $\leqslant |\delta|! \leqslant d!$ and hence invertible. □

Definition 6.9 (Basis). — *Let $\mathcal{M}$ be the monomials in B and $\mathcal{M}^* = \mathcal{M} \setminus \{1\}$. For $\nu \in \mathbb{N}^{(\mathcal{M})} \simeq \mathbb{N}^{(\mathbb{N}^r)}$ we let*

$$\mathbf{z}_\nu = \gamma^\nu(x) = \mathop{\times}_{\alpha\in\mathbb{N}^r} \gamma^{\nu_\alpha}(x^\alpha) \in \Gamma_A(B)$$

By paragraph 4.5 these elements form a basis of $\Gamma_A(B)$. A basis for $\Gamma^d_A(B)$ is then $\big(\mathbf{z}_\nu\big)_{\nu\in\mathbb{N}^{(\mathcal{M})},|\nu|=d}$ or written differently $\big(\mathbf{z}_\nu \times \mathbf{1}^{d-|\nu|}\big)_{\nu\in\mathbb{N}^{(\mathcal{M}^*)},|\nu|\leqslant d}$.

Definition 6.10 (Multidegree). — *Let the* multidegree mdeg : $\mathcal{M} \to \mathbb{N}^r$ *be defined by* $\mathrm{mdeg}(x^\alpha) = \alpha$. *We have a $\mathbb{N}^r$-grading on B given by*

$$B = \bigoplus_{\alpha\in\mathbb{N}^r} B_\alpha = \bigoplus_{\alpha\in\mathbb{N}^r} Ax^\alpha.$$

This grading on $\Gamma^1_A(B) = B$ induces in a natural way a $\mathbb{N}^r$-grading on the A-algebra $\Gamma_A(B)$ such that

$$\operatorname{mdeg}(\mathbf{z}_\nu) = \sum_{\alpha\in\mathbb{N}^r} \nu_\alpha \alpha.$$

We let $\Gamma^d_A(B)_\alpha$ be the A-module generated by the basis elements $\mathbf{z}_\nu$, $|\nu| = d$ of multidegree α. This makes $\Gamma^d_A(B) = \bigoplus_{\alpha\in\mathbb{N}^r} \Gamma^d_A(B)_\alpha$ into a $\mathbb{N}^r$-graded A-algebra as is easily seen from Formula 5.3.

The total degree *is the sum of the degree in every variable, e.g. the total degree of $\mathbf{z}_\nu$ is $\sum_{\alpha\in\mathbb{N}^r} \nu_\alpha |\alpha|$.*

Remark 6.11. — The multisymmetric polynomials e_α and p_α both have multidegree α.

Definition 6.12. — *We let $\Gamma^d_A(B)_{\langle\alpha\rangle} = A\big[\Gamma^d_A(B)_{\beta,\beta<\alpha}\big]$ be the subalgebra of $\Gamma^d_A(B)$ generated by elements of multidegree strictly less than α.*

Definition 6.13. — *The* length *of an element $f \in \Gamma^d_A(B)$ is the smallest integer ℓ such that $f = g \times \mathbf{1}^{d-\ell}$ for some $g \in \Gamma^\ell_A(B)$.*

Definition 6.14. — *Let $\mathcal{P}(A)$ be the set of primes $p \in \mathbb{N}$ such that $p \cdot 1_A \in A$ is not invertible.*

Remark 6.15. — If A is purely of characteristic 0, i.e. a $\mathbb{Q}$-algebra, then $\mathcal{P}(A) = \emptyset$. If A is a local ring with residue field of characteristic $p > 0$ or A is an algebra over a field of characteristic $p > 0$ then $\mathcal{P}(A) = \{p\}$. If A is a $\mathbb{Z}_{(p)}$-algebra then $\mathcal{P}(A) \subseteq \{p\}$.

7. Generators for the ring of multisymmetric polynomials

As before we let A be any ring, $r \geqslant 1$ a fix integer and $B = A[x_1, \dots, x_r]$. In this section we will prove the main theorem of this paper 7.19 in which a minimal generating set of $\Gamma^d_A(B) \cong \mathrm{TS}^d_A(B)$ as an A-algebra is given for any ring A.

7.1 Classical proof in characteristic zero. — In characteristic zero, it can be proved [10, 15, 25, 14] that the elementary multisymmetric functions $(e_\alpha)_{|\alpha|\leqslant d}$ generate the A-algebra $\Gamma^d_A(B)$ as follows:

1) Any multisymmetric function is a polynomial in the multisymmetric power sums $(p_\alpha)_{\alpha\in\mathbb{N}^r}$, see [22, pp. 15–16], [10, §5] or [14, Lemma 1]. As any element of length 1 is a sum of multisymmetric power sums, this can easily be proved using induction on the length.

2) The p_α:s can be expressed in the elementary multisymmetric functions $(e_\alpha)_{|\alpha|\leqslant d}$ and vice versa, see [10, §4], [14, Lemma 2–3] or Proposition 6.7.

When $r = 1$ step 2 is given by the classical Newton identities (6.1).

7.2 Proof in arbitrary characteristic. — The proof will roughly follow the same line as in characteristic zero but a much more careful treatment is required in arbitrary characteristic.

Let $g_{k,\alpha} = \gamma^k(x^\alpha) \times \mathbf{1}^{d-k}$ where $x^\alpha \in B$ is a monomial and $1 \leqslant k \leqslant d$ is an integer. We will first show in Proposition 7.3 that $\Gamma^d_A(B)$ is generated as an A-algebra by $(g_{k,\alpha})_{(k,\alpha)\in\mathcal{C}_0}$ where

$$\mathcal{C}_0 = \{(k,\alpha) \ : \ 1 \leqslant k \leqslant d,\ \alpha \in \mathbb{N}^r \setminus 0\}.$$

Using an analogue, Proposition 7.5, of the Newton identities, we will then show in Corollary 7.6 that if $\gcd(\alpha)$ is invertible in A then $g_{k,\alpha}$ together with elements of strictly smaller multidegree generate every element of multidegree $k\alpha$. We can therefore choose a subset $\mathcal{C}$ of $\mathcal{C}_0$ such that every multidegree $k\alpha$ occurs once in $\mathcal{C}$ and $(g_{k,\alpha})_{(k,\alpha)\in\mathcal{C}}$ generates $\Gamma^d_A(B)$:

(i) If every prime is invertible in A, we can let $\mathcal{C}$ be the subset of $\mathcal{C}_0$ with $k = 1$. This then gives the same generating set as obtained in step 1) of paragraph 7.1.

(ii) If k is a field of characteristic $p > 0$ and A is a k-algebra or a local ring with residue field k, we can choose $\mathcal{C}$ as the pairs (k,α) with $k = p^s$, $s \in \mathbb{N}$ and $p \nmid \alpha$.

(iii) For general A we can choose $\mathcal{C}$ as the subset of $\mathcal{C}_0$ such that $\gcd(\alpha) = 1$.

The difficult part is then to get a characterization of the multidegrees for which the corresponding generators are generated by elements of smaller multidegree. The main ingredient is a careful study, Proposition 7.15, of the possible relations between the elementary multisymmetric functions and multiples of the generators of Corollary 7.7. This is the analogue of the second step of 7.1. Using this ingredient and Main Lemma 2.10, an explicit minimal generator set is obtained in Theorem 7.19.

We begin with the following proposition which appears as [26, Cor. 4.5 b)] and [23, Cor. 2.3].

Proposition 7.3. — *$\Gamma^d_A(B)$ is generated as an A-algebra by elements of the form $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k}$ where x^α is a monomial in B and $1 \leqslant k \leqslant d$.*

Proof. — We will use induction on the length, see Definition 6.13, and prove that every element of the basis $\left(\mathbf{z}_\nu \times \mathbf{1}^{d-|\nu|}\right)_{\nu\in\mathbb{N}^{(\mathcal{M}^*)},|\nu|\leqslant d}$ can be written as a sum of products of elements $\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}$. The length of an element $u=\mathbf{z}_\nu\times\mathbf{1}^{d-|\nu|}$ is $\ell=|\nu|$. If u is not in the collection of the proposition then $u=\mathbf{z}_{\nu_1}\times\mathbf{z}_{\nu_2}\times\mathbf{1}^{d-\ell}$ for some non-zero $\nu_1,\nu_2\in\mathbb{N}^{(\mathcal{M}^*)}$ such that $\nu=\nu_1+\nu_2$. Using Formula 5.3 we can then write

$$\begin{aligned}u&=\mathbf{z}_{\nu_1}\times\mathbf{z}_{\nu_2}\times\mathbf{1}^{d-|\nu_1|-|\nu_2|}\\&=\big(\mathbf{z}_{\nu_1}\times\mathbf{1}^{d-|\nu_1|}\big)\big(\mathbf{z}_{\nu_2}\times\mathbf{1}^{d-|\nu_2|}\big)-\sum_{\substack{\mu\in\mathbb{N}^{(\mathcal{M}^*)}\\|\mu|<\ell}}c_\mu\mathbf{z}_\mu\times\mathbf{1}^{d-|\mu|}\end{aligned}$$

for some $c_\mu\in\mathbb{N}$. As this is a sum of products of terms of length $<\ell$ we can conclude by induction. □

7.4. — The classical Newton identities (6.1) show that for $x^\alpha\in B$ and $m\leqslant d$

$$\gamma^1(x^{m\alpha})\times\mathbf{1}^{d-1}+(-1)^m m\gamma^m(x^\alpha)\times\mathbf{1}^{d-m}\in\Gamma_A^d(B)_{\langle m\alpha\rangle}.$$

We will now slightly generalize this in the following proposition. Recall from paragraph 5.5 that for $e\geqslant d$ we have a *surjection* $\rho_d^e:\Gamma_A^e(B)\to\Gamma_A^d(B)$ such that if $\nu\in\mathbb{N}^{(\mathcal{M}^*)}$

$$\rho_d^e\big(\mathbf{z}_\nu\times\mathbf{1}^{e-|\nu|}\big)=\begin{cases}\mathbf{z}_\nu\times\mathbf{1}^{d-|\nu|} & \text{if } |\nu|\leqslant d\\ 0 & \text{if } |\nu|>d.\end{cases}$$

In particular, basis elements of length $>d$ are mapped to zero.

Proposition 7.5 (Generalized Newton relations). — *Let $x^\alpha\in B$ and k,m be positive integers such that $k\leqslant d$. Then*

$$\gamma^k(x^{m\alpha})\times\mathbf{1}^{d-k}-(-1)^{km-k}m\gamma^{km}(x^\alpha)\times\mathbf{1}^{d-km}\in\Gamma_A^d(B)_{\langle km\alpha\rangle}$$

if $km\leqslant d$ and

$$\gamma^k(x^{m\alpha})\times\mathbf{1}^{d-k}\in\Gamma_A^d(B)_{\langle km\alpha\rangle}$$

if $km>d$.

Proof. — Using the homomorphism ρ_d^e defined in paragraph 5.5 with $e\geqslant km$ we can assume that $km\leqslant d$. Further using the homomorphism $\Gamma_{\mathbb{Z}}^d(\mathbb{Z}[t])\to\Gamma_A^d(A[t])\to\Gamma_A^d(B)$ where the second map is induced by $A[t]\to B$, mapping t to x^α, it is enough to show that

$$\gamma^k(t^m)\times\mathbf{1}^{d-k}-(-1)^{km-k}m\gamma^{km}(t)\times\mathbf{1}^{d-km}\in\Gamma_{\mathbb{Z}}^d(\mathbb{Z}[t])_{\langle km\rangle}.$$

Since $\Gamma_{\mathbb{Z}}^d(\mathbb{Z}[t])$ is a polynomial ring in $e_1(t),\dots,e_d(t)$, where $e_i(t)=\gamma^i(t)\times\mathbf{1}^{d-i}$, we can write $e_k(t^m)$ *uniquely* as a polynomial in $e_1(t),\dots,e_{km}(t)$. Clearly, all terms of this polynomial will be in $\Gamma_{\mathbb{Z}}^d(\mathbb{Z}[t])_{\langle km\rangle}$ except the term $e_{km}(t)$. To determine the coefficient of $e_{km}(t)$ we tensor with $\mathbb{Q}$. The classical Newton identities, equation (6.1), show that

$$e_1\big((t^m)^k\big) + (-1)^k k e_k(t^m) \in \Gamma^d_{\mathbb{Q}}(\mathbb{Q}[t^m])_{\langle km\rangle}$$
$$e_1(t^{km}) + (-1)^{km} km e_{km}(t) \in \Gamma^d_{\mathbb{Q}}(\mathbb{Q}[t])_{\langle km\rangle}$$

and thus $e_k(t^m) = (-1)^{km-k} m e_{km}(t) + \Gamma^d_{\mathbb{Z}}(\mathbb{Z}[t])_{\langle km\rangle}$. □

Corollary 7.6. — *Let $x^{k\alpha} \in B$ be a monomial with* $\gcd(\alpha)$ *invertible in A. Then the subalgebra $A\big[\Gamma^d_A(B)_{\beta,\beta\leqslant k\alpha}\big] \subseteq \Gamma^d_A(B)$ is generated by $\Gamma^d_A(B)_{\langle k\alpha\rangle}$ together with, if $k \leqslant d$, the element $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k}$.*

Proof. — Follows immediately from Propositions 7.3 and 7.5. □

Corollary 7.7. — *$\Gamma^d_A(B)$ is generated as an A-algebra by the elements*

$$\big(\gamma^k(x^\alpha) \times \mathbf{1}^{d-k}\big)_{(k,x^\alpha)\in\mathcal{C}}$$

where $\mathcal{C} \subseteq \{1,2,\dots,d\} \times \mathcal{M}^*$ is one of the collections

$$\mathcal{C}_1 = \{(k,x^\alpha) \;:\; \gcd(\alpha)\cdot 1_A \textit{ invertible, } k \textit{ product of primes in } \mathcal{P}(A)\}$$
$$\mathcal{C}_2 = \{(k,x^\alpha) \;:\; \gcd(\alpha) = 1\}.$$

Proof. — If we let $\mathcal{C} = \{1,2,\dots,d\}\times\mathcal{M}^*$ be the full set of indices (k,x^α) then the corresponding set of elements $\big\{\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}\big\}$ is a generating set of $\Gamma^d_A(B)$ by Proposition 7.3. That $\mathcal{C}_1$ and $\mathcal{C}_2$ also give generating sets of $\Gamma^d_A(B)$ follows from Corollary 7.6. □

Remark 7.8. — Both generating sets of Corollary 7.7 have exactly one generator of each multidegree in $\mathbb{N}^r \setminus 0$. If $A = \mathbb{Z}$ then the two collections $\mathcal{C}_1$ and $\mathcal{C}_2$ coincide. In [23, pf. of Thm. 1] Vaccarino gives a proof of Corollary 7.7 with the second collection using a slightly different version of Proposition 7.3. As it is sometimes convenient to also have the first collection we will use either collection. Besides, all proofs work equally well with both collections.

Theorem 7.9 ([23, Thm. 1]). — *The ring of multisymmetric functions $\Gamma^d_A(A[x_1,x_2,\dots,x_r]) \cong \mathrm{TS}^d_A(A[x_1,x_2,\dots,x_r])$ is generated as an A-algebra by $\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}$ where $(k,x^\alpha)\in\{1,2,\dots,d\}\times\mathcal{M}^*$ is such that* $\gcd(\alpha)=1$ *and the total degree* $|\operatorname{mdeg}\big(\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}\big)| = k|\alpha|$ *is less than or equal to* $\max\big(d, r(d-1)\big)$.

Proof. — We repeat the proof in [23]. A result of Fleischmann [5, Thm. 4.6], cf. Corollaries 8.6 and 8.7, shows that $\Gamma^d_A(B)$ is generated by the elements of total degree $\leqslant \max\big(d, r(d-1)\big)$. The theorem then follows from Corollary 7.7 using the second collection. □

Remark 7.10. — As mentioned in the introduction, the generating set of Theorem 7.9 is not minimal. We will proceed to find a minimal subset of either the first or second collection of Corollary 7.7 which generates $\Gamma^d_A(B)$. Such a minimal subset is then *unique*. In fact, as the generators of both collections are homogeneous and each multidegree occurs exactly once, any minimal subset of $\mathcal{C}$ which generates $\Gamma^d_A(B)$ consists of the elements $\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}$ such that $\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}\notin\Gamma^d_A(B)_{\langle k\alpha\rangle}$.

Remark 7.11. — To determine if $\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}\notin\Gamma^d_A(B)_{\langle k\alpha\rangle}$ it will be useful to lift this relation to a relation in $\Gamma^n_A(B)$ where n is an integer such that $n\geqslant k|\alpha|$, cf. the proof of Theorem 7.19. In several of the following results involving x^α we will therefore use $\Gamma^n_A(B)$ instead of $\Gamma^d_A(B)$ with an n such that $n\geqslant k|\alpha|$.

Remark 7.12. — Let $x^\alpha\in\mathcal{M}^*$ and choose $n\in\mathbb{N}$ such that $|\alpha|\leqslant n$. The multisymmetric Newton identities, Proposition 6.7, show that in $\Gamma^n_A(B)$

$$((\alpha))p_\alpha(x)+(-1)^{|\alpha|}|\alpha|e_\alpha(x)\in\Gamma^n_A(B)_{\langle\alpha\rangle}. \tag{7.1}$$

If $|\alpha|$ divides $((\alpha))$, the image of $|\alpha|$ in A is not a zero divisor, and the LHS of relation (7.1) belongs to $|\alpha|\Gamma^n_A(B)_{\langle\alpha\rangle}$, then we obtain the relation

$$\frac{(|\alpha|-1)!}{\alpha_1!\dots\alpha_r!}p_\alpha(x)+(-1)^{|\alpha|}e_\alpha(x)\in\Gamma^n_A(B)_{\langle\alpha\rangle}.$$

For arbitrary α and A this relation is not true, but we will show that there exist similar relations between $\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}$ and $e_{k\alpha}(x)$. We will first show that if such a relation exists then it is unique.

Proposition 7.13. — *Let $x^{k\alpha}$ be a monomial in B such that* $\gcd(\alpha)$ *is invertible in A and $n\geqslant k|\alpha|$. Let $a\in A$ be such that*

$$a\gamma^k(x^\alpha)\times\mathbf{1}^{n-k}\in\Gamma^n_A(B)_{\langle k\alpha\rangle}.$$

Then $a=0$.

Proof. — Let $A'\twoheadrightarrow A$ be any lifting of A to a ring of characteristic 0, e.g. $A'=\mathbb{Z}[(T_a)_{a\in A}]$, and let $I=\ker(A'\twoheadrightarrow A)$ and $B'=A'[x_1,x_2,\dots,x_r]$. We have an induced surjection $\Gamma^n_{A'}(B')\twoheadrightarrow\Gamma^n_{A'}(B')\otimes_{A'}A\cong\Gamma^n_A(B)$. Let $a'\in A'$ be a lifting of a. Then

$$a'\gamma^k(x^\alpha)\times\mathbf{1}^{n-k}+\sum_{\substack{\nu\in\mathbb{N}^{(\mathcal{M})}\\|\nu|=n}}i_\nu\mathbf{z}_\nu\in\Gamma^n_{A'}(B')_{\langle k\alpha\rangle}$$

for some $i_\nu\in I$. Since $\Gamma^n_{A'}(B')_{\langle ka\rangle}$ is graded by multidegree, taking the part with multidegree $k\alpha$ we obtain by Corollary 7.6

$$(a'+i)\gamma^k(x^\alpha)\times\mathbf{1}^{n-k}\in\Gamma^n_{A'}(B')_{\langle k\alpha\rangle} \tag{7.2}$$

with $i \in I$. The homomorphism $B' = A'[x_1, x_2, \dots, x_r] \twoheadrightarrow A'[t]$, taking x_j to t for every $1 \leqslant j \leqslant r$, induces a homomorphism $\Gamma^n_{A'}(B') \twoheadrightarrow \Gamma^n_{A'}(A'[t]) \cong A'[e_1(t), e_2(t), \dots, e_n(t)]$ which applied to equation (7.2) gives

$$(a' + i)\gamma^k(t^{|\alpha|}) \times \mathbf{1}^{n-k} \in \Gamma^n_{A'}(A'[t])_{\langle k|\alpha|\rangle}.$$

Thus by the generalized Newton relations of Proposition 7.5 it follows that

$$(a' + i)|\alpha| e_{k|\alpha|}(t) \in \Gamma^n_{A'}(A'[t])_{\langle k|\alpha|\rangle}.$$

As $\Gamma^n_{A'}(A'[t])_{\langle k|\alpha|\rangle} = A'[e_1(t), e_2(t), \dots, e_{k|\alpha|-1}(t)]$ and $\Gamma^n_{A'}(A'[t])$ is a polynomial ring we see that $(a' + i)|\alpha| = 0$. But the integer $|\alpha|$ is not a zero divisor in A' by construction. Hence $a' + i = 0$ and a fortiori $a = 0$. □

As an immediate corollary of Proposition 7.13 we see that the generators of total degree $\leqslant d$ in any of the collections of Corollary 7.7 are contained in the minimal generating subset:

Corollary 7.14. — *Let $x^{k\alpha} \in \mathcal{M}^*$ then $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k} \notin \Gamma^d_A(B)_{\langle k\alpha\rangle}$ if $k|\alpha| \leqslant d$.*

We now establish relations of the kind mentioned in Remark 7.12.

Proposition 7.15. — *Let $f_1, f_2, \dots, f_s \in \mathcal{M}^*$ be non-trivial monomials in B and $\ell_1, \ell_2, \dots, \ell_s$ positive integers such that $f_1^{\ell_1} \dots f_s^{\ell_s} = x^{k\alpha}$ with $g = \gcd(\alpha)$ invertible in A and let $n \geqslant k|\alpha|$. Then $m = ((\ell))\frac{kg}{|\ell|} \in \mathbb{Z}$ and $a = m/g \in A$ is the unique element in A such that*

$$\gamma^\ell(f) \times \mathbf{1}^{n-|\ell|} - (-1)^{|\ell|-k} a\gamma^k(x^\alpha) \times \mathbf{1}^{n-k} \in \Gamma^n_A(B)_{\langle k\alpha\rangle}. \tag{7.3}$$

Proof. — The existence and uniqueness of a follow from Corollary 7.6 and Proposition 7.13 respectively. Proposition 7.5 shows that

$$\gamma^\ell(f) \times \mathbf{1}^{n-|\ell|} - (-1)^{|\ell|-k'} ag\gamma^{k'}(x^{\alpha'}) \times \mathbf{1}^{n-k'} \in \Gamma^n_A(B)_{\langle k'\alpha'\rangle}$$

with $k' = kg$ and $\alpha' = \alpha/g$. Replacing α with α' and k with k' we can thus assume that $g = 1$.

To determine the value of a it is now enough to consider the case when $A = \mathbb{Z}$ as $\Gamma^n_A(B) = \Gamma^n_{\mathbb{Z}}(\mathbb{Z}[x_1, x_2, \dots, x_r]) \otimes_{\mathbb{Z}} A$ and a is unique. This also shows that a is the image of an integer in $\mathbb{Z}$. Multiplying both sides of equation (7.3) with $\ell! = \ell_1!\ell_2! \dots \ell_s!$ we obtain

$$\left(\mathop{\times}_{i=1}^{s} f_i^{\times \ell_i}\right) \times \mathbf{1}^{n-|\ell|} - (-1)^{|\ell|-k} a'\gamma^k(x^\alpha) \times \mathbf{1}^{n-k} \in \Gamma^n_A(B)_{\langle k\alpha\rangle}$$

with $a' = \ell! a$. As B is a free A-module so is $\Gamma^d_A(B)$ by paragraph 4.5. Thus $\ell!$ is not a zero divisor in $\Gamma^n_A(B)$ and it is enough to verify that $a' = \big(|\ell| - 1\big)!k$. Replacing ℓ and f with $\ell' = 1^{|\ell|}$ and $f' = (f_1, f_1, f_1, \dots, f_s, f_s)$ we can thus assume that $\ell = 1^{|\ell|}$. Further, using Proposition 7.5 it is enough to show that

$$\Big(\mathop{\times}_{i=1}^{s} f_i\Big) \times \mathbf{1}^{n-s} - (-1)^{s-1}(s-1)!\gamma^1(x^{k\alpha}) \times \mathbf{1}^{n-1} \in \Gamma^n_A(B)_{\langle k\alpha\rangle}.$$

This is obvious for $s = 1$. For $s > 1$ we have by induction on s that

$$\begin{aligned}\Big(\mathop{\times}_{i=1}^{s} f_i\Big) \times \mathbf{1}^{n-s} &= \big(f_1 \times \cdots \times f_{s-1} \times \mathbf{1}^{n-(s-1)}\big)\big(f_s \times \mathbf{1}^{n-1}\big)\\ &\qquad - \sum_{i=1}^{s-1} f_1 \times f_2 \times \cdots \times f_i f_s \times \cdots \times f_{s-1} \times \mathbf{1}^{n-(s-1)}\\ &= -(s-1)(-1)^{s-2}(s-2)!\gamma^1(x^{k\alpha}) \times \mathbf{1}^{n-1} + \Gamma^n_A(B)_{\langle k\alpha\rangle}\end{aligned}$$

which completes the proof. □

Corollary 7.16. — *Let $x^{k\alpha}$ be a monomial such that $g = \gcd(\alpha)$ is invertible in A and let $n \geqslant k|\alpha|$. Then there exists a unique element $a \in \mathbb{Z} \cdot 1_A \subseteq A$ such that*

$$(a/g)\gamma^k(x^\alpha) \times \mathbf{1}^{n-k} - e_{k\alpha} \in \Gamma^n_A(B)_{\langle k\alpha\rangle}.$$

For every prime $p \in \mathcal{P}(A)$ we have that

$$\operatorname{ord}_p(a) = \operatorname{ord}_p((k\alpha)) - \operatorname{ord}_p\big(|\alpha|\big).$$

Proof. — From Proposition 7.15 it follows that $a = (-1)^{k|\alpha|-k}((k\alpha))\frac{kg}{k|\alpha|}$ and thus that $\operatorname{ord}_p(a) = \operatorname{ord}_p((k\alpha)) - \operatorname{ord}_p\big(|\alpha|\big)$. □

We are now able to completely characterize the cases in which the elementary symmetric polynomials generate all elements of total degree $\leqslant d$ in $\Gamma^d_A(B)$.

Lemma 7.17. — *Let $x^{k\alpha}$ be a monomial in B such that $\gcd(\alpha)$ is invertible in A and $k|\alpha| \leqslant d$. Then the following statements are equivalent:*

(i) *$A\big[\Gamma^d_A(B)_{\beta,\beta\leqslant k\alpha}\big] \subseteq \Gamma^d_A(B)$ is generated by $\Gamma^d_A(B)_{\langle k\alpha\rangle}$ and $e_{k\alpha}$.*

(ii) *$\gamma^k(x^\alpha) \times \mathbf{1}^{d-k} \in \Gamma^d_A(B)_{\langle k\alpha\rangle} + Ae_{k\alpha}$.*

(iii) *$\operatorname{ord}_p\,((k\alpha)) - \operatorname{ord}_p\big(|\alpha|\big) = 0$ for every $p \in \mathcal{P}(A)$ such that $p \leqslant d$.*

Proof. — (i) $\iff$ (ii) by Corollary 7.6. (ii) $\iff$ (iii) follows from Corollary 7.16. □

Proposition 7.18. — *The subalgebra $A\big[\Gamma^d_A(B)_{\beta,|\beta|\leqslant d}\big] \subseteq \Gamma^d_A(B)$ is generated by the elementary multisymmetric polynomials $(e_\alpha)_{|\alpha|\leqslant d}$ where $e_\alpha = \gamma^\alpha(x) \times \mathbf{1}^{d-|\alpha|}$, if and only if one of the following conditions is satisfied*

(i) *$r = 1$.*

(ii) *$r = 2$ and $d = 3$.*

(iii) $r = 2$, $d = 4$ *and* 3 *is invertible in* A.

(iv) $(d-1)!$ *is invertible in* A.

Proof. — When $r = 1$ it is well known that $\Gamma^d_A(B)$ is the polynomial ring $A[e_1, e_2, \dots, e_d]$ which shows that (i) is sufficient.

By Lemma 7.17 and induction on $|\alpha|$ it is enough to check that

$$\operatorname{ord}_p\ ((k\alpha)) - \operatorname{ord}_p\big(|\alpha|\big) = 0$$

for every monomial $x^{k\alpha}$ and $p \in \mathcal{P}(A)$ such that $p \leqslant d$, $k|\alpha| \leqslant d$ and $\gcd(\alpha)$ is invertible in A.

If d itself is a prime in $\mathcal{P}(A)$ then this prime has not to be checked. In fact, if $d \mid k\alpha$ then $d = k$ and $\alpha = \mathbf{e}_i$ for some i giving $\operatorname{ord}_d\ ((k\mathbf{e}_i)) - \operatorname{ord}_d(1) = 0$. If $d \nmid k\alpha$ then either $k|\alpha| < d$ which gives $\operatorname{ord}_d\ ((k\alpha)) - \operatorname{ord}_d\big(|\alpha|\big) = 0 - 0 = 0$ or $k = 1$ and $|\alpha| = d$ which gives $\operatorname{ord}_d\ ((\alpha)) - \operatorname{ord}_d\big(|\alpha|\big) = 1 - 1 = 0$. It is thus sufficient that $(d-1)!$ is invertible which is condition (iv).

If a prime $2 < p < d$ is not invertible and $r \geqslant 2$ then

$$\gamma^1(x_1^{p-1}x_2^2) \times \mathbf{1}^{d-1} = \gamma^1(x^\alpha) \times \mathbf{1}^{d-1}$$

with $\alpha = (p-1)\mathbf{e}_1 + 2\mathbf{e}_2$ is an element which is not generated by elementary multisymmetric polynomials. In fact $\operatorname{ord}_p\ ((\alpha)) - \operatorname{ord}_p\big(|\alpha|\big) = 1 - 0 = 1$.

It is thus necessary that every prime $p < d$, except possibly 2, is invertible. Therefore we need only consider the case where 2 is not invertible and $d \geqslant 3$. If $r \geqslant 3$ then

$$\gamma^1(x_1x_2x_3) \times \mathbf{1}^{d-1}$$

is not generated by the e_α:s as $\operatorname{ord}_2\ ((1,1,1)) - \operatorname{ord}_2(1+1+1) = 1 - 0 = 1$. If $r = 2$ and $d \geqslant 5$ then

$$\gamma^1(x_1^3x_2^2) \times \mathbf{1}^{d-1}$$

is not generated by the e_α:s since $\operatorname{ord}_2\ ((3,2)) - \operatorname{ord}_2(3+2) = 1 - 0 = 1$. Finally if $r = 2$ and $d \leqslant 4$ then $\operatorname{ord}_2\ ((\alpha)) - \operatorname{ord}_2\big(|\alpha|\big) = 0$ for all $\alpha \in \{(1,1),(2,1),(3,1)\}$ and this completes the proof of the proposition. □

We will now show the main theorem of this section. It gives a *minimal* generator set for $\Gamma^d_A(B)$ where A is any ring and improves [23, Thm. 1] also when $A = \mathbb{F}_p$ and $d = p^s$. A sharp bound on the total degree for any A is given in Corollary 8.8.

THEOREM 7.19. — *Let* $\mathcal{C}$ *be one of the two collections of Corollary 7.7. Let* $\widetilde{\mathcal{C}}$ *be the subset of* $\mathcal{C}$ *such that* $(k, x^\alpha) \in \widetilde{\mathcal{C}}$ *if either* $k|\alpha| \leqslant d$ *or* $Q_p(k\alpha) \leqslant Q_p(d)$ *for some* $p \in \mathcal{P}(A)$.

The A*-algebra* $\Gamma^d_A(B)$ *is then generated by* $\big(\gamma^k(x^\alpha) \times \mathbf{1}^{d-k}\big)_{(k,\alpha)\in\widetilde{\mathcal{C}}}$ *and this is a minimal set of generators.*

Proof. — By Corollary 7.7, the elements $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k}$ with $(k,\alpha) \in \mathcal{C}$ generate $\Gamma^d_A(B)$. As every multidegree occurs exactly once in $\mathcal{C}$ it is clear that we get a minimal set of generators by taking those $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k}$ which cannot be written as sums of products of elements of strictly smaller multidegree, i.e. $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k}$ is in the minimal set if and only if $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k} \notin \Gamma^d_A(B)_{\langle k\alpha\rangle}$.

If $k|\alpha| \leqslant d$ then Corollary 7.14 shows that $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k} \notin \Gamma^d_A(B)_{\langle k\alpha\rangle}$. If $k|\alpha| > d$ and $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k} \in \Gamma^d_A(B)_{\langle k\alpha\rangle}$ then we lift the corresponding relation in $\Gamma^d_A(B)$ to $\Gamma^n_A(B)$, where $n = k|\alpha|$, using the homomorphism $\rho^n_d : \Gamma^n_A(B) \twoheadrightarrow \Gamma^d_A(B)$ defined in paragraph 5.5 and obtain

$$\gamma^k(x^\alpha) \times \mathbf{1}^{n-k} = \sum_{\substack{\nu\in\mathbb{N}^{(\mathcal{M}^*)} \\ d+1\leqslant|\nu|\leqslant n}} a_\nu \mathbf{z}_\nu \times \mathbf{1}^{n-|\nu|} + \Gamma^n_A(B)_{\langle k\alpha\rangle} \tag{7.4}$$

for some $a_\nu \in A$. Conversely, if there exist $a_\nu \in A$ such that relation (7.4) holds then $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k} \in \Gamma^d_A(B)_{\langle k\alpha\rangle}$. The theorem now follows from the following lemma:

Lemma 7.20. — *Let $x^{k\alpha}$ be a monomial such that* $\gcd(\alpha)$ *is invertible in A. Let d and n be positive integers such that $d < k|\alpha| \leqslant n$. Then there exists a relation in $\Gamma^n_A(B)$ of the form*

$$\gamma^k(x^\alpha) \times \mathbf{1}^{n-k} = \sum_{\substack{\nu\in\mathbb{N}^{(\mathcal{M}^*)} \\ d<|\nu|\leqslant n}} a_\nu \mathbf{z}_\nu \times \mathbf{1}^{n-|\nu|} + \Gamma^n_A(B)_{\langle k\alpha\rangle} \tag{7.5}$$

where $a_\nu \in A$ are almost all zero, if and only if $Q_p(k\alpha) > Q_p(d)$ for every prime $p \in \mathcal{P}(A)$.

Proof. — We can assume that every term $\mathbf{z}_\nu \times \mathbf{1}^{n-|\nu|}$ has multidegree $k\alpha$. The sum is then over the set $\mathcal{S}_{k\alpha,d}$ of Definition 2.9. Proposition 7.15 gives that

$$\mathbf{z}_\nu \times \mathbf{1}^{n-|\nu|} - c_\nu \gamma^k(x^\alpha) \times \mathbf{1}^{n-k} \in \Gamma^n_A(B)_{\langle k\alpha\rangle}$$

where $c_\nu = (-1)^{|\nu|-k} k((\nu))/|\nu|$. Thus

$$\Big(1 - \sum_{\nu\in\mathcal{S}_{k\alpha,d}} a_\nu c_\nu\Big)\big(\gamma^k(x^\alpha) \times \mathbf{1}^{n-k}\big) \in \Gamma^n_A(B)_{\langle k\alpha\rangle} \tag{7.6}$$

if and only if (7.5) holds. Moreover, relation (7.6) is equivalent to $1 = \sum_\nu a_\nu c_\nu$ in A by Proposition 7.13. If $1 = \sum_\nu a_\nu c_\nu$ then for every $p \in \mathcal{P}(A)$ there exists a $\nu \in \mathcal{S}_{k\alpha,d}$ such that $\operatorname{ord}_p(c_\nu) = 0$. Conversely, if this is the case we can choose $a_\nu \in \mathbb{Z}$ such that $\sum_\nu a_\nu c_\nu$ is invertible. By Main Lemma 2.10 the existence of a ν such that $\operatorname{ord}_p(c_\nu) = 0$ is equivalent to $Q_p(k\alpha) > Q_p(d)$. This concludes the proof of the lemma. □

8. Remarks and applications

Remark 8.1. — In Theorem 7.19 it is enough to consider non-invertible primes $\leqslant d$ since if $p > d$ then $Q_p(k\alpha) > Q_p(d) = d$ for any $k|\alpha| > d$.

Remark 8.2. — Let us extend the definition of $Q_p(n)$ to include $p = \infty$ with $Q_\infty(n) = n \in \mathbb{Z}[t]$. We can then replace the condition in Theorem 7.19 with: $(k, \alpha) \in \widetilde{\mathcal{C}}$ if and only if $Q_p(k\alpha) \leqslant Q_p(d)$ for some $p \in \mathcal{P}(A) \cup \{\infty\}$.

Remark 8.3. — We note that it immediately follows from Theorem 7.19 that if $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k}$ is in a minimal set of generators then so is $\gamma^{k'}(x^{\alpha'}) \times \mathbf{1}^{d-k'}$ for every $k'\alpha' < k\alpha$.

Corollary 8.4 ([10, 15, 25, 13, 14, 17]). — *If $d!$ is invertible in A then $\Gamma^d_A(A[x_1, \dots, x_r])$ is minimally generated as an A-algebra by either the elementary multisymmetric polynomials or the multisymmetric power sums of total degree $\leqslant d$.*

Proof. — From Theorem 7.19 and Remark 8.1 we deduce that the elements of total degree $\leqslant d$ generates $\Gamma^d_A(A[x_1, \dots, x_r])$. The statement then follows from Corollary 6.8. □

Corollary 8.5. — *Let A be of equal or mixed characteristic p, i.e. p is the only non-invertible prime in A. Then $\Gamma^d_A(A[x_1, \dots, x_r])$ is minimally generated as an A-algebra by the elements $\gamma^{p^s}(x^\alpha) \times \mathbf{1}^{d-p^s}$ with $s \in \mathbb{N}$ and $\alpha \in \mathbb{N}^r \setminus 0$ such that $p \nmid \alpha$ and $Q_p(p^s\alpha) \leqslant Q_p(d)$ or equivalently $Q_p(\alpha) \leqslant Q_p\big(\lfloor d/p^s \rfloor\big)$.*

Proof. — Follows immediately from Theorem 7.19 using the first collection of Corollary 7.7. □

Corollary 8.6 ([5, Thm. 4.6]). — *Let A be an arbitrary ring. Then $\Gamma^d_A(A[x_1, \dots, x_r])$ is generated as an A-algebra by $\gamma^d(x_1), \gamma^d(x_2), \dots, \gamma^d(x_r)$ and the elements $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k}$ with $k\alpha \leqslant (d-1, d-1, \dots, d-1)$. Further, there is no smaller multidegree bound and if $d = p^s$ for some prime p not invertible in A, then $\Gamma^d_A(A[x_1, \dots, x_r])$ is not generated by elements of strictly smaller multidegree.*

Proof. — If $k\alpha_i \geqslant d$ and $|k\alpha| > d$ then $Q_p(k\alpha) > Q_p(d)$ for any prime p which shows that $\gamma^k(x^\alpha) \times \mathbf{1}^{d-k}$ is not among the minimal generators of Theorem 7.19. On the other hand $(d-1)\mathbf{e}_i = (0, \dots, 0, d-1, 0, \dots, 0) \in \mathbb{N}^r$ is the multidegree of a minimal generator and it follows that there is no smaller multidegree bound. If $d = p^s$ then $Q_p\big((d-1, d-1, \dots, d-1)\big) < Q_p(d)$ which shows that there is an element of every multidegree $\leqslant (d-1, d-1, \dots, d-1)$ in any generating set. □

From Corollary 8.6 we immediately obtain:

Corollary 8.7 ([5, Thm. 4.6, 4.7]). — *If A is an arbitrary ring then $\Gamma^d_A(A[x_1,\dots,x_r])$ is generated as an A-algebra by elements $\gamma^k(x^\alpha)\times \mathbf{1}^{d-k}$ of total degree $k|\alpha|\leqslant \max\bigl(d,r(d-1)\bigr)$. Further, this total degree bound is sharp if $d=p^s$ for some prime $p\in\mathcal{P}(A)$.*

A more careful examination of the conditions in the theorem gives a sharp total degree bound on the generators of $\Gamma^d_A(B)$:

Corollary 8.8. — *Let d be an integer. For every prime p we let $1\leqslant a_p\leqslant p-1$ and $b_p\in\mathbb{N}$ be the unique integers such that $d=a_pp^{b_p}+c_p$ for some $0\leqslant c_p<p^{b_p}$. For any ring A the A-algebra $\Gamma^d_A(A[x_1,\dots,x_r])$ is then minimally generated by elements of total degree at most*

$$\max\left\{d,\max_{p\in\mathcal{P}(A)}\bigl((a_p+r-1)p^{b_p}-r\bigr)\right\}$$

and every generating set contains an element attaining this bound.

Proof. — If $r=1$ then the bound becomes d and is sharp as $\Gamma^d_A(A[x])=A[e_1,e_2,\dots,e_d]$ so we will assume that $r\geqslant 2$. Let p be a prime not invertible in A and $\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}\in\Gamma^d_A(B)$ an element of total degree $k|\alpha|>\max\{d,(a-1)p^b+r(p^b-1)\}$ where $a=a_p$ and $b=b_p$.

If $\beta\in\mathbb{N}^r$ is such that $|\beta|>(l-1)p^m+r(p^m-1)$ for some integer $1\leqslant l\leqslant p-1$ then there exists $\beta'\leqslant\beta$ such that $Q_p(\beta')=lt^m$ and we have that

$$\begin{aligned}|\beta-\beta'|>(r-1)p^m-r&=\bigl(r(p-1)-p\bigr)p^{m-1}+r(p^{m-1}-1)\\&\geqslant(p-2)p^{m-1}+r(p^{m-1}-1)\end{aligned}$$

as $r\geqslant 2$.

We can thus find $\alpha_b,\alpha_{b-1},\dots,\alpha_0$ such that $Q_p(\alpha_b)=at^b$, $Q_p(\alpha_m)=(p-1)t^m$ for $m<b$ and $k\alpha\geqslant\alpha_b+\alpha_{b-1}+\dots+\alpha_0$. This shows that

$$Q_p(k\alpha)\geqslant at^b+(p-1)t^{b-1}+(p-1)t^{b-2}+\dots+(p-1)\geqslant Q_p(d)$$

and as $k|\alpha|>d$ we have that $Q_p(k\alpha)\neq Q_p(d)$. By Theorem 7.19 this implies that $\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}$ is generated by elements of lower degree.

To show that the bound is attained, consider the element $\gamma^k(x^\alpha)\times\mathbf{1}^{d-k}$ with

$$k\alpha=(ap^b-1,p^b-1,\dots,p^b-1),\quad \gcd(\alpha)\text{ invertible}$$

which is not generated by elements of lower degree since

$$\begin{aligned} Q_p(k\alpha) &= Q_p\big((ap^b-1, p^b-1, \dots, p^b-1)\big) \\ &= (a-1)t^b + r(p-1)t^{b-1} + r(p-1)t^{b-2} + \dots + r(p-1) \\ &< Q_p(d). \end{aligned}$$

□

Remark 8.9. — The inequality

$$(a_p + r - 1)p^{b_p} - r \leqslant r\left(a_p p^{b_p} - 1\right) \leqslant r(d-1)$$

with equality if and only if $d = p^{b_p}$, or $r = 1$ and $d = a_p p^{b_p}$, together with Corollary 8.8 gives another proof of Corollary 8.7. Further we see that the total degree bound $\max\big(d, r(d-1)\big)$ is sharp if and only if $r(d-1) \leqslant d$ or $d = p^s$, that is if one of the following conditions is satisfied

(i) $r = 1$.
(ii) $r = 2$ and $d = 2$.
(iii) $d = p^s$ with $p \in \mathcal{P}(A)$.

Corollary 8.10 ([1, Thm. 1]). — *$\Gamma^d_A(A[x_1, \dots, x_r])$ is generated as an A-algebra by elementary multisymmetric polynomials if and only if one of the following conditions is satisfied*

(i) *$r = 1$.*
(ii) *$d!$ is invertible in A.*
(iii) *$r = 2$ and $d = 2$.*
(iv) *$r = 2$, $d = 3$ and 3 is invertible in A.*

Proof. — If $r = 1$ then $\Gamma^d_A(A[x_1, \dots, x_r])$ is the polynomial ring in the elementary polynomials so (i) is sufficient and we can assume that $r \geqslant 2$. It then follows from Proposition 7.18 that every prime such that $2 < p < d$ is invertible in A. If $d > 2$ is a prime then $x_1^{d-1}x_2^2 \times \mathbf{1}^{d-1}$ is a sum of products of elements of total degree $\leqslant d$ if and only if d is invertible by Theorem 7.19 since $Q_d\big((d-1, 2)\big) < Q_d(d)$. Thus it is necessary that every prime such that $2 < p \leqslant d$ is invertible in A. On the other hand condition (ii) is sufficient by Corollary 8.4.

This leaves the case when 2 is not invertible in A but every odd prime $\leqslant d$ is. By Proposition 7.18 we can then assume that $r \geqslant 2$ and $d = 2$ or $r = 2$ and $d \leqslant 4$. If $d = 2$ and $r \geqslant 3$ then $\gamma^1(x_1x_2x_3) \times 1$ is not generated by elements of lower degree as $Q_2\big((1,1,1)\big) < Q_2(3)$. If $d = 4$ then $\gamma^1(x_1^3x_2^2) \times \mathbf{1}^3$ is not generated by elements of lower degree as $Q_2\big((3,2)\big) < Q_2(4)$. In the remaining cases, $r = 2$ and $d = 2$ or $d = 3$, it is easily seen that

$Q_2(k\alpha) < Q_2(d)$ implies that $k|\alpha| \leqslant d$ and we can conclude with Proposition 7.18. □

Remark 8.11. — Let k be an algebraically closed field. It can be shown that the Chow scheme $\operatorname{Chow}_{0,d}(\mathbb{A}^r_k \hookrightarrow \mathbb{P}^r_k)$, parameterizing zero-cycles of degree d in $\mathbb{A}^r_k$, is isomorphic to $\operatorname{Spec}(C)$ where C is the subring of $\Gamma^d_k(k[x_1, x_2, \dots, x_r]) \cong \mathrm{TS}^d_k(k[x_1, x_2, \dots, x_r])$ generated by the elementary multisymmetric polynomials. This gives a morphism

$$\operatorname{Sym}^d(\mathbb{A}^r_k) := \operatorname{Spec}\bigl(\mathrm{TS}^d_k(k[x_1, x_2, \dots, x_r])\bigr) \to \operatorname{Chow}_{0,d}(\mathbb{A}^r_k \hookrightarrow \mathbb{P}^r_k)$$

which is an isomorphism exactly in the cases listed in Corollary 8.10.

In general it is always possible to find a projective embedding $\mathbb{A}^r \hookrightarrow \mathbb{P}^N$ such that

$$\operatorname{Sym}^d(\mathbb{A}^r_k) \to \operatorname{Chow}_{0,d}(\mathbb{A}^r_k \hookrightarrow \mathbb{P}^N_k)$$

is an isomorphism. A bound on the degree of the generators of the ring $\mathrm{TS}^d_k(k[x_1, x_2, \dots, x_r])$ such as Corollary 8.6 gives an *effective* answer to the embedding needed to obtain such an isomorphism.

These issues are thoroughly discussed in [21].

Remark 8.12. — The results of §§7-8 immediately generalize to the case where $B = A[(x_\alpha)_{\alpha \in \mathcal{I}}]$ is the polynomial ring in an infinite number of variables. This is easily seen considering statement by statement but as B is the filtered direct limit of finitely generated polynomial rings, it also follows directly from the fact that $\Gamma^d_A(\cdot)$ commutes with filtered direct limits as shown in paragraph 4.8.

BIBLIOGRAPHY

[1] E. Briand, "When is the algebra of multisymmetric polynomials generated by the elementary multisymmetric polynomials?", *Beiträge Algebra Geom.* **45** (2004), no. 2, p. 353-368.

[2] H. E. A. Campbell, I. Hughes & R. D. Pollack, "Vector invariants of symmetric groups", *Canad. Math. Bull.* **33** (1990), no. 4, p. 391-397.

[3] P. Deligne, "Cohomologie à supports propres", in *exposé XVII of SGA 4, Théorie des topos et cohomologie étale des schémas. Tome 3*, Springer-Verlag, Berlin, 1973, p. 250-480. Lecture Notes in Math., Vol. 305.

[4] D. Ferrand, "Un foncteur norme", *Bull. Soc. Math. France* **126** (1998), no. 1, p. 1-49.

[5] P. Fleischmann, "A new degree bound for vector invariants of symmetric groups", *Trans. Amer. Math. Soc.* **350** (1998), no. 4, p. 1703-1712.

[6] A. Grothendieck, "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas", *Inst. Hautes Études Sci. Publ. Math.* (1964-67), p. 259, 231, 255, 361.

[7] A. Grothendieck & J. L. Verdier, “Prefaisceaux”, in *exposé I of SGA 4, Théorie des topos et cohomologie étale des schémas. Tome 1: Théorie des topos*, Springer-Verlag, Berlin, 1972, p. 1-217. Lecture Notes in Math., Vol. 269.

[8] D. Hilbert, “Ueber die Theorie der algebraischen Formen”, *Math. Ann.* **36** (1890), no. 4, p. 473-534.

[9] F. Junker, “Die Relationen, welche zwischen den elementaren symmetrischen Functionen bestehen”, *Math. Ann.* **38** (1891), no. 1, p. 91-114.

[10] ———, “Uber symmetrische Functionen von mehreren Reihen von Veränderlichen”, *Math. Ann.* **43** (1893), no. 2-3, p. 225-270.

[11] ———, “Die symmetrischen Functionen und die Relationen zwischen den Elementarfunctionen derselben”, *Math. Ann.* **45** (1894), no. 1, p. 1-84.

[12] C. Lundkvist, “Counterexamples regarding Symmetric Tensors and Divided Powers”, Preprint, Feb 2007, arXiv:math/0702733.

[13] M. Nagata, “On the normality of the Chow variety of positive 0-cycles of degree m in an algebraic variety”, *Mem. Coll. Sci. Univ. Kyoto. Ser. A. Math.* **29** (1955), p. 165-176.

[14] A. Neeman, “Zero cycles in $\mathbb{P}^n$”, *Adv. Math.* **89** (1991), no. 2, p. 217-227.

[15] E. Noether, “Der Endlichkeitssatz der Invarianten endlicher Gruppen”, *Math. Ann.* **77** (1915), no. 1, p. 89-92.

[16] ———, “Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p”, *Nachr. Ges. Wiss. Göttingen* (1926), p. 28-35.

[17] D. R. Richman, “Explicit generators of the invariants of finite groups”, *Adv. Math.* **124** (1996), no. 1, p. 49-76.

[18] N. Roby, “Lois polynomes et lois formelles en théorie des modules”, *Ann. Sci. École Norm. Sup. (3)* **80** (1963), p. 213-348.

[19] ———, “Lois polynômes multiplicatives universelles”, *C. R. Acad. Sci. Paris Sér. A-B* **290** (1980), no. 19, p. A869-A871.

[20] D. Rydh, “Families of zero cycles and divided powers”, In preparation, 2007.

[21] ———, “Hilbert and Chow schemes of points, symmetric products and divided powers”, In preparation, 2007.

[22] L. Schläfli, “Über die Resultante eines systemes mehrerer algebraischen Gleichungen”, *Denkschr. Kais. Akad. Wiss. Math.-Natur. Kl.* **4** (1852), p. 9-112, Reprinted in “Gesammelte matematische Abhandlungen”, Band II, Verlag Birkhäuser, Basel, (1953).

[23] F. Vaccarino, “The ring of multisymmetric functions”, *Ann. Inst. Fourier (Grenoble)* **55** (2005), no. 3, p. 717-731.

[24] H. Weber, *Lehrbuch der Algebra*, second ed., vol. 2, Braunschweig, Berlin, 1899, xvi+856 pages.

[25] H. Weyl, *The Classical Groups. Their Invariants and Representations*, Princeton University Press, Princeton, N.J., 1939, xii+302 pages.

[26] D. Ziplies, “Generators for the divided powers algebra of an algebra and trace identities”, *Beiträge Algebra Geom.* (1987), no. 24, p. 9-27.

Manuscrit reçu le 6 mars 2006,
accepté le 20 février 2007.

David RYDH
KTH
Department of Mathematics
100 44 Stockholm (Sweden)
dary@math.kth.se