

Rings of continuous functions, symmetric products and Frobenius algebras *

V. M. Buchstaber and E. G. Rees

19 February 2004

Abstract

We present a generalisation of the theorem due to Kolmogorov and Gel'fand (1939) which characterises the image of the evaluation map from a compact Hausdorff space X to the linear space $C(X)^*$, the dual of the ring of continuous functions $C(X)$ on X . The generalisation characterises the image of the evaluation map from symmetric products of X . There are applications to the study of multi-symmetric polynomials.

The formulae that are used were introduced by G. Frobenius in 1896 to define higher characters of finite groups. These formulae have reappeared in several independent contexts over the last decade or so. They have been used by Wiles and Taylor to study representations, Hoehnke and Johnson and, later, McKay to study finite groups. The formulae also arose in the authors' joint work on multi-valued groups. We investigate various properties of these formulae.

We also use these formulae to state and prove a theorem about the structure constants of a Frobenius algebra. This is related to a result in a paper of H.-J. Hoehnke published in 1958. As a corollary we give a self-contained proof of the fact that the 1, 2, and 3 characters of the regular representation determine a finite group up to isomorphism, a result first proved by H.-J. Hoehnke and K.W Johnson in 1962.

Contents

1. Introduction
2. Symmetric products

*This survey is based on the talk given by Elmer Rees at the conference 'Kolmogorov and contemporary mathematics', Moscow 2003.

3. Properties of n -homomorphisms
4. Frobenius algebras
5. Appendix A. Proof of Mansfield's Lemma
6. Appendix B. The algebra of multi-symmetric polynomials

1 Introduction

In 1939, A.N. Kolmogorov, in collaboration with I.M. Gel'fand, published the paper [11] entitled 'On rings of continuous functions on topological spaces'. The main result identifies a compact Hausdorff space S with the space of maximal ideals in the ring of continuous functions on S . First courses and text books on functional analysis now invariably include such a result.

In modern terminology, the result can be stated as follows.

Theorem 1 *If X is a compact Hausdorff space, then, with suitable topologies on the function spaces, the evaluation map*

$$\mathcal{E} : X \rightarrow \text{Hom}(C(X), \mathbb{C})$$

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

This theorem is analogous to Hilbert's Nullstellensatz:

If V is an affine variety with co-ordinate ring $A = \mathbb{C}[x_1, \dots, x_n]/J$ where J is the (radical) ideal defining V then the evaluation map

$$\mathcal{E} : V \rightarrow \text{Hom}(A, \mathbb{C})$$

is an isomorphism (of varieties) onto the set of ring homomorphisms $A \rightarrow \mathbb{C}$.

Familiar re-statements of these theorems are obtained by noting that the set of all ring homomorphisms $A \rightarrow \mathbb{C}$ is easily identified with the set (usually denoted $\text{m-Spec}(A)$) of all maximal ideals in A .

The point of view that we take is that the set of ring homomorphisms $f : A \rightarrow \mathbb{C}$ is the 'algebraic variety' in $\text{Hom}(A, \mathbb{C})$ defined by the (infinite) set of equations $f(1) = 1$ and $f(ab) = f(a)f(b)$ for all $a, b \in A$. Since the map f is linear it is enough to consider the equations $f(1) = 1$ and $f(a^2) = f(a)^2$ for a in a basis of A .

The usual proof of the Kolmogorov-Gel'fand theorem found in text books proceeds by a contradiction argument: Suppose I is an ideal in $C(X)$ such

that there is no $x \in X$ at which all $\varphi \in I$ vanish. Then, for each $x \in X$, there is a $\varphi_x \in I$ which is real valued and greater than 1 on some neighbourhood U_x of x . By compactness of X , one can show that there is a $\varphi \in I$ which is everywhere greater than 1; hence, a constant function lies in I and therefore $I = C(X)$.

The paper [2] includes a constructive proof for this theorem, in the sense that we included the proof of a more general result which (in this case) yields, from a given ring homomorphism

$$f : C(X) \rightarrow \mathbb{C}$$

a unique $x \in X$ such that $f(\varphi) = \varphi(x)$ for all $\varphi \in C(X)$. It is possible that such a proof had already appeared in the literature but we are not aware of one.

We recall the proof here; firstly, in the case where X is a finite set. In this case $C(X) \cong \mathbb{C}^n$ where $n = \#X$ and we can choose as basis $\{\delta_x : x \in X\}$ for $C(X)$ where $\delta_x(x) = 1$, $\delta_x(y) = 0$ if $x \neq y$. Clearly $1 = \sum \delta_x$. Also, since $\delta_x^2 = \delta_x$ one has that $f(\delta_x)^2 = f(\delta_x)$ so $f(\delta_x) = 0$ or 1. However, $1 = f(1) = \sum_{x \in X} f(\delta_x)$ so there is a unique $x_0 \in X$ such that $f(\delta_{x_0}) = 1$ and

it is easy to check that $f(\varphi) = \varphi(x_0)$ for all $\varphi \in C(X)$.

Secondly, we adapt this proof to the more general case where X is a compact Hausdorff space.

Definition 2 For $K \subset X$ a compact subset, we call a sequence of continuous functions $\varphi_r : X \rightarrow [0, 1]$ ($r \in \mathbb{N}$) an **enclosing sequence** for K if

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

Clearly, $\varphi_r \varphi_s = \varphi_s$ if $s > r$.

Example 3 If K is a closed subset of the metric space X , then

$$\begin{aligned} \varphi_r(x) &= 0 && \text{if } d(x, K) \geq \frac{1}{r}, \\ &= 1 && \text{if } d(x, K) \leq \frac{1}{r+1} \\ &= (r+1)(1 - rd(x, K)) && \text{if } \frac{1}{r+1} \leq d(x, K) \leq \frac{1}{r} \end{aligned}$$

is an enclosing sequence for K .

Enclosing sequences exist for closed subsets of a compact Hausdorff space, but we leave the proof of this more general case for the reader.

Lemma 4 Let $\{\varphi_r\}$ be an enclosing sequence for K then, for each r , there is an open neighbourhood U_r of K such that $\varphi_r = 1$ on U_r .

Proof. Let $U_r = \{x : \varphi_{r+1}(x) > 0\}$, clearly $K \subset U_r$. Using the fact that $\varphi_r \varphi_{r+1} = \varphi_{r+1}$, it is easy to check that U_r has the required property. ■

Lemma 5 Let $\{\varphi_r\}$ be an enclosing sequence for K and $\psi : X \rightarrow \mathbb{R}$ is such that $\psi(x) = 1$ for all x in an open set U containing K . Then $(1 - \psi)\varphi_r = 0$ for large r .

Proof. For $x \notin U$, choose r s.t. $\varphi_r(x) = 0$, then $\varphi_r^{-1}[0, 1)$ is an open neighbourhood of x whose closure does not meet U . Cover $X \setminus U$ by a finite number of such neighbourhoods and let r_0 be the largest of the corresponding r 's, then $(1 - \psi)\varphi_{r_0} = 0$ and so $(1 - \psi)\varphi_s = (1 - \varphi)\varphi_{r_0}\varphi_s = 0$ for $s > r_0$. ■

Lemma 6 If $f : C(X) \rightarrow \mathbb{C}$ is a ring homomorphism and φ_r is a sequence in $C(X)$ such that $\varphi_r \varphi_s = \varphi_s$ for all $r < s$, then either there is an r_0 such that $f(\varphi_r) = 0$ for $r \geq r_0$ or $f(\varphi_r) = 1$ for all r .

Proof. Since $(f(\varphi_r) - 1)f(\varphi_s) = 0$ for all $r < s$, if $f(\varphi_r) \neq 1$ one has $f(\varphi_s) = 0$ for $s > r$. Hence the result. ■

Definition 7 If $f : C(X) \rightarrow \mathbb{C}$ is a ring homomorphism and $\{\varphi_r\}$ is an enclosing sequence for $K \subset X$, then we define $w_f^\varphi(K) \in \{0, 1\}$ to be $f(\varphi_r)$ for large r .

Proposition 8 If $\{\varphi_r\}, \{\psi_r\}$ are both enclosing sequences for K then $w_f^\varphi(K) = w_f^\psi(K)$ (which we then denote simply by $w_f(K)$).

Proof. Suppose $w_f^\varphi(K) = 1$ and $w_f^\psi(K) = 0$ then $f(\varphi_r) = 1$ for all r whereas $f(\psi_r) = 0$ for all r greater than some r_0 . Use the lemma with $\psi = \psi_{r_0}$ to find M with $\psi_{r_0}\varphi_M = \varphi_M$. So $f(1 - \psi_{r_0})f(\varphi_M) = 0$; but $f(1 - \psi_{r_0}) = 1$ so $f(\varphi_r) = 0$ for $r > M$. ■

Definition 9 If $f : C(X) \rightarrow \mathbb{C}$ is a homomorphism we define the **support** of f to be $S_f = \{x : w_f(x) = 1\}$.

Proposition 10 The cardinality of S_f is 1.

Proof. First, suppose S_f contains two distinct points x, y . Choose an enclosing sequence $\{\varphi_r\}$ for the set $\{x, y\}$ then $f(\varphi_r) = 1$; for a large enough r we can also choose continuous functions ψ_1, ψ_2 such that $\psi_1(x) = 1, \psi_1(y) = 0, \psi_2(x) = 0, \psi_2(y) = 1$ and such that $(\psi_1 + \psi_2)^{-1}1 \subset \varphi_r^{-1}1$ and $\text{Supp}\psi_1 \cap \text{Supp}\psi_2 = \emptyset$. Then $f(\psi_1) = f(\psi_2) = 1$ so $f(\psi_1 + \psi_2) = 2$, a contradiction.

Secondly, suppose S_f is empty, so for each $x \in X$, there is a $\varphi_x : X \rightarrow \mathbb{R}$ such that $\varphi_x(x) = 1$ with $f(\varphi_x) = 0$. The open sets $\{y : \varphi_x(y) > 0\}$ cover X so X is covered by finitely many of them with corresponding functions

$\varphi_1, \varphi_2, \dots, \varphi_n$ so $\varphi = \varphi_1 + \dots + \varphi_n$ does not vanish anywhere and $f(\varphi) = f(\varphi_1) + f(\varphi_2) + \dots + f(\varphi_n) = 0$. However, on the one hand, $f\left(\varphi \frac{1}{\varphi}\right) = f(1) = 1$ and on the other $f\left(\varphi \frac{1}{\varphi}\right) = f(\varphi)f\left(\frac{1}{\varphi}\right) = 0$. ■

To complete the proof we show that the homomorphism $C(X) \rightarrow \mathbb{C}$ defined by $\varphi \rightarrow \varphi(x_0)$ where $S_f = \{x_0\}$ is the same as f .

Proposition 11 *Let $S_f = \{x_0\}$ and $\psi : X \rightarrow \mathbb{C}$ be a continuous function then $f(\psi) = \psi(x_0)$.*

Proof. Let $\{\varphi_r\}$ be an enclosing sequence for $\{x_0\}$. We consider two cases. Firstly, if $\text{Supp}\psi \cap S_f = \emptyset$ then there is an open neighbourhood of x_0 on which ψ vanishes. So one can choose an r such that $\psi\varphi_r = 0$; however $f(\varphi_r) = 1$ and so $f(\psi) = 0$.

Secondly, if $x_0 \in \text{Supp}\psi$, consider the function $\theta_r = (\psi - \psi(x_0))\varphi_r$, its modulus is at most $|\psi - \psi(x_0)|$ and it vanishes outside a neighbourhood of x_0 ; by the continuity of ψ , $\theta_r \rightarrow 0$ in the supremum norm as $r \rightarrow \infty$. Hence $f(\theta_r) \rightarrow 0$ as $r \rightarrow \infty$. Since $x_0 \notin \text{Supp}\psi(1 - \varphi_r)$, by the first part of this proof, $f(\psi) = f(\psi\varphi_r)$. But $f(\psi) = f(\psi\varphi_r)f(\theta_r) + \psi(x_0)f(\varphi_r)$ and so $f(\psi) = \psi(x_0)f(\varphi_r)$. ■

2 Symmetric Products

Recall that the symmetric product of a space X is the quotient space $\text{Sym}^n(X) = \{(x_1, \dots, x_n) : (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) \sim (x_1, x_2, \dots, x_n) \text{ for all permutations } \sigma \in \Sigma_n\}$.

Continuous functions on $\text{Sym}^n(X)$ are precisely the continuous functions $f : X^n \rightarrow \mathbb{C}$ which are symmetric.

Analogous to the above we consider the evaluation map

$$\mathcal{E} : \text{Sym}^n(X) \rightarrow \text{Hom}(C(X), \mathbb{C})$$

defined by $\mathcal{E}(x_1, x_2, \dots, x_n)(\varphi) = \varphi(x_1) + \varphi(x_2) + \dots + \varphi(x_n)$. We describe the image of \mathcal{E} in terms of equations. The equations are closely related to formulae first used by G. Frobenius [9], [10] and to those used more recently by a number of authors including A. Wiles [19], R. Taylor [18], H.-J.

Hoehnke and K.W. Johnson [13], R. Rouquier [17], L. Nyssen [15].

From the point of view developed in [3]:

Let A be an associative algebra with 1 over \mathbb{C} and $f : A \rightarrow \mathbb{C}$ a linear, trace like map (i.e. $f(ab) = f(ba)$), then we define $\Phi_n(f) : A^{\otimes n} \rightarrow \mathbb{C}$ by $\Phi_1(f) = f$, $\Phi_2(f)(a_1 \otimes a_2) = f(a_1)f(a_2) - f(a_1a_2)$ and then by induction

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

Note that a ring homomorphism $f : A \rightarrow \mathbb{C}$ satisfies $f(1) = 1$ and $\Phi_2(f) \equiv 0$.

Definition 12 *A Frobenius n -homomorphism satisfies $f(1) = n$ and $\Phi_{n+1}(f) \equiv 0$.*

Theorem 13 *The image*

$$\mathcal{E} : \text{Sym}^n(X) \rightarrow \text{Hom}(C(X), \mathbb{C})$$

is defined precisely by the equations $f(1) = n$ and $\Phi_{n+1}(f) \equiv 0$.

We now give some alternative descriptions of these equations in the case of a commutative algebra A .

1. $\Phi_n(f)(a \otimes \dots \otimes a)$ is the determinant of the matrix

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

and $\Phi_n(f)(a_1 \otimes a_2 \otimes \dots \otimes a_n)$ can be obtained by polarisation, since $\Phi_n(f)$ is multi-linear.

2. Each $\sigma \in \Sigma_n$ the symmetric group on n letters, can be decomposed into a product of disjoint cycles of total length n , say $\sigma = \gamma_1 \gamma_2 \dots \gamma_r$. If $\gamma = (i_1 \dots i_m)$ is a cycle, let $f_\gamma(a_1, a_2, \dots, a_n) = f(a_{i_1} a_{i_2} \dots a_{i_m})$ then $\Phi_n(f)(a_1, a_2, \dots, a_n) = \sum_{\sigma \in \Sigma_n} \varepsilon_\sigma f_{\gamma_1}(a_1, a_2, \dots, a_n) f_{\gamma_2}(a_1, a_2, \dots, a_n) \dots f_{\gamma_r}(a_1, a_2, \dots, a_n)$ where ε_σ is the sign of the permutation σ .

For example,

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

We note that this last version applies to a trace like homomorphism f defined on a non-commutative algebra A . It is often easier to work with these formulae in ‘diagonal’ form and use polarisation to obtain the general formula. For example, $\Phi_3(f)(a, a, a) = s_1^3 - 3s_1s_2 + 2s_3$ where

$$s_1 = f(a), \quad s_2 = f(a^2) \quad \text{and} \quad s_3 = f(a^3).$$

We use the notation s_k to highlight the connection with the Newton formulae relating the elementary symmetric functions F_n with the power sums s_k . We will now develop this relationship where F_n is used to denote the polynomial in the variables s_k which equals $\Phi_n(f)(a, a, \dots, a)$ with

$$s_k = f(a^k).$$

By its definition,

$$F_n = \sum_{\sigma \in \Sigma_n} \left(\prod_{k=1}^n ((-1)^{k+1} s_k)^{m_k(\sigma)} \right)$$

where $m_k(\sigma)$ is the number of cycles of length $k \geq 1$ in the full disjoint cycle representation of σ . Now the number of elements in Σ_n with m_k cycles of length k is

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

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 $\Pi(n)$ is the set of partitions of n and \mathbf{m} is the partition with m_k parts of size k so $\sum_{k=1}^n k m_k = n$.

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 hence we have

Theorem 14

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

We also have

Proposition 15

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

Proof. If we let $F(t) = \sum_{n=0}^{\infty} F_n \frac{t^n}{n!}$ then differentiating the expression in the Theorem gives

$$F'(t) = F(t)(s_1 t^2 - s_2 t^2 + s_3 t^3 - \dots).$$

The result of the Proposition follows immediately. ■

We now characterise the expressions F_n using differential operators.

Lemma 16 Let $d = \sum_{r=2}^{\infty} r s_{r-1} \frac{\partial}{\partial s_r}$, then

a) $\frac{\partial F_n}{\partial s_1} = n F_{n-1}$

b) $d F_n = -n(n-1) F_{n-1}$

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

d) $\text{Ker} \left(\frac{\partial}{\partial s_1} \right) \cap \text{Ker}(d)$ is the set of constant polynomials.

Proof.

a) By differentiating the right hand side of the expression in Theorem 14

we have that $\frac{\partial F(t)}{\partial s_1} = tF(t)$ so

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

and comparing coefficients gives the result.

b) Applying d similarly we get

$$dF(t) = F(t)[-s_1 t^2 + s_2 t^3 - s_3 t^4 + \dots] = -t^2 F'(t).$$

Comparing the coefficients of t^n gives

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

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

d) If f is a polynomial in the kernel of $\frac{\partial}{\partial s_1}$ then it is a polynomial in the variables s_2, s_3, \dots . If f is in the kernel of both d and $\frac{\partial}{\partial s_1}$ then by c) it is in the kernel of $\frac{\partial}{\partial s_2}$. The proof is now completed by induction using c). ■

This leads immediately to

Theorem 17 *The sequence of polynomials F_n is characterised by the properties :*

1. $F_1 = s_1,$
2. $\frac{\partial F_n}{\partial s_1} = nF_{n-1}$
3. $dF_n = -n(n-1)F_{n-1}$

3 Frobenius Algebras

When A is an associative algebra over \mathbb{C} , we let $J(A)$ denote the associated Jordan algebra with multiplication $a \circ b = (ab + ba)/2$. If the structure constants for A with respect to a basis $\{e_i : i \in I\}$ are a_{ij}^k (so that $e_i e_j = \sum a_{ij}^k e_k$) then those for $J(A)$ are $a_{(ij)}^k = a_{ij}^k + a_{ji}^k$.

Definition 18 An algebra A together with a trace-like linear map $f : A \rightarrow \mathbb{C}$ is called a Frobenius algebra if the pairing $A \times A \rightarrow \mathbb{C}$ defined by $f(ab)$ is non-degenerate.

Theorem 19 If (A, f) is a Frobenius algebra, the structure constants of $J(A)$ are determined by knowing Φ_1, Φ_2 and Φ_3 .

A related result is contained in [12], although the hypotheses there are different and, indeed, seem to include something similar to the result of Theorem 2.8 of [3]. The above Theorem therefore seems rather stronger.

Corollary 20 The maps $\Phi_k, k \geq 4$ are determined by Φ_1, Φ_2, Φ_3 .

This leads to the result [13] that a finite group is determined by its Frobenius k -characters for $k = 1, 2, 3$.

Proof. By definition

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

so

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

Similarly

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

This becomes

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

By the definition of a Frobenius algebra the matrix $R_{ij} = f(e_ie_j) = \sum_r a_{ij}^r f(e_r)$ is symmetric and non-singular. Hence, one can solve uniquely for $a_{(ij)}^r = a_{ij}^r + a_{ji}^r$ from the above equation. This proves the theorem. ■

More explicitly, in the case of a commutative Frobenius algebra A , let

$$R_i = f(e_i), R_{ij} = f(e_i e_j) \text{ and } R_{ijk} = f(e_i e_j e_k).$$

In terms of the values of Φ_2, Φ_3 we have,

$$\begin{aligned} R_{ij} &= \Phi_2(e_i, e_j) - R_i R_j \\ 2R_{ijk} &= \Phi_3(e_i, e_j, e_k) + R_i R_{jk} + R_j R_{ik} + R_k R_{ij} - R_i R_j R_k \end{aligned}$$

Let R^{ij} be the inverse of the matrix R_{ij} (it is invertible because A is a Frobenius algebra); then, the following straightforward calculation yields an explicit formula for the structure constants of A :

Proposition 21 *The structure constants of a Frobenius algebra A are given by*

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

Proof. Using that

$$R_{ijk} = f(e_i e_j e_k) = \sum_n f(a_{ij}^n e_n e_k)$$

we have that

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

■

Proof. We need to show that one can calculate the value of each Φ_k from the $a_{(ij)}^k$ [rather than a_{ij}^k]. We do this by induction; in the expansion of $\Phi_k(e_1, e_2, \dots, e_k)$ in terms of the values of f , the only term that cannot be immediately expressed in Φ_r with $r < k$ is

$$\sum_{\sigma \in \Sigma_{k-1}} f(e_i e_{\sigma(2)} e_{\sigma(3)} \dots e_{\sigma(k)}) = \frac{1}{k} \sum_{\sigma \in \Sigma_k} f(e_{\sigma(1)} e_{\sigma(2)} \dots e_{\sigma(k)}).$$

The multiplication \circ on $J(A)$ may not be associative but the associator is a commutator:

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

Because f is trace-like, one has that $f((a \circ b) \circ c) = f(a \circ (b \circ c))$. It follows that the value of f on an iterated product of elements in $J(A)$ behaves as if the multiplication in $J(A)$ is associative, hence

$$2^{k-1} \sum_{\sigma \in \Sigma_k} f(e_{\sigma(1)} e_{\sigma(2)} \dots e_{\sigma(k)}) = \sum_{\sigma \in \Sigma_k} f(e_{\sigma(1)} \circ e_{\sigma(2)} \circ \dots \circ e_{\sigma(k)}).$$

■

The result about finite groups is the following

Corollary 22 *If G is a finite group and χ is the character of the regular representation, then G is determined up to isomorphism by χ , $\Phi_2(\chi)$ and $\Phi_3(\chi)$.*

Proof. By the above Theorem, the Jordan algebra $J(\mathbb{C}G)$ is determined by the data χ , $\Phi_2(\chi)$ and $\Phi_3(\chi)$ and so determines the multiplication on G up to an ambiguity of order. The following Lemma completes the proof. The proof of this Lemma in [14] is an elementary (but tricky) case by case analysis. We present a slightly different proof in the Appendix.

Lemma 23 (Mansfield) *Let G be a finite group whose multiplication rule is not known precisely, but for each pair of elements $g, h \in G$ one knows the set $\{gh, hg\}$ then one can determine the set of functions $\{m, m^{\text{op}} : G \times G \rightarrow G\}$ where $m(x, y) = xy$ and $m^{\text{op}}(x, y) = yx$.*

In [14] this Lemma is used to prove the result of Formanek and Sibley [8] that the group determinant of a finite group (first studied by Dedekind) determines the group. The group determinant of a group G which has n elements is defined as follows : Choose a bijection between G and the set $\{x_1, x_2, \dots, x_n\}$. Then the group determinant is the element of the polynomial ring $\mathbb{Z}[x_1, x_2, \dots, x_n]$ obtained by taking the determinant of the matrix obtained from the group multiplication table by replacing each entry from G by the corresponding x_r .

4 Appendix : Proof of Mansfield's Lemma

We now restate the Lemma.

Lemma 24 *Let G be finite group with multiplication $(x, y) \rightarrow xy$. If $*$ is an associative multiplication defining a group structure on G such that, for each pair $x, y \in G$, $x * y = xy$ or yx , then either $x * y = xy$ for all $x, y \in G$ or $x * y = yx$ for all $x, y \in G$.*

An alternative way to state the lemma is to define $A = \{(x, y) : x * y = xy\}$ and $B = \{(x, y) : x * y = yx\}$. The assumption of the Lemma is that $A \cup B = G \times G$ and the conclusion is that either $A = G \times G$ or $B = G \times G$. Clearly, $A \cap B$ is symmetric.

Proof. (Based on Exercise 26 of §4 in [1]).

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

Proof. It is immediate that $xy = yx \Rightarrow x * y = y * x$.

For the converse, we can suppose $x * y = xy$ (otherwise, interchange x and y) and that $xy \neq yx$, otherwise the result is immediate.

Consider $x * x * y = x^2 * y$ and suppose it does not equal x^2y , then it equals yx^2 but it also equals $x * xy = xyx$ (or x^2y). Hence $yx^2 = xyx$ which implies $yx = xy$. As $xy \neq yx$, we have $x * x * y = x^2y$.

Now, $x * y * x * y$ equals $xy * xy = (xy)^2$; it also equals (by assumption) $x * x * y * y = x^2y * y = x^2y^2$ or yx^2y . So either $xyxy = x^2y^2$ (and this implies $yx = xy$) or $xyxy = yx^2y$ (which also implies $yx = xy$). ■

Corollary 26 $x * y = xy \Leftrightarrow y * x = yx$. *i.e. A is symmetric.*

Proof. Suppose $x * y = xy$ and $y * x = xy$, then by Fact 25, $xy = yx$. Hence $x * y = xy \Rightarrow y * x = yx$. The opposite implication follows by symmetry. ■

Since both A and $A \cap B$ are symmetric and $A \cup B = G \times G$ we have that B is symmetric, proving

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

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

Proof. If $xy = yx$, then $x * y * x = xy * x = xyx$ or x^2y and these are equal.

On the other hand, $xy \neq yx$ and now suppose $x * y * x \neq xyx$, then there are two cases:

- (a) $x * y = xy$ and $y * x = yx$ so $x * y * x = xy * x = x^2y$ or xyx and it also equals $x * yx = xyx$ or yx^2 . So $x * y * x = x^2y = yx^2$. Consider $x * x * y = x^2 * y = x^2y = x * y * x$ so $x * y = y * x$ a contradiction.
- (b) $x * y = yx$ and $y * x = xy$. Again we have $x * y * x = yx * x = yx^2$ and $x * y * x = x * xy = x^2y$. So $x * x * y = x * y * x$ and $x * y = y * x$ a contradiction. ■

We consider $G \times G$ as a square array, so that $R_x = \{(x, y) : y \in G\}$ is a row.

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

Proof. Suppose Fact 29 is not true, then there is an x such that R_x meets both $G \times G \setminus A$ and $G \times G \setminus B$ i.e. there are $y, z \in G$ with $x * y = yx \neq xy = y * x$ and $x * z = xz \neq zx = z * x$. Under these circumstances, we show that $yxz = zxy$.

There are two cases:

- (a) $y * z \neq z * y$. Then by the above corollaries, $yz \neq zy$.

Consider $z * x * y = zx * y = yzx$ or zxy ; it also equals $z * yx = zyx$ or yxz . But $yzx \neq zyx$, $yzx \neq yxz$ and $zxy \neq zyx$, so $z * x * y = zxy = yxz$.

- (b) $y * z = z * y$ ($= yz = zy$). We assume that $yxz \neq zxy$ to obtain a contradiction.

Consider $z * x * y$; it equals $zx * y = yzx$ or zxy and also equals $z * yx = zyx$ or yxz . By the assumption and the facts that $zxy \neq zyx$ and $yzx \neq yxz$, we conclude that $z * x * y = yzx = zyx$.

Consider $x * z * y$; it is not equal to $z * x * y = yzx$. But it equals $x * y * z = x * yz = xyz$ or yzx , hence $x * z * y = xyz = xzy$.

Finally, consider $z * y * x$; it is not equal to $z * x * y = yzx$. But it equals $yz * x = xyz$ or yzx . Hence $z * y * x = xyz = xzy$.

Therefore $x * (z * y) = (z * y) * x$, i.e. $x * zy = zy * x$ and so $xzy = zyx$ from which we deduce that $z * x * y = x * z * y$ which contradicts $x * z \neq z * x$. ■

Finally consider $x * z * x * y$. By Fact 28 it equals $xzx * y = xzxy$ or $yxzx$.

It also equals $xz * yx = xzyx$ or $yxxz$. There are two cases to consider:

- (a) $x * z * x * y = xzxy = xzyx$ or $yxxz$. The first possibility yields $xy = yx$ a contradiction. The second possibility and the above calculation yields

$$yxxz = xzxy = yxzx \text{ again leading to } xy = yx.$$

- (b) $x * z * x * y = yxzx = xzyx$ or $yxxz$. The second possibility yields $xz = zx$, a contradiction. So $xzyz = yxzx = xzyx$ which also yields $xz = zx$. This proves Fact 29.

■

By Fact 29, for every x , either $R_x \subset A$ or $R_x \subset B$. Suppose $R_x \subset A$ but $R_x \not\subset B$ and $R_u \subset B$ but $R_u \not\subset A$ then $x * y = xy$ for all y and there is a z with $xz \neq zx$. Similarly $u * v = vu$ for all v and there is a w with $uw \neq wu$.

Consider $x * u = xu$, it equals $ux = u * x$ and $R_{xu} \subset A$ or B . Suppose $R_{xu} \subset A$, then consider the element $x * u * w = xu * w = xuw$, it also equals $x * wu = xwu$. This is a contradiction. So suppose $R_{xu} \subset B$, then consider the element $z * x * u = z * xu = xuz = uxz$, it also equals $zx * u = uzx$. So $xz = zx$, a contradiction and Mansfield's lemma is proved.

■

References

- [1] N. Bourbaki, *Éléments de Mathématiques. Algèbre. Chapires 1-3.* Paris: Hermann, 1970.
- [2] V. M. Buchstaber and E. G. Rees, A constructive proof of the generalised Gel'fand isomorphism. *Funktsional. Anal. i Prilozhen.* 35 (2001), no. 4, 20–25, 95; translation in *Funct. Anal. Appl.* 35 (2001), no. 4, 257–260
- [3] V. M. Buchstaber and E. G. Rees, The Gel'fand map and symmetric products. *Selecta Math. (N.S.)* 8 (2002), no. 4, 523–535
- [4] V. M. Buchstaber and E. G. Rees, Multi-valued groups, their representations and Hopf algebras, *Transformation groups Vol 1* (1997), 325 -349, Birkhauser-Boston.
- [5] V. M. Buchstaber and E. G. Rees, Multi-valued groups, n -Hopf algebras and n -ring homomorphisms, Chapter in *Lie groups and Lie algebras* (1998) 85 - 107, Kluwer Academic Publisher.
- [6] V. M. Buchstaber and E. G. Rees, Frobenius k -characters and n -ring homomorphisms. (Russian) *Uspekhi Mat. Nauk* 52 (1997), no. 2(314),159–160; translation in *Russian Math. Surveys* 52 (1997), no. 2, 398–39
- [7] E. Formanek, The polynomial identities and invariants of $n \times n$ matrices, *Amer. Math. Soc.* (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, Sitzungber. Preuss. Akad. Wiss. Berlin (1896), 985-1021.
- [10] G. Frobenius, Über die Primfaktoren der gruppensdeterminante. Sitzungber. 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**:1 (1939), 7–10.
- [12] H.-J. Hoehnke, Über Komponierbare Formen und hypercomplexe Grossen, *Math. Zeitschrift*, **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. **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-representations. Math. Ann. 306 (1996), 257–283.
- [16] T. W. Palmer, Banach algebras and the general theory of *-algebras. Vol 1: Algebras and Banach algebras. Cambridge: Cambridge University Press, 1994. (Encyclopedia Math. Appl. Vol. 49.
- [17] R. Rouquier, Characterisation des caracteres et pseudo-caracteres. 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), no. 2, 281–332
- [19] A. Wiles, On ordinary λ -adic representations associated to modular forms. Invent. Math. 94 (1988), no. 3, 529–573.