Russian Math. Surveys **59**:1 125–145 ©2004 RAS(DoM) and LMS

Uspekhi Mat. Nauk **59**:1 125–144 DOI 10.1070/RM2004v059n01ABEH000704

Rings of continuous functions, symmetric products, and Frobenius algebras

V. M. Buchstaber [Bukhshtaber] and E. G. Rees

Abstract. A constructive proof is given for the classical theorem of Gel'fand and Kolmogorov (1939) characterising the image of the evaluation map from a compact Hausdorff space X into the linear space $C(X)^*$ dual to the ring $C(X)$ of continuous functions on X. Our approach to the proof enabled us to obtain a more general result characterising the image of the evaluation map from the symmetric products $\mathrm{Sym}^n(X)$ into $C(X)^*$. A similar result holds if $X = \mathbb{C}^m$ and leads to explicit equations for symmetric products of affine algebraic varieties as algebraic subvarieties in the linear space dual to the polynomial ring. This leads to a better understanding of the algebra of multisymmetric polynomials.

The proof of all these results is based on a formula used by Frobenius in 1896 in defining higher characters of finite groups. This formula had no further applications for a long time; however, it has appeared in several independent contexts during the last fifteen years. It was used by A. Wiles and R. L. Taylor in studying representations and by H.-J. Hoehnke and K. W. Johnson and later by J. McKay in studying finite groups. It plays an important role in our work concerning multivalued groups. Several properties of this remarkable formula are described. It is also used to prove a theorem on the structure constants of Frobenius algebras, which have recently attracted attention due to constructions taken from topological field theory and singularity theory. This theorem develops a result of Hoehnke published in 1958. As a corollary, a direct self-contained proof is obtained for the fact that the 1-, 2-, and 3-characters of the regular representation determine a finite group up to isomorphism. This result was first published by Hoehnke and Johnson in 1992.

Contents

The present paper is based on the talk given by E. G. Rees at the conference "Kolmogorov and contemporary mathematics," Moscow, 2003.

AMS 2000 *Mathematics Subject Classification.* Primary 46E25, 05E05; Secondary 05A18, 54C40, 20C15, 20C05.

§1. Introduction

In 1939 Kolmogorov and Gel'fand published the paper "On rings of continuous functions on topological spaces" (see [11]). The main result of their paper identifies a compact Hausdorff space X with the space of maximal ideals of the ring of continuous functions on X. Monographs and textbooks containing basic functional analysis usually include this result. In modern terminology it can be stated as follows.

Theorem 1. *Let X be a compact Hausdorff space. Then, for an appropriate topology on the space of continuous complex-valued functions $C(X)$ on X, the evaluation map*

$$\mathcal{E}\colon X \to \operatorname{Hom}(C(X), \mathbb{C}), \qquad \mathcal{E}(x)\varphi = \varphi(x),$$

is a homeomorphism onto the set of all ring homomorphisms $C(X) \to \mathbb{C}$.

This theorem is an analogue of Hilbert's Nullstellensatz: *If V is an affine algebraic variety with coordinate ring $A = \mathbb{C}[x_1, \dots, x_n]/J$, where J is a (radical) ideal defining V, then the evaluation map*

$$\mathcal{E}\colon V \to \operatorname{Hom}(A, \mathbb{C})$$

defines an isomorphism between the variety V and the set of all ring homomorphisms.

Well-known reformulations of these theorems can be obtained by noting that the set of all ring homomorphisms $A \to \mathbb{C}$ can readily be identified with the set (usually denoted by m-Spec(A)) of all maximal ideals of A.

We take the following point of view: the set of all ring homomorphisms $f\colon A \to \mathbb{C}$ is the algebraic variety in the linear space $\operatorname{Hom}(A, \mathbb{C})$ given by the infinite set of equations

$$\{f(1) = 1 \text{ and } f(ab) = f(a)f(b) \text{ for every } a, b \in A\}$$

involving the coordinate maps $a\colon \operatorname{Hom}(A, \mathbb{C}) \to \mathbb{C}$, $a(f) = f(a)$. Since we deal with linear homomorphisms, it suffices to consider only the equations $f(1) = 1$ and $f(a^2) = f(a)^2$, where a ranges over an additive basis in A.

The standard proof of the Kolmogorov–Gel'fand theorem found in textbooks argues by contradiction as follows.

Let I be a proper ideal in the function ring $C(X)$ such that there are no points $x \in X$ at which all functions $\varphi \in I$ vanish. Then for any point $x \in X$ there is a non-negative real-valued function $\varphi_x \in I$ whose values are greater than 1 in some neighbourhood U_x of x. Using the fact that the space X is compact, we can construct a real-valued function $\varphi \in I$ whose values are greater than 1 on the entire space X. Such a function is invertible, and hence a non-zero constant function belongs to I, that is, $I = C(X)$.

In [2] we presented a constructive proof of our theorem in [3] that characterises the symmetric products $\operatorname{Sym}^n(X)$ as algebraic varieties in $C(X)^*$. In the case $n = 1$ this gives a proof of the Gel'fand–Kolmogorov theorem. For a given ring homomorphism $f\colon C(X) \to \mathbb{C}$ the proof constructs a unique point $x \in X$ such that $f(\varphi) = \varphi(x)$ for any $\varphi \in C(X)$. In the (extensive) literature on this topic we found no proof of the Gel'fand–Kolmogorov theorem similar to that presented below.

Let us first consider the case in which X is a finite set. Then $C(X) \cong \mathbb{C}^n$, where n is the number of elements in X. Consider the basis $\{\delta_x : x \in X\}$ for $C(X)$ with $\delta_x(x) = 1$ and $\delta_x(y) = 0$ if $x \neq y$. It is clear that $1 = \sum \delta_x$. Since $\delta_x^2 = \delta_x$, for a ring homomorphism f we have $f(\delta_x)^2 = f(\delta_x)$, and hence $f(\delta_x) = 0$ or 1 for each x. On the other hand, $1 = f(1) = \sum_{x \in X} f(\delta_x)$, and hence there is a unique point $x_0 \in X$ such that $f(\delta_{x_0}) = 1$; finally, using the expansion $\varphi = \sum \varphi(x)\delta_x$, we see that $f(\varphi) = \varphi(x_0)$ for any $\varphi \in C(X)$.

Let us now show how to adapt this argument to the case of a compact Hausdorff space X.

Definition 1. Let $K \subset X$ be a compact subset of a topological space X. A sequence of continuous functions $\varphi_r \colon X \to [0,1]$ $(r \in \mathbb{N})$ is said to be *enclosing* for K if

1) $\varphi_r(\mathrm{Supp}(\varphi_{r+1})) = 1$ for any $r \in \mathbb{N}$,
2) $\varphi_r(x) = 1$ for every $r \Leftrightarrow x \in K$.

It is clear that $\varphi_r \varphi_s = \varphi_s$ for $s > r$.

Example. Let K be a compact subset of a metric space X with the metric $d(\,\cdot\,,\cdot\,)$. Then the sequence of functions

$$\varphi_r(x) = \begin{cases} 0 & \text{if } d(x,K) \geqslant 1/r, \\ 1 & \text{if } d(x,K) \leqslant 1/(r+1), \\ (r+1)(1 - r d(x,K)) & \text{if } 1/(r+1) \leqslant d(x,K) \leqslant 1/r, \end{cases}$$

is enclosing for K.

The definition of an enclosing sequence for a compactum K obviously generalises to that of an *enclosing net* (in other words, a *generalised sequence*) of continuous functions $\varphi_t \colon X \to [0,1]$ $(t \in T)$, where T is some directed set. The proof of the fact that an enclosing net exists for any compactum K in a compact Hausdorff space X is left to the reader. Moreover, to avoid overloading our argument with technical details, we speak in what follows about enclosing sequences, and in the end use the fact that the assertions thus obtained remain valid for enclosing nets.

Lemma 2. *Let $\{\varphi_r\}$ be an enclosing sequence for a compactum K. Then for any r there is an open neighbourhood U_r of K such that $\varphi_r = 1$ on U_r.*

Proof. We set $U_r = \{x : \varphi_{r+1}(x) > 0\}$. Then $K \subset U_r$ and $U_r \subset \mathrm{Supp}(\varphi_{r+1})$. Hence, $\varphi_r = 1$ on U_r.

Lemma 3. *Let $\{\varphi_r\}$ be an enclosing sequence for a compactum K and let $\psi \colon X \to \mathbb{R}$ be a function such that $\psi(x) = 1$ for any $x \in U$, where U is an open neighbourhood of K. Then $(1 - \psi)\varphi_r = 0$ for large enough r.*

Proof. Let $x \notin U$. We choose an r such that $\varphi_r(x) = 0$. Then the set $\varphi_r^{-1}[0,1)$ is an open neighbourhood of x whose closure is disjoint from U. Let us cover the compact space $X \backslash U$ by finitely many neighbourhoods of this kind and denote by r_0 the largest number r corresponding to these neighbourhoods. Then $(1-\psi)\varphi_{r_0} = 0$, and hence $(1 - \psi)\varphi_s = (1 - \varphi)\varphi_{r_0}\varphi_s = 0$ for $s > r_0$.

Lemma 4. *Let $f\colon C(X) \to \mathbb{C}$ be a ring homomorphism and let φ_r be a sequence of functions in $C(X)$ such that $\varphi_r\varphi_s = \varphi_s$ for any $r < s$. Then either there is an r_0 such that $f(\varphi_r) = 0$ for $r \geqslant r_0$ or $f(\varphi_r) = 1$ for any r.*

Proof. We have $(f(\varphi_r) - 1)f(\varphi_s) = 0$ for any $r < s$. In this case if $f(\varphi_r) \neq 1$, then $f(\varphi_s) = 0$ for any $s > r$. This argument implies the desired result.

Definition 2. Let $f\colon C(X) \to \mathbb{C}$ be a ring homomorphism and let $\{\varphi_r\}$ be an enclosing sequence for a compactum $K \subset X$. By the *weight* of K with respect to the sequence $\{\varphi_r\}$ we mean the number $w_f^{\varphi}(K) \in \{0, 1\}$ equal to $f(\varphi_r)$ for large values of r.

Proposition 5. *Let $\{\varphi_r\}$ and $\{\psi_r\}$ be two enclosing sequences for a given compactum K. Then $w_f^{\varphi}(K) = w_f^{\psi}(K)$.*

This tells us that the weight $w_f(K)$ of a compactum does not depend on the choice of an enclosing sequence.

Proof. Suppose that $w_f^{\varphi}(K) = 1$ and $w_f^{\psi}(K) = 0$. Then $f(\varphi_r) = 1$ for any r, whereas $f(\psi_r) = 0$ for any r greater than some r_0. Using Lemma 3 with $\psi = \psi_{r_0}$, we find an $m > r_0$ such that $\psi_{r_0}\varphi_m = \varphi_m$. Thus, $f(1 - \psi_{r_0})f(\varphi_m) = 0$; however, $f(1 - \psi_{r_0}) = 1$, and hence $f(\varphi_r) = 0$ for $r > m$. The contradiction thus obtained proves the proposition.

Definition 3. By the *support* of a ring homomorphism $f\colon C(X) \to \mathbb{C}$ we mean the set $S_f = \{x : w_f(x) = 1\}$.

Proposition 6. *For any ring homomorphism f the set S_f consists of a single point.*

Proof. We first assume that the set S_f contains two distinct points, say, x and y. Let us choose an enclosing sequence $\{\varphi_r\}$ for the set $\{x, y\}$. Then $f(\varphi_r) = 1$. For r large enough we can choose continuous functions ψ_1 and ψ_2 such that $\psi_1(x) = 1$, $\psi_1(y) = 0$, $\psi_2(x) = 0$, and $\psi_2(y) = 1$, $(\psi_1 + \psi_2)^{-1}1 \subset \varphi_r^{-1}1$, and $\operatorname{Supp}\psi_1 \cap \operatorname{Supp}\psi_2 = \varnothing$. Then $f(\psi_1) = f(\psi_2) = 1$ by construction, so $f(\psi_1 + \psi_2) = 2$, which is a contradiction.

We now assume that the set S_f is empty. Then for any point $x \in X$ there is a function $\varphi_x\colon X \to \mathbb{R}$ such that $\varphi_x(x) = 1$ and $f(\varphi_x) = 0$. The open sets $\{y : \varphi_x(y) > 0\}$ cover the space X. Choosing a finite sub-covering of this covering, we take the corresponding set of functions $\varphi_1, \ldots, \varphi_n$. Then the function $\Phi = \varphi_1 + \cdots + \varphi_n$ does not vanish at any point of X; however, $f(\Phi) = f(\varphi_1) + f(\varphi_2) + \cdots + f(\varphi_n) = 0$. We see that, on the one hand, $f\left(\Phi\,\dfrac{1}{\Phi}\right) = f(1) = 1$, and on the other hand, $f\left(\Phi\,\dfrac{1}{\Phi}\right) = f(\Phi)f\left(\dfrac{1}{\Phi}\right) = 0$. This contradiction proves Proposition 6.

Thus, to any ring homomorphism $f\colon C(X) \to \mathbb{C}$ we can assign the ring homomorphism $\widehat{f}\colon C(X) \to \mathbb{C}$, $\widehat{f}(\varphi) = \varphi(x_0)$, where $S_f = \{x_0\}$. To complete the proof of Theorem 1, it remains to show that $\widehat{f} = f$.

Proposition 7. *Let $S_f = \{x_0\}$ and let $\psi\colon X \to \mathbb{C}$ be a continuous function. Then $f(\psi) = \psi(x_0)$.*

Proof. Let $\{\varphi_r\}$ be an enclosing sequence for the set $\{x_0\}$. We consider two cases.

Assume first that $\operatorname{Supp}\psi \cap S_f = \varnothing$. In this case there is an open neighbourhood of the point x_0 on which the function ψ vanishes. Then $\psi\varphi_r = 0$ for any r large enough, and at the same time we have $f(\varphi_r) = 1$. Hence, $f(\psi) = 0$.

Assume now that $x_0 \in \operatorname{Supp}\psi$. Let us consider the function $\theta_r = (\psi - \psi(x_0))\varphi_r$. We have $|\theta_r| \leqslant |\psi - \psi(x_0)|$, and θ_r vanishes outside some neighbourhood of x_0 because of the factor φ_r. Since ψ is continuous, it follows that θ_r tends to zero with respect to the sup norm, and hence $f(\theta_r) \to 0$ as $r \to \infty$. On the other hand, $f(\theta_r) = (f(\psi) - \psi(x_0)f(1))f(\varphi_r) \to (f(\psi) - \psi(x_0))w_f(x_0)$ for r large enough. Hence, $f(\psi) = \psi(x_0)$. This proves Proposition 7.

§ 2. Symmetric products

We recall that by a symmetric product of a space X one means the quotient space

$$\operatorname{Sym}^n(X) = X^n/S_n = \big\{(x_1, \dots, x_n) : (x_{\sigma(1)}, \dots, x_{\sigma(n)}) \sim (x_1, \dots, x_n),\ \sigma \in S_n\big\},$$

where S_n is the group of all permutations of a set with n elements.

The continuous functions on $\operatorname{Sym}^n(X)$ correspond exactly to the continuous functions $f\colon X^n \to \mathbb{C}$ invariant under all permutations of the coordinates, that is, the symmetric functions.

Let us consider an analogue of the evaluation map:

$$\mathcal{E}\colon \operatorname{Sym}^n(X) \to \operatorname{Hom}(C(X), \mathbb{C}), \qquad \mathcal{E}(x_1, \dots, x_n)(\varphi) = \varphi(x_1) + \dots + \varphi(x_n).$$

We shall describe the image of this map by using equations. These equations are given by formulae which were first used by Frobenius [9], [10] and more recently by a number of authors, including Wiles [19], Taylor [18], Hoehnke and Johnson [13], Rouquier [17], and Nyssen [15]. The formulae play an important role in the theory of multivalued groups (see [4]–[6]). We follow the approach developed in [3].

Let A be an associative algebra with unit over the field $\mathbb{C}$ of complex numbers and let $f\colon A \to \mathbb{C}$ be a linear trace-like map (that is, $f(ab) = f(ba)$ for every $a, b \in A$). We introduce linear maps $\Phi_n(f)\colon A^{\otimes n} \to \mathbb{C}$ by setting $\Phi_1(f) = f$, $\Phi_2(f)(a_1 \otimes a_2) = f(a_1)f(a_2) - f(a_1a_2)$, and so on by induction:

$$\begin{aligned}\Phi_{n+1}(f)(a_1 \otimes a_2 \otimes \dots \otimes a_{n+1}) &= f(a_1)\Phi_n(f)(a_2 \otimes \dots \otimes a_{n+1}) \\ &\quad - \Phi_n(f)(a_1a_2 \otimes a_3 \otimes \dots \otimes a_{n+1}) - \dots - \Phi_n(f)(a_2 \otimes a_3 \otimes \dots \otimes a_1a_{n+1}).\end{aligned}$$

We note that a ring homomorphism $f\colon A \to \mathbb{C}$ satisfies the conditions $f(1) = 1$ and $\Phi_2(f) \equiv 0$.

Definition 4. By a *Frobenius n-homomorphism* we mean a linear homomorphism $f\colon A \to \mathbb{C}$ satisfying the conditions $f(1) = n$ and $\Phi_{n+1}(f) \equiv 0$.

Our choice of name for the above homomorphisms is explained by the fact that the recursion formula first arose in the papers [9] and [10] of Frobenius in the case of

group algebras of finite groups. For instance, the following result (in our notation) was obtained in [9].

Let G be a finite group and let $A = \mathbb{C}G$ be its group algebra. Then the character $\chi\colon G \to \mathbb{C}$ of any n-dimensional linear representation of G can be extended to a linear homomorphism $\chi\colon A \to \mathbb{C}$ such that $\chi(1) = n$ and $\Phi_{n+1}(\chi) \equiv 0$.

A generalisation of the Gel'fand–Kolmogorov theorem to the case of symmetric products is given by the following result.

Theorem 8. *Let X be a compact Hausdorff space. Then the image of the map*

$$\mathcal{E}\colon \operatorname{Sym}^n(X) \to \operatorname{Hom}(C(X), \mathbb{C})$$

is exactly the subspace of all Frobenius n-homomorphisms, that is, it is given by the equations $f(1) = n$ and $\Phi_{n+1}(f) \equiv 0$.

A more detailed statement and a constructive proof of this theorem which uses the above technique of enclosing sequences (and enclosing nets in the case of general compact Hausdorff spaces) can be found in [2].

In analogy to Definition 4, one can introduce the notion of Frobenius n-homomorphisms $f\colon A \to B$, where B is an arbitrary commutative algebra. If B has no zero divisors, then the Frobenius n-homomorphisms have properties which are important for our purposes. Therefore, in what follows we assume that B is an integral domain. In [3] the proof of Theorem 8 is obtained as a consequence of a general result characterising Frobenius n-homomorphisms $f\colon A \to B$.

Let A be a commutative algebra. We denote by S^nA the symmetric subalgebra of $A^{\otimes n}$. Every element $a \in S^nA$ can be represented in the form

$$\mathbf{a} = \sum_{\sigma \in S_n} a_{\sigma(1)} \otimes \cdots \otimes a_{\sigma(n)},$$

and the product in S^nA in the form

$$\mathbf{ab} = \sum_{\sigma_1, \sigma_2 \in S_n} a_{\sigma_1(1)} b_{\sigma_2(1)} \otimes \cdots \otimes a_{\sigma_1(n)} b_{\sigma_2(n)}.$$

Theorem 9. *A linear map $f : A \to B$ is a Frobenius n-homomorphism if and only if $f(1) = n$ and the restriction of the homomorphism $\Phi_n(f)\colon A^{\otimes n} \to B$ to S^nA gives a ring homomorphism*

$$\frac{1}{n!}\Phi_n(f)\colon S^nA \to B.$$

We now present a combinatorial result used in an essential way in the proof of this theorem.

Let X be a finite set and let $\mathcal{P}(X)$ be the free Abelian group generated by the set of all partitions of X. We recall that every permutation σ of X determines a partition of X given by the orbits of the action of the subgroup generated by σ. All the permutations determining the same partition have the same sign; for a given

partition π we denote by $\epsilon(\pi)$ the corresponding sign and by $n(\pi)$ the number of permutations generating π. We set

$$\chi(X) = \sum_{\pi} \epsilon(\pi) n(\pi) \pi \in \mathcal{P}(X),$$

where the sum is taken over all partitions of the set X.

Let π_1 and π_2 be partitions of sets X and Y, respectively. Then a natural partition $\pi_1\pi_2$ of the disjoint union $X \sqcup Y$ is defined. Thus, the element $\chi(X)\chi(Y) \in \mathcal{P}(X \sqcup Y)$ is well defined.

If $g\colon X \to Y$ is a surjection and π is a partition of the set Y, then one can take the pre-images of the parts of π and obtain a partition $g^*\pi$; thus, an induced homomorphism $g^*\colon \mathcal{P}(Y) \to \mathcal{P}(X)$ is defined.

If the maps $i_1 \colon X \to Z$ and $i_2 \colon Y \to Z$ are embeddings and if $Z = i_1(X) \cup i_2(Y)$, then we say that (Z, i_1, i_2) is an *amalgamated union* of the sets X and Y. There is a corresponding map $q\colon X \sqcup Y \to Z$, which is surjective.

The following rather unexpected purely combinatorial result was obtained in [3] using polynomials which are solutions of a hypergeometric differential equation.

Lemma 10.

$$\sum q^*\chi(Z) = \chi(X)\chi(Y),$$

where the sum is taken over all distinct amalgamated unions of X and Y, including the disjoint union.

The main steps in the proof of Theorem 9 are as follows.

1. Let $X = (a_1, \dots, a_n)$, where $a_k \in A$. Using the homomorphism $f\colon A \to B$, we define a homomorphism

$$f\colon \mathcal{P}(X) \to B$$

whose value on a partition $\pi = (P_1, \dots, P_k) \in \mathcal{P}(X)$, where $P_i = (a_{i_1}, \dots, a_{i_q})$, is equal to

$$f(\pi) = \prod_{i=1}^{k} f(a_{i_1} \cdots a_{i_q}).$$

Then

$$f(\chi(X)) = \Phi_n(f)(a_1, \dots, a_n).$$

2. Let $X = (a_1, \dots, a_n)$ and $Y = (b_1, \dots, b_n)$ be disjoint sets. It follows from the definitions that

$$f(\chi(X)\chi(Y)) = f(\chi(X))f(\chi(Y)).$$

3. Let $f\colon A \to B$ be an n-homomorphism. Using Lemma 10 we obtain

$$f(\chi(X)\chi(Y)) = \sum_{\sigma \in S_n} f(\chi(X \sqcup_\sigma Y)).$$

Here $Z = X \sqcup_\sigma Y$ stands for an amalgamated union such that Z consists of n elements; in this case, the maps i_1 and i_2 are one-to-one, and therefore Z is determined by some permutation σ.

4. The last step of the proof is to use the relation $\Phi_{n+1}(f) \equiv 0$ to establish the equality

$$\sum_{\sigma \in S_n} \Phi_n(f)(a_1 b_{\sigma(1)}, \dots, a_n b_{\sigma(n)}) = n!\, \Phi_n(f)(\mathbf{ab}).$$

Let us now denote by $\Phi_n(A)$ the set of all Frobenius n-homomorphisms of the ring A to the field $\mathbb{C}$ of complex numbers. By construction, $\Phi_n(A)$ is an algebraic subvariety of the linear space $A^* = \operatorname{Hom}(A, \mathbb{C})$ with the coordinates $a\colon A^* \to \mathbb{C}$, where $a(f) = f(a)$. We set

$$\Phi_n(\mathbb{C}[u_1, \dots, u_m]) = \Phi_n(m).$$

Theorem 11. *The map*

$$\mathcal{E}\colon \operatorname{Sym}^n(\mathbb{C}^m) \to \operatorname{Hom}(\mathbb{C}[u_1, \dots, u_m], \mathbb{C}),$$
$$\mathcal{E}(x_1, \dots, x_n)(p) = p(x_1) + \dots + p(x_n),$$

defines a homeomorphism

$$\mathcal{E}\colon \operatorname{Sym}^n(\mathbb{C}^m) \to \Phi_n(m).$$

Using this result, we present in Appendix B a description of an embedding

$$\operatorname{Sym}^n(\mathbb{C}^m) \subset \mathbb{C}^N, \qquad N = \binom{n+m}{n} - 1,$$

in the context of the theory of multisymmetric polynomials.

Proof. The proof of the fact that the evaluation map $\mathcal{E}$ is an embedding is immediate (see [3]). Let $f\colon \mathbb{C}[u_1, \dots, u_m] \to \mathbb{C}$ be a Frobenius n-homomorphism. Then by Theorem 9, the map

$$\frac{1}{n!}\Phi_n(f)\colon S^n(\mathbb{C}[u_1, \dots, u_m]) \to \mathbb{C}$$

is a ring homomorphism. In what follows, the symmetric algebra $S^n(\mathbb{C}[u_1, \dots, u_m])$ can be identified with the algebra of polynomial functions on the algebraic variety $\operatorname{Sym}^n(\mathbb{C}^m)$, that is, with the algebra of multisymmetric polynomials. Then, by Hilbert's Nullstellensatz, there is an n-tuple $(x_1, \dots, x_n) \in \operatorname{Sym}^n(\mathbb{C}^m)$ such that for $a = \sum_{\sigma \in S_n} p_{\sigma(1)} \otimes \dots \otimes p_{\sigma(n)}$ we have the formula

$$a(x_1, \dots, x_n) = \sum_{\sigma \in S_n} p_{\sigma(1)}(x_1) \otimes \dots \otimes p_{\sigma(n)}(x_n).$$

Let us take for a the element

$$a = p \otimes 1 \otimes \dots \otimes 1 + 1 \otimes p \otimes \dots \otimes 1 + \dots + 1 \otimes 1 \otimes \dots \otimes p,$$

where $p \in \mathbb{C}[u_1, \dots, u_m]$. Then

$$\frac{1}{n!}\Phi_n(f)(p) = \sum_{k=1}^{n} p(x_k).$$

On the other hand, using the fact that the homomorphism $\Phi_n(f)$ is linear and symmetric and applying the formula

$$\Phi_n(f)(p \otimes 1 \otimes \cdots \otimes 1) = f(p)(f(1) - 1) \cdots (f(1) - (n-1))$$

(see [3]), we obtain

$$\frac{1}{n!}\Phi_n(f)(a) = f(p)$$

because $f(1) = n$, that is, $f(p) = \sum_{k=1}^{n} p(x_k)$, and hence $f = \mathcal{E}(x_1, \dots, x_n)$. This completes the proof of Theorem 11.

Theorem 12. *Let A be a finitely generated commutative algebra and let V be the affine algebraic variety* m-Spec(A). *Then the map*

$$\mathcal{E}\colon \operatorname{Sym}^n(V) \to \operatorname{Hom}(A, \mathbb{C}),$$
$$\mathcal{E}(f_1, \dots, f_n)(a) = f_1(a) + \cdots + f_n(a),$$

where $f_k\colon A \to \mathbb{C}$, $k = 1, \dots, n$, are ring homomorphisms (whose kernels are maximal ideals, which are the points of V), defines a homeomorphism

$$\mathcal{E}\colon \operatorname{Sym}^n(V) \to \Phi_n(A).$$

For a detailed proof of this result, see [3].

The proof of Theorem 8 using Theorem 9 can be carried out by the scheme of the proof of Theorem 11. One must also use the fact that for a compact Hausdorff space X the ring $C(X)^{\otimes n}$ is dense in the ring $C(X^n)$ by the Stone–Weierstrass theorem (for the details, see [16], Proposition 1.10.21), and therefore the ring $S^n(C(X))$ is dense in the ring $C(\operatorname{Sym}^n(X))$. This enables one to use the Gel'fand–Kolmogorov theorem and get a point of the space $\operatorname{Sym}^n(X)$ correponding to the ring homomorphism $\frac{1}{n!}\Phi_n(f)\colon S^n(C(X)) \to \mathbb{C}$.

§ 3. Properties of n-homomorphisms

The results of the previous section show that Frobenius n-homomorphisms of commutative algebras have important applications. Thus, the study of the properties of these homomorphisms in this special case arose naturally. It turns out that in this investigation it is useful to apply another description of the defining equations, which was given in [4], [5].

Let A be a commutative algebra. Then the following assertions hold.

1. The value $\Phi_n(a, \dots, a) := \Phi_n(f)(a \otimes \cdots \otimes a)$, where $a \in A$, is equal to the determinant of the matrix

$$\begin{pmatrix} f(a) & 1 & 0 & 0 & \cdots & 0 \\ f(a^2) & f(a) & 2 & 0 & \cdots & 0 \\ f(a^3) & f(a^2) & f(a) & 3 & & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \\ \vdots & \vdots & & & f(a) & n-1 \\ f(a^n) & f(a^{n-1}) & \cdots & \cdots & f(a^2) & f(a) \end{pmatrix}.$$

2. The value $\Phi_n(f)(a_1,\dots,a_n)=\Phi_n(f)(a_1\otimes\cdots\otimes a_n)$ is a multilinear function of the variables $a_1,\dots,a_n$ and can therefore be obtained from $\Phi_n(a,\dots,a)$ by the standard polarisation procedure.

3. Let us represent a permutation $\sigma\in S_n$ as a product of disjoint cycles of total length n, say, $\sigma=\gamma_1\cdots\gamma_r$. Let $\gamma=(i_1,\dots,i_m)$ be a cycle. We set $f_\gamma(a_1,\dots,a_n)=f(a_{i_1}\cdots a_{i_m})$. Then the following formula holds:

$$\Phi_n(f)(a_1,\dots,a_n)=\sum_{\sigma\in S_n}\varepsilon(\sigma)f_{\gamma_1}(a_1,\dots,a_n)\cdots f_{\gamma_r}(a_1,\dots,a_n),\qquad(3.1)$$

where $\varepsilon(\sigma)$ is the sign of the permutation σ.

For instance,

$$\begin{aligned}\Phi_3(f)(a_1,a_2,a_3)&=f(a_1)f(a_2)f(a_3)-f(a_1)f(a_2a_3)\\&\quad-f(a_2)f(a_1a_3)-f(a_3)f(a_1a_2)+2f(a_1a_2a_3).\end{aligned}$$

We note that the formula (3.1) also holds in the case of trace-like homomorphisms f of a non-commutative algebra A. This formula arose in [7] in the case of matrix algebras A and the trace homomorphism f.

It is often simpler to work with the formula (3.1) in its 'diagonal' form and then to use polarisation to obtain general formulae. For instance, $\Phi_3(f)(a,a,a)=s_1^3-3s_1s_2+2s_3$, where $s_1=f(a)$, $s_2=f(a^2)$, and $s_3=f(a^3)$. We use the notation s_k to stress the connection with the classical Newton formula expressing the elementary symmetric functions $e_n=\sum t_{i_1}\cdots t_{i_n}$ of the commuting variables $t_1,t_2,\dots$ (the sum is taken over all sets $I_n=(i_1<\cdots<i_n)$) as polynomials in the power sums $s_k=\sum t_i^k$,

$$n!\,e_n=\det\begin{pmatrix}s_1&1&0&0&\cdots&0\\s_2&s_1&2&0&\cdots&0\\s_3&s_2&s_1&3&&0\\\vdots&\vdots&\ddots&\ddots&\ddots&\\\vdots&\vdots&&&s_1&n-1\\s_n&s_{n-1}&\cdots&\cdots&s_2&s_1\end{pmatrix}.$$

Let us now describe the development of this connection, denoting by F_n the polynomial in the variables s_k, $k=1,\dots,n$, which becomes equal to $\Phi_n(f)(a,\dots,a)$ under the substitution $s_k=f(a^k)$. The formula

$$F_n=\sum_{\sigma\in S_n}\Big(\prod_{k=1}^{n}((-1)^{k+1}s_k)^{m_k(\sigma)}\Big),$$

where $m_k(\sigma)$ is the number of cycles of length $k\geqslant 1$ in the decomposition of the permutation σ into a product of disjoint cycles, follows immediately from the definition of the polynomial $F_n(s_1,\dots,s_n)$. Further, the number of elements of the group S_n with m_k cycles of length k is equal to

$$n!\Big/\prod_{k=1}^{n}(k^{m_k}m_k!).$$

Hence,

$$F_n = \sum_{\mathbf{m}\in\Pi(n)} \prod_{k=1}^{n} \left((-1)^{k+1}\frac{s_k}{k}\right)^{m_k},$$

where $\Pi(n)$ denotes the set of partitions of the number n and $\mathbf{m} = (m_1, \dots, m_n)$ is the partition of n with m_k the multiplicity of k in this partition. Thus, $\sum_{k=1}^{n} km_k = n$. Therefore,

$$F_n t^n = \sum_{\mathbf{m}\in\Pi(n)} \prod_{k=1}^{n} \left((-1)^{k+1}\frac{s_k t^k}{k}\right)^{m_k},$$

and we obtain the following assertion.

Theorem 13.

$$\sum_{n=0}^{\infty} F_n \frac{t^n}{n!} = \exp\left(\sum_{k=1}^{\infty} (-1)^{k+1} s_k \frac{t^k}{k}\right).$$

This result implies the following recursion.

Proposition 14.

$$F_n = (n-1)! \sum_{k=1}^{n} (-1)^{k+1} s_k \frac{F_{n-k}}{(n-k)!}\,.$$

Proof. We set

$$F(t) = \sum_{n=0}^{\infty} F_n \frac{t^n}{n!}\,.$$

Then Theorem 13 implies the relation

$$F'(t) = F(t)(s_1 - s_2 t + s_3 t^2 - \cdots),$$

which immediately implies the desired formula.

Let us now give a characterisation of the polynomials F_n using differential operators.

Lemma 15.

Let $d = \sum_{r=2}^{\infty} r s_{r-1} \dfrac{\partial}{\partial s_r}$. *Then the following assertions hold*:

(a) $\dfrac{\partial F_n}{\partial s_1} = nF_{n-1}$;

(b) $dF_n = -n(n-1)F_{n-1}$;

(c) $\left[\dfrac{\partial}{\partial s_k}, d\right] = (k+1)\dfrac{\partial}{\partial s_{k+1}}$;

(d) $\left(\operatorname{Ker}\dfrac{\partial}{\partial s_1}\right) \cap (\operatorname{Ker} d)$ *consists entirely of constants.*

Proof. (a) Differentiating the right-hand side of the relation in Theorem 13 with respect to s_1, we obtain $\dfrac{\partial F(t)}{\partial s_1} = tF(t)$. Hence,

$$\sum_{n=0}^{\infty} \frac{\partial F_n}{\partial s_1}\frac{t^n}{n!} = t\sum_{n=0}^{\infty} F_n \frac{t^n}{n!}\,.$$

Equating the coefficients of like powers of t, we obtain the result in (a).

(b) Applying the operator d to the same relation, we obtain

$$dF(t) = F(t)[-s_1t^2 + s_2t^3 - s_3t^4 + \cdots] = -t^2F'(t).$$

Equating the coefficients of t^n, we obtain

$$\frac{dF_n}{n!} = -\frac{F_{n-1}}{(n-2)!}\,.$$

(c) $d\dfrac{\partial}{\partial s_k} - \dfrac{\partial}{\partial s_k}d = \displaystyle\sum_{r=2}^{\infty} r s_{r-1}\frac{\partial}{\partial s_r}\frac{\partial}{\partial s_k} - \frac{\partial}{\partial s_k}\sum_{r=2}^{\infty} r s_{r-1}\frac{\partial}{\partial s_k} = (k+1)\frac{\partial}{\partial s_{k+1}}.$

(d) Let $\dfrac{\partial f}{\partial s_1} = 0$. Then $f = f(s_2, s_3, \dots)$. If f belongs to the intersection of the kernels of the operators $\dfrac{\partial}{\partial s_1}$ and d, then $\dfrac{\partial}{\partial s_2}f = 0$ by assertion (c). Assertion (c) enables us to complete the proof of the result (d) by induction.

Lemma 15 immediately implies the following result.

Theorem 16. *The sequence $\{F_n(s_1, \dots, s_n)\}$ of polynomials is completely characterised by the properties*

0) $F_n(0) = 0$, $n = 1, 2, \dots$,
1) $F_0 = 1$,
2) $\dfrac{\partial F_n}{\partial s_1} = nF_{n-1}$,
3) $dF_n = -n(n-1)F_{n-1}$,

that is, the generating function $F(t) = F(t; s_1, s_2, \dots)$ is the unique solution of the system of equations

$$\frac{\partial}{\partial s_1}F(t) = tF(t),$$
$$dF(t) = -t^2\frac{\partial}{\partial t}F(t)$$

under the initial condition $F(0; s_1, s_2, \dots) = 1$.

§ 4. Frobenius algebras

Let A be an associative algebra over $\mathbb{C}$. A linear map $f\colon A \to \mathbb{C}$ is said to be *trace-like* if $f(ab) = f(ba)$ for any a and b in A.

Definition 5. By a *Frobenius algebra* we mean an algebra A together with a trace-like linear map $f\colon A \to \mathbb{C}$ such that the bilinear form

$$A \times A \to \mathbb{C}, \qquad (a, b) \mapsto f(ab)$$

is non-degenerate.

We denote by $J(A)$ the Jordan algebra with the additive structure of A and with the product

$$a \circ b = \frac{1}{2}(ab + ba).$$

Let us consider a basis $\{e_i\colon i \in I\}$ for A and denote the corresponding structure constants by a_{ij}^k (that is, $e_i e_j = \sum a_{ij}^k e_k$). Then the numbers $a_{(ij)}^k = \frac{1}{2}(a_{ij}^k + a_{ji}^k)$ are the structure constants of the Jordan algebra $J(A)$ with respect to the same basis.

Theorem 17. *Let (A, f) be a Frobenius algebra. Then the structure constants of the Jordan algebra $J(A)$ are completely determined by the homomorphisms $\Phi_k = \Phi_k(f)$, $k = 1, 2, 3$.*

A result related to Theorem 17 was obtained in [12] under other assumptions. The theorem includes an assertion similar to the conclusion of Theorem 2.8 in [3], and therefore seems to give a stronger result.

Corollary 18. *For a given homomorphism $f\colon A \to \mathbb{C}$ the linear maps $\Phi_k = \Phi_k(f)\colon A^{\otimes k} \to \mathbb{C}$, $k \geqslant 4$, are determined by the maps Φ_1, Φ_2, Φ_3.*

Corollary 18 implies the well-known result of [13] that a finite group is completely determined by its Frobenius k-characters for $k = 1, 2, 3$.

Proof of Theorem 17. By definition,

$$\Phi_2(e_i, e_j) = f(e_i)f(e_j) - f(e_i e_j).$$

We set $R_{ij} = f(e_i e_j)$. Then

$$R_{ij} = \sum_r a_{ij}^r f(e_r) = f(e_i)f(e_j) - \Phi_2(e_i, e_j). \tag{4.1}$$

Similarly,

$$\begin{aligned}\Phi_3(e_i, e_j, e_k) = f(e_i)f(e_j)f(e_k) &- f(e_i)\sum_r a_{jk}^r f(e_r) \\ &- f(e_j)\sum_r a_{ik}^r f(e_r) - f(e_k)\sum_r a_{ij}^r f(e_r) \\ &+ \sum_{r,s}(a_{ij}^r + a_{ji}^r)a_{rk}^s f(e_s).\end{aligned}$$

Hence,

$$\begin{aligned}\sum(a_{ij}^r + a_{ji}^r)R_{rk} = f(e_i)R_{jk} + f(e_j)R_{ik} + f(e_k)R_{ij} \\ - f(e_i)f(e_j)f(e_k) + \Phi_3(e_i, e_j, e_k).\end{aligned} \tag{4.2}$$

It follows from the definition of the Frobenius algebra that the matrix $R_{ij} = f(e_ie_j) = \sum_r a_{ij}^r f(e_r)$ is symmetric and non-degenerate. Regarding the equation (4.2) for fixed i and j as a system of linear equations with respect to the vector $(a_{(ij)}^r,\ r = 1,\dots,n)$, we see that this system has a unique solution. The proof of the theorem is complete.

A more explicit answer can be obtained for a commutative Frobenius algebra A. We set

$$R_i = f(e_i), \qquad R_{ij} = f(e_ie_j), \qquad R_{ijk} = f(e_ie_je_k).$$

In terms of the values of the homomorphisms Φ_2 and Φ_3 we obtain

$$\begin{aligned} R_{ij} &= \Phi_2(e_i,e_j) - R_iR_j,\\ 2R_{ijk} &= \Phi_3(e_i,e_j,e_k) + R_iR_{jk} + R_jR_{ik} + R_kR_{ij} - R_iR_jR_k. \end{aligned}$$

The matrix R_{ij} is invertible by the definition of Frobenius algebra. We denote by R^{ij} the matrix inverse to R_{ij}. Direct calculations give the following explicit formula for the structure constants of the algebra A.

Proposition 19. *The structure constants of a commutative Frobenius algebra are given by the formula*

$$a_{ij}^k = \sum_m R_{ijm}R^{mk}.$$

Proof. Using the formula

$$R_{ijk} = f(e_ie_je_k) = \sum_n f(a_{ij}^n e_ne_k),$$

we obtain

$$\sum_m R_{ijm}R^{mk} = \sum_{m,n} a_{ij}^n R_{nm}R^{mk} = a_{ij}^k.$$

Proof of Corollary 18. It suffices to prove that, to compute the values of the homomorphism Φ_k, one needs the structure constants $a_{(ij)}^k$ and not a_{ij}^k. We use induction.

In the expansion of $\Phi_m(e_1,\dots,e_m)$ in terms of the values of the homomorphism f the only summand which cannot be immediately expressed by using the values of Φ_r with $r < m$ is

$$\sum_{\sigma\in S_{m-1}} f(e_1e_{\sigma(2)}e_{\sigma(3)}\cdots e_{\sigma(m)}) = \frac{1}{m}\sum_{\sigma\in S_m} f(e_{\sigma(1)}e_{\sigma(2)}\cdots e_{\sigma(m)}).$$

The multiplication in the Jordan algebra $J(A)$ may not be associative, but the associator can be expressed in terms of commutators, namely,

$$\begin{aligned} 4((a\circ b)\circ c - a\circ(b\circ c)) &= abc + bac + cab + cba - abc - acb - bca - cba\\ &= [b,ac] - [b,ca] = [b,[a,c]]. \end{aligned}$$

Since f is trace-like, it follows that $f([a,b])=0$, and we see that

$$f((a\circ b)\circ c)=f(a\circ(b\circ c)).$$

Hence, on iterated products of elements of $J(A)$ the homomorphism f behaves as if this algebra is associative. Thus,

$$2^{m-1}\sum_{\sigma\in S_m} f(e_{\sigma(1)}\cdots e_{\sigma(m)})=\sum_{\sigma\in S_m} f(e_{\sigma(1)}\circ\cdots\circ e_{\sigma(m)}).$$

In the case of finite groups we obtain the following result.

Let G be a finite group with the set $\{g_1,\dots,g_n\}$ of elements. We consider the Frobenius algebra $\mathbb{C}G$ with the structure map $f=\frac{1}{n}\chi\colon \mathbb{C}G\to\mathbb{C}$, where χ is the character of the regular representation of G.

Corollary 20. *The linear maps $\Phi_1=f$, Φ_2, and Φ_3 determine the following parts of the structure of the group algebra $\mathbb{C}G$:*

1) *Φ_1 determines the identity element e of G;*
2) *Φ_2 determines inverse elements, that is, it distinguishes the pairs (g_i,g_j) such that $g_ig_j=e$;*
3) *Φ_1, Φ_2, and Φ_3 determine the structure constants of the Jordan algebra $J(\mathbb{C}G)$.*

Proof. The character χ of the regular representation takes the value n at the identity element e of G and the value 0 at any other element, and this obviously implies the assertion 1), because $\Phi_1=f=\frac{1}{n}\chi$. Further, it follows from (4.1) that

$$\Phi_2(h,g)=\begin{cases}-1 & \text{if } hg=e,\ h\neq e;\\ 0 & \text{otherwise.}\end{cases}$$

We thus find the pairs of mutually inverse elements. Let us rewrite this result in terms of structure constants. We order the elements of G in such a way that $g_1=e$ and we write $g_ig_j=\sum_{k=1}^n a_{ij}^k g_k$. In the case under consideration the quantities a_{ij}^k take the values 0 and 1, and $\sum_{k=1}^n a_{ij}^k=1$ for any pair (i,j). Assertion 1) means that

$$a_{i1}^k=a_{1i}^k=\delta_{ik}.$$

Assertion 2) recovers the values

$$a_{ij}^1=-\Phi_2(g_i,g_j)\quad\text{if}\quad i+j>2.$$

We now find the information about the structure constants a_{ij}^k that is determined by the map Φ_3. By (4.2) we have

$$\Phi_3(g_i,g_j,g_k)=\sum_r(a_{ij}^r+a_{ji}^r)a_{rk}^1\quad\text{if}\quad i+j+k>3.$$

We know that the matrix $a_{r,k}^1$ is invertible, which enables us to complete the proof.

Theorem 21. *Let G be a finite group and let χ be the character of the regular representation of G. The linear maps χ, $\Phi_2(\chi)$, and $\Phi_3(\chi)$ determine the group G uniquely up to isomorphism.*

Proof. Using Corollary 20, we see immediately that the homomorphisms χ, $\Phi_2(\chi)$, and $\Phi_3(\chi)$ determine the multiplication on the set of elements of the group G up to permutation of the factors.

The following lemma and the fact that that a group is isomorphic to its opposite (using the map $g \mapsto g^{-1}$) enables one to complete the proof of this theorem.

Lemma 22 (Mansfield [14]). *Let G be a finite group in which the multiplication rule is not known precisely but the set $\{gh, hg\}$ is known for each pair of elements $g, h \in G$. Then one can recover the set $\{m, m^{\mathrm{op}} \colon G \times G \to G\}$ of functions, where $m(x, y) = xy$ and $m^{\mathrm{op}}(x, y) = yx$.*

The proof of this lemma presented in [14] uses an elementary (but tricky) examination of all cases. For completeness of the exposition, we present a somewhat simplified proof in Appendix A (§ 5).

In [14] this lemma was used to prove the result of Formanek and Sibley [8] that the group determinant of a finite group (which was first considered by Dedekind) determines the group.

The group determinant of a group G is defined as follows.

Choose a one-to-one correspondence between the set $\{g_1, \dots, g_n\}$ of elements of G, where $g_1 = e$, and the set $\{x_1, \dots, x_n\}$ of commuting variables. The group determinant is the determinant of the matrix obtained from the multiplication table of the group by the substitution $g_i \to x_i$. The group determinant is a homogeneous polynomial of degree n in $\{x_1, \dots, x_n\}$ with integral coefficients.

We introduce the matrix $M_G = (m_{ij} = x_k)$, where the correspondence $(i, j) \to k$ is given by $g_i g_j^{-1} = g_k$. It is clear that M_G differs from the multiplication table only by the order of the columns, and hence $D_G = \pm \det M_G$. We note that $\det M_G = x_1^n + \cdots$.

Let us consider the n-dimensional linear space $\mathbb{C}^n \simeq \mathbb{C}G$ and the right regular representation of the group G in the basis $\{g_1, \dots, g_n\}$:

$$T \colon \mathbb{C}^n \to \mathbb{C}^n, \qquad T(g)g_k = g_k g^{-1}.$$

Denote by T_i the matrix of the action of the operator $T(g_i)$ in this basis. Then

$$M_G = \sum x_i T_i.$$

We consider the character

$$\chi \colon \mathbb{C}G \to \mathbb{C}$$

of the representation T and extend it to a linear $\mathbb{C}[x_1, \dots, x_n]$-homomorphism

$$f \colon \mathbb{C}G[x_1, \dots, x_n] \to \mathbb{C}[x_1, \dots, x_n].$$

Lemma 23. *Let* $a = \sum_{i=1}^{n} x_i g_i \in \mathbb{C}G[x_1, \dots, x_n]$. *Then*

$$\Phi_n(f)(a, \dots, a) = D_G.$$

The famous expansion of the group determinant into irreducible factors obtained by Frobenius in [10] can be obtained immediately from the expansion of the regular representation T into irreducible representations: *let* $\chi = \chi_1 + \dots + \chi_q$ *be an expansion of the regular representation* T *into irreducible representations and let* n_i *be the dimension of the representation with character* χ_i; *then*

$$D_G = \prod_{i=1}^{q} \Phi_{n_i}(\chi_i)^{n_i}.$$

§ 5. Appendix A. Proof of Mansfield's lemma

As we promised, we give here a new proof of the following result.

Lemma 24. *Let* G *be a group with the multiplication* $(x, y) \to xy$. *If* $*$ *is an associative multiplication on* G *related to the original multiplication in such a way that for each pair* $x, y \in G$ *the product* $x * y$ *is equal to either* xy *or* yx, *then* $x * y = xy$ *for all* $x, y \in G$ *or* $x * y = yx$ *for all* $x, y \in G$.

We reformulate the lemma as follows. Let $A = \{(x, y) : x * y = xy\}$ and $B = \{(x, y) : x * y = yx\}$. Then it follows from the conditions of the lemma that $A \cup B = G \times G$, and one must prove that $A = G \times G$ or $B = G \times G$. It is clear that the set $A \cap B$ is symmetric.

The proof of the lemma follows Exercise 26 in § 4 of [1]. For a given pair $x, y \in G$ we have the following assertion.

Fact 25. $x * y = y * x \iff xy = yx$.

The implication $xy = yx \implies x * y = y * x$ is obvious. In the converse direction, let $x * y = y * x$. Then without loss of generality one can set $x * y = xy$. If this is not the case, then $y * x = x * y = yx$, and we can transpose the variables x and y.

In what follows we assume that $xy \neq yx$, because otherwise there is nothing to prove. Let us consider the element $x * x * y = x^2 * y$ and assume that it differs from x^2y. At the same time it follows from the above that $x * x * y = x * xy$ is equal to xyx or x^2y. Thus, $yx^2 = xyx$, and hence $yx = xy$. The contradiction shows that $x * x * y = x^2y$.

We have $x * y * x * y = xy * xy = (xy)^2$. On the other hand, by assumption the element $x * y * x * y = x * x * y * y = x^2y * y$ is equal to x^2y^2 or yx^2y, that is, $(xy)^2 = x^2y^2$ or $(xy)^2 = yx^2y$. In both the cases we arrive at the relation $xy = yx$, which is a contradiction.

Corollary 26. $x * y = xy \iff y * x = yx$, *that is, the set* A *is symmetric.*

Proof. Let $x * y = xy$ and $y * x = xy$. Then it follows from Fact 25 that $xy = yx$. Thus, $x * y = xy \implies y * x = yx$. The converse implication follows by symmetry.

Since both the sets A and $A \cap B$ are symmetric and $A \cup B = G \times G$, we immediately see that B is a symmetric set. Thus, we have proved the following assertion.

Corollary 27. $x * y = yx \Longleftrightarrow y * x = xy$.

Fact 28. *$x * y * x = xyx$ for every $x, y \in G$.*

Proof. If $xy = yx$, then $x * y * x = xy * x = xyx$ or x^2y. The desired relation holds because $xyx = x^2y$. On the other hand, suppose that $xy \neq yx$ and $x * y * x \neq xyx$. Then only the following two cases are possible.

a) $x * y = xy$ and $y * x = yx$. Then $x * y * x = xy * x = x^2y$ or xyx. Since the multiplication is associative, it follows that $x * y * x = x * yx$ is equal to xyx or yx^2. Thus, $x * y * x = x^2y = yx^2$. Moreover, $x * x * y = x^2 * y = x^2y = x * y * x$. Hence, $x * y = y * x$, which contradicts our assumptions.

b) $x * y = yx$ and $y * x = xy$. We again have $x * y * x = yx * x = yx^2$ and $x * y * x = x * xy = x^2y$. Thus, $x * x * y = x * y * x$ and $x * y = y * x$. This contradiction completes the proof of Fact 28.

We now regard $G \times G$ as a square array with rows $R_x = \{(x, y) : y \in G\}$.

Fact 29. *For each $x \in G$ either $R_x \subset A$ or $R_x \subset B$.*

Proof. Suppose that Fact 29 fails. Then there is an element x such that R_x intersects both the sets $G \times G \setminus A$ and $G \times G \setminus B$, that is, there are elements $y, z \in G$ such that $x * y = yx \neq xy = y * x$ and $x * z = xz \neq zx = z * x$. Let us show that under these assumptions we have $yxz = zxy$. Two cases are possible here.

a) $y * z \neq z * y$. As was shown above, in this case $yz \neq zy$. The element $z * x * y$ is equal to either zxy or yzx. This element is also equal to $z * yx = zyx$ or yxz. However, $yzx \neq zyx$, $yzx \neq yxz$, and $zxy \neq zyx$, and thus $z * x * y = zxy = yxz$.

b) $y * z = z * y$ $(= yz = zy)$. We show that the assumption $yxz \neq zxy$ leads to a contradiction. Consider the element $z * x * y$. It is equal to $zx * y$, which equals yzx or zxy, but it is also equal to $z * yx = zyx$ or yxz. Under our assumptions and using the facts that $zxy \neq zyx$ and $yzx \neq yxz$, we obtain $z * x * y = yzx = zyx$. Now consider the element $x * z * y$. It differs from $z * x * y = yzx$. However, it is equal to $x * y * z = x * yz = xyz$ or to yzx. Hence, $x * z * y = xyz = xzy$. Finally, consider the element $z * y * x$. It differs from $z * x * y = yzx$ and is equal to $yz * x = xyz$ or yzx. Hence, $z * y * x = xyz = xzy$. Thus, $x * (z * y) = (z * y) * x$, that is, $x * zy = zy * x$, and therefore $xzy = zyx$. This implies that $z * x * y = x * z * y$, and thus contradicts the condition $x * z \neq z * x$.

Let us finally consider the element $x * z * x * y$. According to Fact 28, it is equal to $xzx * y = xzxy$ or $yxzx$. On the other hand, it is equal to $xz * yx = xzyx$ or $yxxz$. We must again consider two cases.

a) $x * z * x * y = xzxy$ is equal to $xzyx$ or $yxxz$. In the first case we obtain $xy = yx$. The second case, together with the above calculations, gives $yxxz = xzxy = xyxz$, which gives $xy = yx$. So in both cases we get that $xy = yx$, which is a contradiction.

b) $x * z * x * y = yxzx$ is equal to $xzyx$ or $yxxz$. In the second case we have $xz = zx$, that is, a contradiction. Thus, $xzyx = yxzx = zxyx$, which also gives $xz = zx$. This completes the proof of Fact 29.

According to Fact 29, for every x we have either $R_x \subset A$ or $R_x \subset B$. Suppose that $R_x \subset A$ but $R_x \not\subset B$, and that $R_u \subset B$ but $R_u \not\subset A$. Then $x * y = xy$ for any y, and there is a z such that $xz \neq zx$. Similarly, $u * v = vu$ for any v, and there is a w such that $uw \neq wu$.

Consider the element $x*u = xu$. It is equal to $ux = u*x$, and R_{xu} is a subset of A or B. Suppose that $R_{xu} \subset A$. We then consider the element $x*u*w = xu*w = xuw$, which must also be equal to $x*wu = xwu$, a contradiction. We now assume that $R_{xu} \subset B$ and consider the element $z*x*u = z*xu = xuz = uxz$, which is also equal to $zx*u = uzx$. This implies that $xz = zx$, a contradiction. This proves Mansfield's lemma.

§ 6. Appendix B. The algebra of multisymmetric polynomials

Let $n>1$. We recall that a polynomial $p(x_1,\dots,x_n)$, where $x_k=(x_{1k},\dots,x_{mk}) \in \mathbb{C}^m$, is said to be multisymmetric if it is invariant with respect to all permutations of the set of arguments $(x_1,\dots,x_n)$. The algebra of polynomial functions on the algebraic variety $\operatorname{Sym}^n(\mathbb{C}^m)$ can be canonically identified with the algebra of multisymmetric polynomials, which we denote by $\mathcal{SP}^n(\mathbb{C}^m)$. For each tuple $\omega=(i_1,\dots,i_m)$ of non-negative integers we introduce the multisymmetric Newton polynomials p_ω,

$$p_\omega(x_1,\dots,x_n) = \sum_{k=1}^{n} x_{1k}^{i_1}\cdots x_{mk}^{i_m};$$

for $m=1$ these are the classical Newton polynomials.

We set $|\omega| = i_1+\dots+i_m$. Let $\{z_\omega\}$, $\omega \in \mathbb{Z}^m_{\geqslant 0}$, be a set of commuting variables graded by the rule $\deg z_\omega = |\omega|$. We consider the graded polynomial ring $L=\mathbb{C}[z_\omega]$ and introduce in L a system $\{\mathcal{F}_{\omega_1,\dots,\omega_j}\}$ of homogeneous polynomials, $\deg \mathcal{F}_{\omega_1,\dots,\omega_j} = |\omega_1|+\dots+|\omega_j|$, by the 'Frobenius-type' formulae

$$\mathcal{F}_{\omega_1} = z_{\omega_1}, \quad \mathcal{F}_{\omega_1,\omega_2} = z_{\omega_1}z_{\omega_2} - z_{\omega_1+\omega_2}, \quad \text{and by recurrence:}$$
$$\mathcal{F}_{\omega_1,\dots,\omega_{j+1}} = z_{\omega_1}\mathcal{F}_{\omega_2,\dots,\omega_{j+1}} - \mathcal{F}_{\omega_1+\omega_2,\omega_3,\dots,\omega_{j+1}} - \dots - \mathcal{F}_{\omega_2,\dots,\omega_j,\omega_1+\omega_{j+1}}.$$

Following the above scheme (See § 3), one can readily obtain an explicit expression for the polynomial $\mathcal{F}_{\omega_1,\dots,\omega_j}$. In what follows it will be important that the linear part of the polynomial $\mathcal{F}_{\omega_1,\dots,\omega_j}$ is equal to $(-1)^{(j-1)}(j-1)!\, z_{\omega_1+\dots+\omega_j}$.

The fact that the ring L can be canonically identified with the polynomial ring on the linear space $\operatorname{Hom}(\mathbb{C}[u_1,\dots,u_m],\mathbb{C})$ enables us to pass to the homomorphism of polynomial rings that is induced by the evaluation map $\mathcal{E}$, and we obtain the following result from Theorem 11.

Theorem 30. *For given n and m the ring homomorphism*

$$\mathcal{E}^*\colon L \to \mathcal{SP}^n(\mathbb{C}^m)$$

is an epimorphism.

Let $\mathcal{SYZ}(m,n)$ be the kernel of the homomorphism $\mathcal{E}^*$. Then $\mathcal{SYZ}(m,n)$ is the ideal of L generated by the polynomials $\mathcal{F}_{\omega_1,\dots,\omega_{n+1}}$ such that $|\omega_1|,\dots,|\omega_{n+1}|>0$.

Consider the subring $L_n \subset L$ generated by the elements $\{z_\omega\}$ with $|\omega|<n+1$. Using the above form of the linear part of the polynomial $\mathcal{F}_{\omega_1,\dots,\omega_{n+1}}$, we obtain the following assertion.

Corollary 31. *The restriction of the homomorphism $\mathcal{E}^*$ to L_n gives an epimorphism*

$$\mathcal{E}_n^*\colon L_n \to \mathcal{SP}^n(\mathbb{C}^m).$$

Let $\operatorname{Syz}(m,n)$ *be the kernel of the homomorphism $\mathcal{E}_n^*$. Then*

$$\operatorname{Syz}(m,n) = \mathcal{SYZ}(m,n) \cap L_n.$$

By construction, L_n is the polynomial ring on $\mathbb{C}^N$, where $N = \binom{n+m}{n} - 1$. We obtain the following assertion.

Corollary 32.

$$\operatorname{Sym}^n(\mathbb{C}^m) \sim \operatorname{Spec}\bigl(L_n/\operatorname{Syz}(n,m)\bigr) \subset \mathbb{C}^N.$$

In conclusion we note that the assertion that the homomorphism $\mathcal{E}^*$ is onto is equivalent to the first fundamental theorem of the classical theory of invariants, which claims that a multisymmetric polynomial in n vector arguments can be expressed (though not uniquely) as a polynomial in the multisymmetric Newton polynomials p_ω, $|\omega| \leqslant n$. The classical case $m = 1$ is the only case in which this expression is unique.

Bibliography

[1] N. Bourbaki, *Éléments de Mathématique. Algèbre*, Chapitres I–III, Hermann, Paris 1970.

[2] V. M. Buchstaber and E. G. Rees, "A constructive proof of the generalised Gel'fand isomorphism", *Funktsional. Anal. i Prilozhen.* **35**:4 (2001), 20–25; English transl., *Funct. Anal. Appl.* **35** (2001), 257–260.

[3] V. M. Buchstaber and E. G. Rees, "The Gel'fand map and symmetric products", *Selecta Math.* (N.S.) **8** (2002), 523–535.

[4] V. M. Buchstaber and E. G. Rees, "Multivalued groups, their representations and Hopf algebras", *Transform. Groups* **2** (1997), 325–349.

[5] V. M. Buchstaber and E. G. Rees, "Multivalued groups, n-Hopf algebras and n-ring homomorphisms", Lie Groups and Lie Algebras, (Math. Appl., vol. 433) Kluwer, Dordrecht 1998, pp. 85–107.

[6] V. M. Buchstaber and E. G. Rees, "Frobenius k-characters and n-ring homomorphisms", *Uspekhi Mat. Nauk* **52**:2 (1997), 159–160; English transl., *Russian Math. Surveys* **52** (1997), 398–399.

[7] E. Formanek, *The polynomial identities and invariants of $n \times n$ matrices*, Amer. Math. Soc., Providence, RI 1991.

[8] E. Formanek and D. Sibley, "The group determinant determines the group", *Proc. Amer. Math. Soc.* **112** (1991), 649–656.

[9] G. Frobenius, "Über Gruppencharaktere", *Sitzungsber. Preuß. Akad. Wiss. Berlin* **1896**, 985–1021.

[10] G. Frobenius, "Über die Primfaktoren der gruppendeterminante", *Sitzungsber. Preuß. Akad. Wiss. Berlin* **1896**, 1343–1382.

[11] I. M. Gel'fand and A. N. Kolmogorov, "On rings of continuous functions on topological spaces", *Dokl. Akad. Nauk SSSR* **22** (1939), 11–15; English transl., *Selected works of A. N. Kolmogorov*, vol. I: *Mathematics and mechanics*, Kluwer, Dordrecht 1991, pp. 291–297.

[12] H.-J. Hoehnke, "Über komponierbare Formen und konkordante hyperkomplexe Größen", *Math. Z.* **70** (1958), 1–12.

[13] H.-J. Hoehnke and K. W. Johnson, "The 1-, 2- and 3-characters determine a group", *Bull. Amer. Math. Soc.* (N.S.) **27** (1992), 243–245.

[14] R. Mansfield, "A group determinant determines its group", *Proc. Amer. Math. Soc.* **116** (1992), 939–941.
[15] L. Nyssen, "Pseudo-représentations", *Math. Ann.* **306** (1996), 257–283.
[16] T. W. Palmer, *Banach algebras and the general theory of $*$-algebras*, vol. I: *Algebras and Banach algebras*, (Encyclopedia Math. Appl., vol. 49) Cambridge Univ. Press, Cambridge 1994.
[17] R. Rouquier, "Caractérisation des caractères et pseudo-caractères", *J. Algebra* **180** (1996), 571–586.
[18] R. L. Taylor, "Galois representations associated to Siegel modular forms of low weight", *Duke Math. J.* **63** (1991), 281–332.
[19] A. Wiles, "On ordinary λ-adic representations associated to modular forms", *Invent. Math.* **94** (1988), 529–573.

Steklov Institute of Mathematics, Russian Academy of Sciences;
University of Edinburgh, School of Mathematics
E-mail address: buchstab@mendeleevo.ru; E.Rees@ed.ac.uk

Received 15/JAN/04
Translated by E. G. REES