Can. J. Math., Vol. XLI, No. 3, 1989, pp. 556–576

GENERALIZED MATRICES

FRIEDRICH ROESLER

Introduction. Similar to the multiplication of square matrices one can define multiplications for three dimensional matrices, i.e., for the "cubes" of the vector space

$$\mathcal{W}(I,K) := \{\mathcal{A} = (\alpha_{xyz})_{x,y,z\in I};\, \alpha_{xyz} \in K\}$$

where I denotes a finite set of indices and K is any field. The multiplications shall imitate the matrix multiplication: To obtain the coefficient γ_{xyz} of the product $(\gamma_{xyz}) = (\alpha_{xyz})(\beta_{xyz})$, all coefficients α_{xij}, $i,j \in I$, of the horizontal plane with index x of (α_{xyz}) are multiplied with certain coefficients β_{hgz} of the vertical plane with index z of (β_{xyz}) and the results are added:

$$\text{(M)} \qquad \gamma_{xyz} := \sum_{i,j\in I} \alpha_{xij}\beta_{h(xyzij),g(xyzij),z}$$

where the mappings $h, g : I^5 \longrightarrow I$ determine the multiplication rule (M) in detail.

The aim of this paper is to construct and to interpret all possible multiplications of type (M) on $\mathcal{W}(I,K)$ which are associative with unit element

$$\mathcal{E} = (\delta_{x,y}\delta_{y,z})_{x,y,z\in I}$$

and to determine the K-algebra structure on $\mathcal{W}(I,K)$.

Section 1 deals with the construction. The key result is Proposition 4: Every associative multiplication on $\mathcal{W}(I,K)$ with unit element $\mathcal{E}$ induces a natural group structure G on I. This allows one to construct all associative multiplications on $\mathcal{W}(I,K)$ in the following way:

– First impose any group structure G on I.

– Then take any mapping $f : G^3 \longrightarrow G$ such that $f(x,y,z)$ is bijective with respect to y and

$$f(e,y,e) = y^{-1}, \quad f(x,e,e) = e, \quad f(x,x,x) = e.$$

(There are $(n!)^{n^2-1}n^{2-2n}$ possibilities to choose f, where $n = |G|$.)

– Finally define the multiplication (M) with the mappings

$$h(x,y,z,i,j) = j,$$
$$g(x,y,z,i,j) = f^*(j, f(x,i,j)^{-1}f(x,y,z), z),$$

Received September 12, 1988.

where f^* denotes the inverse of f with respect to its second argument.

(Proposition 1 and Theorem 6.) Theorem 7 describes the structure of $\mathcal{W}(I,K)$ as a tensor product: If G is the group induced on I by the multiplication on $\mathcal{W}(I,K)$, then

$$\mathcal{W}(I,K) \cong K[G] \otimes_K M(I,K)$$

where $M(I,K)$ is the algebra of square matrices $(\alpha_{xy})_{x,y\in I}$ over K.

Section 2 deals with an algebraic interpretation of the cubes. Matrices give a description, by matrix multiplication, of linear mappings between spaces of column vectors. With this in mind one can interpret the cubes $\mathcal{A} \in \mathcal{W}(I,K)$ (via cube multiplication) as linear mappings $\mathcal{A}^\phi$ between spaces of matrices:

$$\phi : \mathcal{W}(I,K) \longrightarrow \mathrm{End}_K(M(I,K)), \quad \mathcal{A} \longmapsto \mathcal{A}^\phi$$

then becomes an embedding of the $|I|^3$-dimensional algebra of cubes into the $|I|^4$-dimensional algebra of endomorphisms of $M(I,K)$, with $\mathcal{A}^\phi \circ \mathcal{B}^\phi = (\mathcal{AB})^\phi$ being a consequence of the associative law in $\mathcal{W}(I,K)$. To characterize the cubes completely one has to impose $K[G]$-module structures on $M(I,K)$ (via the regular representation of G) and on $\mathcal{W}(I,K)$. The restricted ϕ,

$$\phi : \mathcal{W}(I,K) \longrightarrow \mathrm{End}_{K[G]}(M(I,K))$$

then is an isomorphism (Theorem 11), and $\mathcal{A}$ is invertible in $\mathcal{W}(I,K)$ if and only if the (twisted) vertical planes of $\mathcal{A}$ form a $K[G]$-basis of $M(I,K)$ (Corollary 12); exactly as in the case of square matrices, which are invertible if and only if their columns form a basis of the column space. Finally $\mathcal{W}(I,K)$ is embedded into $M(I^2,K)$ (Theorem 14), which allows one to transfer the theory of eigenvalues from the matrices to the cubes. For instance (Proposition 15): $\mathcal{A} \in \mathcal{W}(I,K)$ is diagonalizable if and only if $M(I,K)$ is the sum of the eigenspaces of $\mathcal{A}$.

I am grateful to Prof. A. Leutbecher for his suggestion that $\mathcal{W}(I,K)$ can be represented as a tensor product.

1. PROPOSITION 1. *If the multiplication (M) on $\mathcal{W}(I,K)$ is associative with unit element $\mathcal{E}$, then $h(x,y,z,i,j) = j$.*

Proof. Comparing corresponding entries on both sides of $\mathcal{BE} = \mathcal{B}, \mathcal{B} = (\beta_{xyz})_{x,y,z\in I}$, gives

$$(1) \qquad \sum_{\substack{i,j\in I \\ h(xyzij)=g(xyzij)=z}} \beta_{xij} = \beta_{xyz}$$

for all $x,y,z \in I$. $\mathcal{BE} = \mathcal{B}$ for all $\mathcal{B} \in \mathcal{W}(I,K)$ then shows that β_{xyz} has to be the only summand of the left hand sum in (1), hence

$$(2) \qquad h(x,y,z,y,z) = g(x,y,z,y,z) = z$$

for all $x, y, z \in I$. The associative law

$$(\mathcal{E}_{xij}\mathcal{B})\mathcal{C} = \mathcal{E}_{xij}(\mathcal{B}\mathcal{C})$$

with

$$\mathcal{E}_{xij} = (\delta_{x,u}\delta_{i,v}\delta_{j,w})_{u,v,w\in I} \quad \text{and} \quad \mathcal{C} = (1)_{u,v,w\in I}$$

reads in components as

$$\sum_{r,s} \beta_{h(xrsij),g(xrsij),s} = \sum_{r,s} \beta_{h(xyzij),r,s} \, .$$

This being valid for all $x, y, z, i, j \in I$ and all $\beta_{xyz} \in K$ implies that both sums must contain the same β's. Now the first β-index shows

(3) $$h(x, r, s, i, j) = h(x, y, z, i, j)$$

for all $r, s \in I$, and hence

$$\begin{aligned} j &= h(x, i, j, i, j) \quad \text{by (2)} \\ &= h(x, y, z, i, j) \end{aligned}$$

by (3), for all $x, y, z, i, j \in I$.

Proposition 1 shows that (M) can be simplified to

(M′) $$\gamma_{xyz} := \sum_{i,j\in I} \alpha_{xij}\beta_{j,g(xyzij),z}$$

with $g: I^5 \longrightarrow I$. If such a mapping g is given, $\mathcal{W}(g, K)$ will denote the vector space $\mathcal{W}(I, K)$ together with the multiplication (M′) on $\mathcal{W}(I, K)$.

Let $\mathcal{G}(I)$ be the set of all mappings $g: I^5 \longrightarrow I$ such that the multiplication on $\mathcal{W}(g, K)$ is associative with unit element $\mathcal{E}$. To survey all these multiplications entails an analysis of the set $\mathcal{G}(I)$. The next proposition gives a first characterisation for the elements of $\mathcal{G}(I)$:

PROPOSITION 2. $g \in \mathcal{G}(I)$ *if and only if*

(G1) $g(x, y, z, *, z): I \longrightarrow I$ *is bijective*,

(G2) $g(x, y, z, i, j) = g(l, g(x, y, z, k, l), z, g(x, i, j, k, l), j)$,

(G3) $g(x, x, x, x, x) = x$.

COROLLARY 3. (G1)–(G3) *imply*

(G4) g *is bijective in its second and its fourth argument*,

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press

(G5) $g(x, y, z, y, z) = z,$

(G6) $g(x, y, z, x, x) = y.$

Proof. Eq. (1) in the proof of Proposition 1 shows that $\mathcal{E}$ is a right unit if and only if

(4) $g(x, y, z, i, z) = z$ is equivalent to $i = y$.

Similarly,

$$\mathcal{E}(\beta_{xyz}) = (\beta_{x,g(xyzxx),z})_{x,y,z}$$

shows that $\mathcal{E}$ is a left unit if and only if

(5) $g(x, y, z, x, x) = y$

for all $x, y, z \in I$. The associative law holds in $\mathcal{W}(I, K)$ as soon as one has

$$(\mathcal{E}_{xij}\mathcal{B})\mathcal{C} = \mathcal{E}_{xij}(\mathcal{B}\mathcal{C})$$

for all $x, i, j \in I$ and all $\mathcal{B}, \mathcal{C} \in \mathcal{W}(I, K)$, and this reads in components as

(6)
$$\sum_{r,s} \beta_{j,g(xrsij),s}\gamma_{s,g(xyzrs),z} = \sum_{r,s} \beta_{jrs}\gamma_{s,g(j,g(xyzij),z,r,s),z} .$$

First we prove that $g \in \mathcal{G}(I)$ implies (G1)–(G3): (4) with $x = y = z = i$ yields (G3).

Both sums in (6) must contain the same β's. Hence for all $x, s, i, j \in I$ the mappings $r \longmapsto g(x, r, s, i, j)$ are one-to-one, i.e., g is bijective in its second argument, and one can substitute $g(x, r, s, i, j)$ for r in the right hand side of (6). Comparing the second γ-index proves (G2).

Suppose that there are indices x, y, z, i_1, i_2 in I such that

$$g(x, y, z, i_1, z) = g(x, y, z, i_2, z) =: u.$$

Then by (G2) for $\nu = 1, 2$

$$g(x, i_2, z, y, z) = g\left(z, g(x, i_2, z, i_\nu, z), z, u, z\right).$$

The bijectivity of g in its second argument and (4) yield

$$g(x, i_2, z, i_1, z) = g(x, i_2, z, i_2, z) = z.$$

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press

But then $i_1 = i_2$ by (4), which shows (G1).

Now we prove the corollary: (G2) with $j = z$ is

$$g(x,y,z,i,z) = g\left(l, g(x,y,z,k,l), z, g(x,i,z,k,l), z\right).$$

The left hand side is bijective in i by (G1) and hence the right hand side is it, too. This implies that g must be bijective in its second argument.

Suppose that there are indices x, i, j, z, k_1, k_2 in I such that

$$g(x,i,j,k_1,z) = g(x,i,j,k_2,z) =: w.$$

(G2) with $l = z$ is

$$g(x,y,z,i,j) = g\left(z, g(x,y,z,k,z), z, g(x,i,j,k,z), j\right).$$

The left hand side is independent of k, hence

$$g\left(z, g(x,y,z,k_1,z), z, w, j\right) = g\left(z, g(x,y,z,k_2,z), z, w, j\right).$$

The bijectivity of g in its second argument implies

$$g(x,y,z,k_1,z) = g(x,y,z,k_2,z),$$

and (G1) yields $k_1 = k_2$, i.e., g is bijective in its fourth argument. This proves (G4).

Choose in (G2) $i = y$, $j = l = z$, and k such that

$$g(x,y,z,k,z) = z$$

which is possible because of (G1). Then

$$g(x,y,z,y,z) = g(z,z,z,z,z) = z$$

by (G3), and this is (G5).

(G2) with $i = j = k = l = x$, $w := g(x,y,z,x,x)$ and (G3) show

$$w = g(x,w,z,x,x)$$

for all $w \in I$, because $g(x,y,z,x,x)$ is bijective in y by (G4). This is (G6).

Conversely, we prove that (G1)–(G6) imply (4), (5), and (6): (4) is a consequence of (G1) and (G5). (5) is (G6). To prove (6) we substitute $g(x,r,s,i,j)$ for r in the right hand side of (6), which is admissible because of (G4), and then we use (G2) in the second γ-index.

Remarks. (1) (G1), (G2), (G3) are independent: $g(x,y,z,i,j) = j$ satisfies (G2) and (G3) but not (G1). $g(x,y,z,i,j) = i$ satisfies (G1) and (G3) but not (G2). And if $I = G$ is a group and $c \neq e$ is an element of its center, then

$$g(x,y,z,i,j) = cyi^{-1}j$$

satisfies (G1) and (G2) but not (G3).

(2) In particular (G4) implies that for all $x,y,z \in I$ the mappings

$$I^2 \longrightarrow I^2, \quad (i,j) \longmapsto \big(j, g(x,y,z,i,j)\big)$$

are bijective. Hence the coefficient

$$\gamma_{xyz} = \sum_{i,j} \alpha_{xij}\beta_{j,g(xyzij),z}$$

of $C = \mathcal{A}\mathcal{B}$ not only depends on all coefficients of the xth horizontal plane of $\mathcal{A}$ (which is so by definition) but also on all coefficients of the zth vertical plane of $\mathcal{B}$; in accordance with the matrix multiplication.

Every associative multiplication g of type (M′) on $\mathcal{W}(I,K)$ induces a natural group structure on the index set I, as the next proposition will show. Therefore we require that I contains an element e which will always become the unit element as soon as this group structure is imposed on I. Further, any multiplication of elements in I will be carried out in this group.

A mapping $\mu: I^2 \longrightarrow I$ will be called a group mapping for I, if I together with the multiplication $xy := \mu(x,y)$ on I is a group with unit element e. Then we say that μ induces a group structure on I and denote this group by G_μ.

PROPOSITION 4. *For every* $g \in \mathcal{G}(I)$

$$\mu_g(x,y) := g\,\big(e,x,e,g(e,e,e,y,e),e\big)$$

induces a group structure on I.

COROLLARY 5. $g(e,x,e,y,e) = xy^{-1}$.

Proof. (G2), (G5), and (G6) imply for

$$\nu: I^2 \longrightarrow I, \quad \nu(x,y) := g(e,x,e,y,e):$$

(G2′) $\nu(x,y) = \nu\big(\nu(x,z),\nu(y,z)\big)$,

(G5′) $\nu(x,x) = e$,

(G6′) $\nu(x,e) = x$.

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press

The multiplication on I, defined by μ_g, is

$$xy := \nu\left(x, \nu(e, y)\right).$$

Unit element:

$$\begin{aligned} ex &= \nu\left(e, \nu(e, x)\right) \\ &= \nu\left(\nu(x, x), \nu(e, x)\right) && \text{by (G5')} \\ &= \nu(x, e) && \text{by (G2')} \\ &= x && \text{by (G6')}. \end{aligned}$$

Inverse:

$$\begin{aligned} \nu(e, x)x &= \nu\left(\nu(e, x), \nu(e, x)\right) \\ &= e && \text{by (G5')}. \end{aligned}$$

Associative law:

$$\begin{aligned} (7) \qquad \nu[\nu\left(x, \nu(e, y)\right), y] &= \nu[\nu\left(x, \nu(e, y)\right), \nu(y, e)] && \text{by (G6')} \\ &= \nu[\nu\left(x, \nu(e, y)\right), \nu\left(e, \nu(e, y)\right)] && \text{by (G2'), (G5')} \\ &= \nu(x, e) && \text{by (G2')} \\ &= x && \text{by (G6')}. \\ (8) \qquad \nu[e, \nu(y, \nu(e, z))] &= \nu[\nu(\nu(e, z), \nu(e, z)), \nu(y, \nu(e, z))] && \text{by (G5')} \\ &= \nu[\nu(e, z), y] && \text{by (G2')}. \end{aligned}$$

Hence

$$\begin{aligned} (xy)z &= \nu[\nu\left(x, \nu(e, y)\right), \nu(e, z)] \\ &= \nu[\nu[\nu\left(x, \nu(e, y)\right), y], \nu[\nu(e, z), y]] && \text{by (G2')} \\ &= \nu[x, \nu[e, \nu\left(y, \nu(e, z)\right)]] && \text{by (7), (8)} \\ &= x(yz). \end{aligned}$$

And concerning the corollary:

$$\begin{aligned} g(e, x, e, y, e)y &= \nu(x, y)y \\ &= \nu[\nu(x, y), \nu(e, y)] \\ &= \nu(x, e) && \text{by (G2')}. \\ &= x && \text{by (G6')}. \end{aligned}$$

The group structure $G = G_{\mu_g}$ on I, induced by the group mapping μ_g, $g \in \mathcal{G}(I)$, plays the central part in the description of the set $\mathcal{G}(I)$. The group structure itself deals with only two of the five dimensions of the domain I^5 of g. The remaining three are taken care of by a mapping

$$f: G^3 \longrightarrow G$$

with the following simple properties:

(F1) $f(x, *, z): G \longrightarrow G$ is bijective,

(F2) $f(e, y, e) = y^{-1}$,

(F3) $f(x, e, e) = e$,

(F4) $f(x, x, x) = e$.

Let $\mathcal{F}(I)$ denote the set of all pairs (μ, f) such that $\mu: I^2 \longrightarrow I$ is a group mapping for I and $f: G_\mu^3 \longrightarrow G_\mu$ satisfies (F1)–(F4). $\mathcal{F}(I)$ represents all associative multiplications (M) on $\mathcal{W}(I, K)$:

THEOREM 6. *For* $g \in \mathcal{G}(I)$ *define*

$$f_g: G_{\mu_g}^3 \longrightarrow G_{\mu_g}$$

by

(M″) $\quad f_g(x, y, z) := g(z, g(x, e, e, y, z), e, e, e).$

(i) $\quad f(x, y, z) = f(x, i, j) f\left(j, g(x, y, z, i, j), z\right)$

holds for $f = f_g$. *This equation reflects exactly the position of the indices in the cube multiplication* (M′).

(ii) $\quad \Phi: \mathcal{G}(I) \longrightarrow \mathcal{F}(I), \quad \Phi(g) := (\mu_g, f_g)$

is bijective.

(iii) *In particular if* $(\mu, f) \in \mathcal{F}(I)$ *is given, then* Eq. (M″), *to be read in* G_μ, *determines* $g = \Phi^{-1}\left((\mu, f)\right)$ *uniquely.*

Proof. (i) Let

$$\omega(x, y) := g(x, y, e, e, e).$$

Then

(9) $$g(zyeie) = g[e, g(zyeee), e, g(zieee), e] \quad \text{by (G2)}$$
$$= \omega(z, y)\omega(z, i)^{-1}$$

by Corollary 5, and hence

(10) $$\omega(x, y) = g(xyeee)$$
$$= g[z, g(xyeiz), e, g(xeeiz), e] \quad \text{by (G2)}$$
$$= \omega\left(z, g(xyeiz)\right) \omega\left(z, g(xeeiz)\right)^{-1}$$

by (9). This shows

$$\begin{aligned} f_g(xyz) &= \omega[z, g(xeeyz)] \\ &= \omega[z, g[j, g(xeeij), e, g(xyzij), z]] && \text{by (G2)} \\ &= \omega[j, g(xeeij)]\omega[z, g[j, e, e, g(xyzij), z]] && \text{by (10)} \\ &= f_g(xij) f_g\left(j, g(xyzij), z\right). \end{aligned}$$

(ii) First we show that f_g satisfies (F1)–(F4):
(F1) is an immediate consequence of (G4).
(F2):

$$\begin{aligned} f_g(eye) &= g\left(e, g(eeeye), e, e, e\right) \\ &= g(eeeye) && \text{by (G6)} \\ &= y^{-1} && \text{by Corollary 5.} \end{aligned}$$

(F3):

$$\begin{aligned} f_g(xee) &= g\left(e, g(xeeee), e, e, e\right) \\ &= g(xeeee) && \text{by (G6)} \\ &= e && \text{by (G5).} \end{aligned}$$

(F4):

$$\begin{aligned} f_g(xxx) &= f_g\left(x, g(xxxxx), x\right) && \text{by (G3)} \\ &= f_g(xxx)^{-1} f_g(xxx) && \text{by (M'')} \\ &= e. \end{aligned}$$

Hence $(\mu_g, f_g) \in \mathcal{F}(I)$ for every $g \in \mathcal{G}(I)$.

Now we show that Φ is injective: Assume that there are $g_1, g_2 \in \mathcal{G}(I)$ such that

$$\mu_{g_1} = \mu_{g_2} =: \mu \quad \text{and} \quad f_{g_1} = f_{g_2} =: f.$$

Then (M″) yields

$$\begin{aligned} \mu[f(xij), f\left(j, g_1(xyzij), z\right)] &= f(xyz) \\ &= \mu[f(xij), f\left(j, g_2(xyzij), z\right)]. \end{aligned}$$

μ is injective in its second argument because it is a group mapping, and f is injective in its second argument by (F1). Hence $g_1 = g_2$.

To prove that Φ is surjective, take any $(\mu, f) \in \mathcal{F}(I)$. We will define $g \in \mathcal{G}(I)$ in the group G_μ such that $\Phi(g) = (\mu, f)$. By definition of $\mathcal{F}(I)$, $f\colon G_\mu^3 \longrightarrow G_\mu$ satisfies (F1)–(F4). In particular, (F1) implies that the equation

$$\text{(M}'''\text{)} \qquad f\left(j, g(xyzij), z\right) := f(xij)^{-1} f(xyz)$$

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press

determines a mapping $g: I^5 \to I$. Now we show that

(I) g satisfies (G1)–(G3), and hence $g \in \mathcal{G}(I)$,

(II) $\mu_g = \mu$,

(III) $f_g = f$.

ad (I): The definition of g in (M‴) shows that (F1) implies (G1).

$$\begin{aligned} & f[j, g[l, g(xyzkl), z, g(xijkl), j], z] \\ & = f\left(l, g(xijkl), j\right)^{-1} f\left(l, g(xyzkl), z\right) && \text{by (M}''')\\ & = [f(xkl)^{-1} f(xij)]^{-1}[f(xkl)^{-1} f(xyz)] && \text{by (M}''')\\ & = f(xij)^{-1} f(xyz) \\ & = f[j, g(xyzij), z] \end{aligned}$$

by (M‴), and the injectivity of f in its second argument yields (G2).

$$\begin{aligned} f\left(x, g(xxxxx), x\right) &= e && \text{by (M}''')\\ &= f(xxx) \end{aligned}$$

by (F4), hence with (F1), $g(xxxxx) = x$, i.e., (G3).

ad (II): We have to show $\mu_g(x, y) = xy$ in G_μ with μ_g as defined in Proposition 4.

$$\begin{aligned} \mu_g(x, y)^{-1} &= f\left(e, \mu_g(x, y), e\right) && \text{by (F2)}\\ &= f[e, g[e, x, e, g(eeeye), e], e] && \text{by definition of } \mu_g\\ &= f\left(e, g(eeeye), e\right)^{-1} f(exe) && \text{by (M}''')\\ &= [f(eye)^{-1} f(eee)]^{-1} f(exe) && \text{by (M}''')\\ &= f(eye) f(exe) && \text{by (F4)}\\ &= y^{-1} x^{-1} && \text{by (F2).} \end{aligned}$$

ad (III): We have $g \in \mathcal{G}(I)$ by (I). Hence (i) shows that in G_{μ_g} Eq. (M″) holds for f_g, and further $G_{\mu_g} = G_\mu$ as shown in (II).

$$\begin{aligned} (11) \qquad f_g(xye) &= f_g(xee)^{-1} f_g(xye) && \text{by (F3)}\\ &= f_g\left(e, g(xyeee), e\right) && \text{by (M}'')\\ &= g(xyeee)^{-1} && \text{by (F2) for } f_g\\ &= f\left(e, g(xyeee), e\right) && \text{by (F2) for } f\\ &= f(xee)^{-1} f(xye) && \text{by (M}''')\\ &= f(xye) && \text{by (F3).} \end{aligned}$$

Now finally

$$\begin{aligned} f_g(xij)^{-1} f_g(xye) &= f_g\left(j, g(xyeij), e\right) && \text{by (M}'')\\ &= f\left(j, g(xyeij), e\right) && \text{by (11)}\\ &= f(xij)^{-1} f(xye) \end{aligned}$$

by (M‴), and (11) yields

$$f_g(xij)^{-1} = f(xij)^{-1},$$

hence $f_g = f$.

The proof of (iii) is contained in the proof of (ii).

Remarks. (1) Theorem 6 shows that all associative multiplications of type (M′) on $\mathcal{W}(I, K)$ with unit element $\mathcal{E}$ can be constructed by

– first imposing any group structure G on I,
– then taking any mapping $f\colon G^3 \longrightarrow G$ which satisfies (F1)–(F4),
– finally calculating $g\colon I^5 \longrightarrow I$ out of (M″).

(2) *Examples.* Let G be a finite group. The following table lists all mappings $f\colon G^3 \longrightarrow G$ of the form

$$f(x, y, z) = \prod_{1 \leqq m \leqq 4} X_m^{\epsilon_m}, \quad X_m \in \{x, y, z\}, \epsilon_m \in \{0, 1, -1\},$$

which satisfy (F1)–(F4). The column beside it contains the corresponding mappings g:

$f(x,y,z)$	$g(x,y,z,i,j)$
$y^{-1}z$	$yi^{-1}j$ ("standard example $\mathcal{W}(G, K)$")
zy^{-1}	$yz^{-1}ji^{-1}z$
$z^{-1}y^{-1}z^2$	$yzj^{-1}i^{-1}j^2z^{-1}$
$z^2y^{-1}z^{-1}$	$yz^{-2}j^2i^{-1}j^{-1}z^2$
$xy^{-1}x^{-1}z$	$j^{-1}xyi^{-1}x^{-1}j^2$
$zx^{-1}y^{-1}x$	$jx^{-1}yxz^{-1}jx^{-1}i^{-1}xzj^{-1}$
$x^{-1}y^{-1}xz$	$jx^{-1}yi^{-1}x$
$zxy^{-1}x^{-1}$	$j^{-1}xyx^{-1}z^{-1}jxi^{-1}x^{-1}zj$
$xy^{-1}zx^{-1}$	$zj^{-1}xz^{-1}yi^{-1}jx^{-1}j$
$x^{-1}zy^{-1}x$	$jx^{-1}yz^{-1}ji^{-1}xj^{-1}z$
$x^{-1}y^{-1}zx$	$zjx^{-1}z^{-1}yi^{-1}jxj^{-1}$
$xzy^{-1}x^{-1}$	$j^{-1}xyz^{-1}ji^{-1}x^{-1}jz$
$xzx^{-1}y^{-1}$	$yxz^{-1}jx^{-1}i^{-1}jzj^{-1}$
$y^{-1}x^{-1}zx$	$j^{-1}zjx^{-1}z^{-1}xyi^{-1}x^{-1}jx$
$x^{-1}zxy^{-1}$	$yx^{-1}z^{-1}jxi^{-1}j^{-1}zj$
$y^{-1}xzx^{-1}$	$jzj^{-1}xz^{-1}x^{-1}yi^{-1}xjx^{-1}$

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press

(3) An easy calculation shows that for a group G of order n there exist $(n!)^{n^2-1}n^{2-2n}$ different mappings $f\colon G^3 \longrightarrow G$ satisfying (F1)–(F4). The next theorem shows that the corresponding K-algebras $\mathcal{W}(g,K)$ are all isomorphic:

THEOREM 7. *Let $g \in \mathcal{G}(I)$, $\Phi(g) = (\mu,f)$, $G = G_\mu$, and let $f^*\colon G^3 \longrightarrow G$ denote the inverse of f with respect to its second argument, i.e., $f^*(x,f(x,y,z),z) = y$.*

$$\Psi\colon \mathcal{W}(g,K) \longrightarrow K[G] \otimes_K M(G,K),$$
$$\Psi\left((\alpha_{xyz})\right) : = \sum_{y\in G} y \otimes (\alpha_{x,f^*(xyz),z})_{x,z\in G}$$

is a K-algebra isomorphism from $\mathcal{W}(g,K)$ onto the tensor product of the group algebra of G over K and the algebra of square matrices $(\beta_{xz})_{x,z\in G}$ over K.

Proof. Ψ is K-linear and bijective, for f^* is bijective in its second argument by definition. It only remains to prove the multiplicativity of Ψ:

$$\begin{aligned}\Psi(\mathcal{A})\Psi(\mathcal{B}) &= \left(\sum_u u \otimes (\alpha_{x,f^*(xuz),z})_{x,z}\right)\left(\sum_v v \otimes (\beta_{x,f^*(xvz),z})_{x,z}\right)\\ &= \sum_{u,v} uv \otimes \left(\sum_j \alpha_{x,f^*(xuj),j}\, \beta_{j,f^*(jvz),z}\right)_{x,z}\\ &= \sum_y y \otimes \left(\sum_{i,j} \alpha_{x,f^*(xij),j}\, \beta_{j,f^*(j,i^{-1}y,z),z}\right)_{x,z}.\end{aligned}$$

$$\begin{aligned}\Psi(\mathcal{A}\mathcal{B}) &= \Psi\left(\left(\sum_{i,j} \alpha_{xij}\beta_{j,g(xyzij),z}\right)_{x,y,z}\right)\\ &= \sum_y y \otimes \left(\sum_{i,j} \alpha_{xij}\beta_{j,g(x,f^*(xyz),z,i,j),z}\right)_{x,z}\\ &= \sum_y y \otimes \left(\sum_{i,j} \alpha_{x,f^*(xij),j}\, \beta_{j,g(x,f^*(xyz),z,f^*(xij),j),z}\right)_{x,z}.\end{aligned}$$

And, by definition of f^*:

$$\begin{aligned}f\left(j,f^*(j,i^{-1}y,z),z\right) &= i^{-1}y\\ &= f\left(x,f^*(xij),j\right)^{-1} f\left(x,f^*(xyz),z\right)\\ &= f[j,g[x,f^*(xyz),z,f^*(xij),j],z]\end{aligned}$$

by (M″), which, by (F1), yields

$$f^*(j,i^{-1}y,z) = g\left(x,f^*(xyz),z,f^*(xij),j\right).$$

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press

COROLLARY 8. *For $g \in \mathcal{G}(I)$, $\Phi(g) = (\mu_g, f_g)$, and $G = G_{\mu_g}$,*

$$\psi_g\left((\alpha_{xyz})_{x,y,z}\right) = (\alpha_{x,z\,f_g(xyz)^{-1},z})_{x,y,z}$$

is a K-algebra isomorphism from the standard example $\mathcal{W}(G,K)$ onto $\mathcal{W}(g, K)$.

Proof. Concerning the standard example we have $f(x,y,z) = y^{-1}z$ and hence $f^*(x,y,z) = zy^{-1}$.

$$\Psi_1 \colon \mathcal{W}(G,K) \longrightarrow K[G] \otimes M(G,K),$$
$$\Psi_1\left((\alpha_{xyz})\right) = \sum_y y \otimes (\alpha_{x,zy^{-1},z})_{x,z},$$
$$\Psi_2 \colon \mathcal{W}(g,K) \longrightarrow K[G] \otimes M(G,K),$$
$$\Psi_2\left((\alpha_{xyz})\right) = \sum_y y \otimes (\alpha_{x,f_g^*(xyz),z})_{x,z}$$

are isomorphisms by Theorem 7, and

$$\Psi_2^{-1}\left(\sum_y y \otimes (\alpha_{xyz})_{x,z}\right) = (\alpha_{x,f_g(xyz),z})_{x,y,z}.$$

Hence $\psi_g = \Psi_2^{-1} \circ \Psi_1$ is an isomorphism, too.

The cube multiplication (M′)

$$\gamma_{xyz} = \sum_{i,j \in I} \alpha_{xij}\beta_{j,g(xyzij),z}$$

was introduced as an imitation of the matrix multiplication

$$\gamma_{xz} = \sum_{i \in I} \alpha_{xi}\beta_{g_o(xzi),z}, \qquad g_o(x,z,i) = i.$$

In fact $g_o(x,z,i) = i$ is the only mapping $I^3 \longrightarrow I$ which makes the matrix multiplication associative with unit element $E = (\delta_{x,z})_{x,z}$. Uniqueness arises for the cube multiplication, too, when, in accordance with g_o, one demands that g is independent of its horizontal plane index x and its vertical plane index z. Then the resulting cube algebras are exactly the standard examples $\mathcal{W}(G,K)$.

PROPOSITION 9. *Let $g \in \mathcal{G}(I)$. $g(x,y,z,i,j)$ is independent of x and z if and only if*

$$g(x,y,z,i,j) = yi^{-1}j$$

in G_{μ_g}, i.e., if $\mathcal{W}(g,K)$ is the standard example $\mathcal{W}(G_{\mu_g},K)$.

Proof. Assume that $g(x,y,z,i,j)$ is independent of x and z. Then

$$\begin{aligned} f_g(xye) &= g\left(e, g(xeeye), e, e, e\right) && \text{by definition of } f_g \\ &= g\left(e, g(eeeye), e, e, e\right) && \text{by assumption} \\ &= y^{-1} && \text{by Corollary 5.} \end{aligned}$$

Hence

$$\begin{aligned} f_g(xyz) &= f_g(xye) f_g(z, g(xyeyz), e)^{-1} && \text{by (M}'') \\ &= y^{-1} g(xyeyz) && \\ &= y^{-1} g(xyzyz) && \text{by assumption} \\ &= y^{-1} z && \text{by (G5).} \end{aligned}$$

Finally, (M″) shows that

$$f_g(x,y,z) = y^{-1}z$$

implies

$$g(x,y,z,i,j) = yi^{-1}j.$$

2. The matrices can be viewed as linear mappings between spaces of column vectors. Similarly we will interpret the cubes as linear mappings between spaces of matrices. Let $g \in \mathcal{G}(I)$, $\Phi(g) = (\mu, f)$, $G = G_\mu$, and $n = |G|$. For $u \in G$ one has the canonical (untwisted) embeddings and projections between the matrix algebra $M(G,K)$ and the standard example $\mathcal{W}(G,K)$:

$$\begin{aligned} \iota_u^o &: M(G,K) \longrightarrow \mathcal{W}(G,K), \\ \iota_u^o\left((\beta_{xy})_{x,y\in G}\right) &:= (\beta_{xy}\delta_{u,z})_{x,y,z\in G}, \\ p_u^o &: \mathcal{W}(G,K) \longrightarrow M(G,K), \\ p_u^o\left((\beta_{xyz})_{x,y,z\in G}\right) &:= (\beta_{xyu})_{x,y\in G}. \end{aligned}$$

They allow one to define an operation of $\mathcal{A} \in \mathcal{W}(g,K)$ on $M(G,K)$ via the multiplication in $\mathcal{W}(g,K)$ exactly as $M(G,K)$ operates on K^n:

$$\mathcal{A}(B) := p_u^o\left(\mathcal{A}\,\iota_u^o(B)\right), \quad B \in M(G,K).$$

But computing coefficients shows

$$\mathcal{A}(B) = \left(\sum_{i,j} \alpha_{xij}\beta_{j,g(xyuij)}\right)_{x,y\in G},$$

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press

hence this operation may depend on the choice of $u \in G$, if one does not take the standard multiplication

$$g(x, y, z, i, j) = yi^{-1}j$$

on the underlying set $\mathcal{W}(I, K)$. To avoid this one has to use twisted embeddings and projections, and the adequate twist is the isomorphism ψ_g of Corollary 8:

$$\begin{aligned}
\iota_u &: M(G,K) \longrightarrow \mathcal{W}(g,K), \\
\iota_u &:= \psi_g \circ \iota_u^o, \\
\iota_u\left((\beta_{xy})\right) &= (\beta_{x,zf(xyz)^{-1}}\delta_{u,z})_{x,y,z}, \\
p_u &: \mathcal{W}(g,K) \longrightarrow M(G,K), \\
p_u &:= p_u^o \circ \psi_g^{-1}, \\
p_u\left((\beta_{xyz})\right) &= (\beta_{x,f^*(x,y^{-1}u,u),u})_{x,y},
\end{aligned}$$

where as in Theorem 7 f^* is the inverse of f with respect to its second argument. If $\mathcal{W}(g,K) = \mathcal{W}(G,K)$ is a standard example, then $\iota_u = \iota_u^o$ and $p_u = p_u^o$ and the twist disappears.

The twisted embeddings and projections have the usual properties: Let

$$\mathcal{E}_u := (\delta_{x,u}\delta_{y,u}\delta_{z,u})_{x,y,z}, \quad u \in G,$$

denote the canonical idempotents of $\mathcal{W}(g,K)$ and $\mathcal{W}_u := \mathcal{W}(g,K)\mathcal{E}_u$ the corresponding left ideals. Then

$$\text{(12)} \qquad \mathcal{E}_u\mathcal{E}_v = \delta_{u,v}\mathcal{E}_u, \quad \sum_{u\in G}\mathcal{E}_u = \mathcal{E},$$

$$\text{(13)} \qquad p_u \circ \iota_v = \delta_{u,v}\mathrm{id}_{M(G,K)},$$

$$\text{(14)} \qquad (\iota_u \circ p_u)|\mathcal{W}_v = \delta_{u,v}\mathrm{id}_{\mathcal{W}_v},$$

$$\text{(15)} \qquad \sum_{u\in G}\iota_u \circ p_u = \mathrm{id}_{\mathcal{W}(g,K)}.$$

Now we define the operation of $\mathcal{A} \in \mathcal{W}(g,K)$ on $M(G,K)$ by

$$\mathcal{A}^{\phi}(B) := \left(\sum_{i,j}\alpha_{xij}\beta_{j,yf(xij)}\right)_{x,y}.$$

This yields the desired independence of u and hence corresponds to the matrix situation.

PROPOSITION 10. *$\mathcal{A}^{\phi}(B) = p_u\left(\mathcal{A}\,\iota_u(B)\right)$ for all $u \in G$.*

Proof.

$$\begin{aligned} p_u\left(\mathcal{A}\,\iota_u(B)\right) &= p_u\left((\alpha_{xyz})(\beta_{x,zf(xyz)^{-1}}\delta_{u,z})_{x,y,z}\right) \\ &= p_u\left(\left(\sum_{i,j}\alpha_{xij}\beta_{j,zf}(j,g(xyzij),z)^{-1}\delta_{u,z}\right)_{x,y,z}\right) \\ &= \left(\sum_{i,j}\alpha_{xij}\beta_{j,uf[j,g(x,f^*(x,y^{-1}u,u),u,i,j),u]^{-1}}\right)_{x,y} \\ &= \left(\sum_{i,j}\alpha_{xij}\beta_{j,yf(xij)}\right)_{x,y}, \end{aligned}$$

for

$$\begin{aligned} y^{-1}u &= f\left(x,f^*(x,y^{-1}u,u),u\right) \\ &= f(xij)f[j,g\left(x,f^*(x,y^{-1}u,u),u,i,j\right)u] \quad \text{by} \quad (\mathrm{M}''). \end{aligned}$$

ϕ: $\mathcal{W}(g,K) \longrightarrow \mathrm{End}_K M(G,K)$, $\mathcal{A} \longmapsto \mathcal{A}^{\phi}$, is K-linear and injective into the endomorphism algebra of $M(G,K)$, and the multiplication in $\mathcal{W}(g,K)$ becomes the composition of mappings in $\mathrm{End}_K M(G,K)$:

$$\begin{aligned} (\mathcal{A}^{\phi}\circ\mathcal{B}^{\phi})(C) &= \mathcal{A}^{\phi}\left(p_u(\mathcal{B}\,\iota_u(C))\right) \\ &= p_u[\mathcal{A}\,(\iota_u\circ p_u)(\mathcal{B}\,\iota_u(C))] \\ &= p_u[\mathcal{A}\,(\mathcal{B}\,\iota_u(C))] \quad \text{by} \quad (14) \\ &= p_u[(\mathcal{A}\mathcal{B})\iota_u(C)] \quad \text{by the associative law in } \mathcal{W}(g,K) \\ &= (\mathcal{A}\mathcal{B})^{\phi}(C). \end{aligned}$$

Thus $\mathcal{W}(g,K)$ can be viewed as a n^3-dimensional subalgebra in the K-algebra $\mathrm{End}_K M(G,K)$ of dimension n^4. This subalgebra can be characterized by imposing $K[G]$-module structures on $M(G,K)$ and $\mathcal{W}(g,K)$: Let

$$R: G \longrightarrow M(G,K)^{\times}, \quad R(u) := (\delta_{x,uy})_{x,y\in G}$$

denote the regular representation of G. By

$$Bu := BR(u), \quad B \in M(G,K), \quad u \in G$$

and linear continuation $M(G,K)$ becomes a $K[G]$-module. Similarly

$$\mathcal{R}: G \longrightarrow \mathcal{W}(g,K)^{\times}, \quad \mathcal{R}(u) := (\delta_{zf(xyz)z^{-1},u}\,\delta_{x,z})_{x,y,z\in G}$$

is an injective group morphism, and by

$$\mathcal{B}u := \mathcal{B}\mathcal{R}(u), \quad \mathcal{B} \in \mathcal{W}(g,K), \quad u \in G$$

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press

and linear continuation $\mathcal{W}(g,K)$ becomes a $K[G]$-module, too.

A straightforward calculation shows that the $K[G]$-module structures on $\mathcal{W}(G,K)$ and $\mathcal{W}(g,K)$ are compatible with the isomorphism

$$\psi_g\colon \mathcal{W}(G,K) \longrightarrow \mathcal{W}(g,K)$$

of Corollary 8:

$$\psi_g(\mathcal{B}u) = \psi_g(\mathcal{B})u.$$

Further, the $K[G]$-module structures on $M(G,K)$ and $\mathcal{W}(g,K)$ are compatible with the twisted embeddings and projections:

$$\iota_v(Bu) = \iota_v(B)u, \tag{16}$$

$$p_v(\mathcal{B}u) = p_v(\mathcal{B})u. \tag{17}$$

Finally the mappings $\mathcal{A}^{\phi}$, $\mathcal{A} \in \mathcal{W}(g,K)$, respect the $K[G]$-module structure on $M(G,K)$:

$$\mathcal{A}^{\phi}(Bu) = \mathcal{A}^{\phi}(B)u.$$

This turns out to be a consequence of the associative law in $\mathcal{W}(g,K)$:

$$\begin{aligned}\mathcal{A}^{\phi}(Bu) &= p_v\left(\mathcal{A}\,\iota_v(Bu)\right)\\ &= p_v\left(\mathcal{A}\,(\iota_v(B)\mathcal{R}(u))\right) && \text{by (16)}\\ &= p_v\left((\mathcal{A}\,\iota_v(B))\mathcal{R}(u)\right) && \text{by the associative law in } \mathcal{W}(g,K)\\ &= p_v\left(\mathcal{A}\,\iota_v(B)\right)u && \text{by (17)}\\ &= \mathcal{A}^{\phi}(B)u.\end{aligned}$$

Thus the cubes in $\mathcal{W}(g,K)$ can be interpreted as endomorphisms of the $K[G]$-module $M(G,K)$.

THEOREM 11. $\phi\colon \mathcal{W}(g,K) \longrightarrow \mathrm{End}_{K[G]}M(G,K)$, $\mathcal{A} \longmapsto \mathcal{A}^{\phi}$, *is a* K*-algebra isomorphism.*

COROLLARY 12. *Let* $\{E_u := (\delta_{u,x}\delta_{u,y})_{x,y};\ u \in G\}$ *denote the canonical* $K[G]$*-basis of* $M(G,K)$. *Then*

$$\mathcal{A}^{\phi}(E_u) = p_u(\mathcal{A}),$$

i.e., the images of the canonical basis elements under $\mathcal{A}^{\phi}$ *are the twisted vertical planes of* $\mathcal{A}$. *In particular* $\mathcal{A}$ *is invertible if and only if its twisted vertical planes form a* $K[G]$*-basis of* $M(G,K)$.

Proof of Theorem 11. It only remains to show that ϕ is surjective. Take $\eta \in \mathrm{End}_{K[G]}M(G,K)$ and define for $u \in G$:

$$(\alpha_{xyu})_{x,y} := \eta(E_u), \quad \mathcal{A} := (\alpha_{xyz}) \in \mathcal{W}(G,K).$$

Then for $\psi_g(\mathcal{A}) \in \mathcal{W}(g,K)$,

$$\begin{aligned}(\psi_g(\mathcal{A}))^{\phi}(E_u) &= p_u\left(\psi_g(\mathcal{A})\iota_u(E_u)\right)\\ &= p_u\left(\psi_g(\mathcal{A})\mathcal{E}_u\right)\\ &= p_u\left(\psi_g(\mathcal{A}\mathcal{E}_u)\right) \quad \text{since } \psi_g(\mathcal{E}_u) = \mathcal{E}_u\\ &= p_u^o(\mathcal{A}\mathcal{E}_u) \quad \text{by definition of } p_u\\ &= (\alpha_{xyu})_{x,y}\\ &= \eta(E_u),\end{aligned}$$

hence

$$\psi_g(\mathcal{A})^{\phi} = \eta.$$

Proof of Corollary 12.

$$\mathcal{A}^{\phi}(E_u) = p_u\left(\mathcal{A}\,\iota_u(E_u)\right) = p_u(\mathcal{A}\mathcal{E}_u) = p_u(\mathcal{A}).$$

In the case of the standard example the analogy to the matrix situation becomes obvious.

COROLLARY 13. *$\mathcal{A} = (\alpha_{xyz}) \in \mathcal{W}(G,K)$ is invertible if and only if the vertical planes $(\alpha_{xyz})_{x,y\in G}$, $z \in G$, of $\mathcal{A}$ form a basis of the right $K[G]$-module $M(G,K)$.*

Remark. Similarly, one can define the embeddings ι_u and the projections p_u via the horizontal planes of the cubes. If then $\mathcal{B} \in \mathcal{W}(g,K)$ operates on $M(G,K)$ from the right side,

$$(A)^{\phi}\mathcal{B} = p_u\left(\iota_u(A)\mathcal{B}\right),$$

one can show that $\mathcal{B}$ is invertible if and only if its (twisted) horizontal planes form a basis of $M(G,K)$ as a left $K[G]$-module.

THEOREM 14. *Let $g \in \mathcal{G}(I)$. Then for every $u \in I$*

$$\iota\colon \mathcal{W}(g,K) \longrightarrow M(I^2,K),$$
$$\iota\left((\alpha_{xyz})_{x,y,z\in I}\right) := (\alpha_{j,g(uvwij),w})_{(i,j),(v,w)\in I^2}$$

is an injective K-algebra morphism.

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press

Proof. ι is K-linear, and (G4) implies the injectivity.

$$\begin{aligned}
\iota(\mathcal{E}) &= \iota\left((\delta_{x,z}\delta_{y,z})\right) \\
&= (\delta_{j,w}\delta_{g(uvwij),w})_{(i,j),(v,w)} \\
&= (\delta_{j,w}\delta_{g(uvwiw),w})_{(i,j),(v,w)} \\
&= (\delta_{j,w}\delta_{i,v})_{(i,j),(v,w)},
\end{aligned}$$

for $g(u,v,w,i,w) = w$ if and only if $i = v$, by (G5) and (G1).

$$\begin{aligned}
\iota(\mathcal{A}\mathcal{B}) &= \iota\left(\left(\sum_{r,s}\alpha_{xrs}\beta_{s,g(xyzrs),z}\right)_{x,y,z}\right) \\
&= \left(\sum_{r,s}\alpha_{jrs}\beta_{s,g(j,g(uvwij),w,r,s),w}\right)_{(i,j),(v,w)} \\
&= \left(\sum_{r,s}\alpha_{j,g(ursij),s}\beta_{s,g[j,g(uvwij),w,g(ursij),s],w}\right) && \text{by (G4)} \\
&= \left(\sum_{r,s}\alpha_{j,g(ursij),s}\beta_{s,g(uvwrs),w}\right)_{(i,j),(v,w)} && \text{by (G2)} \\
&= (\alpha_{j,g(ursilj),s})_{(i,j),(r,s)}(\beta_{s,g(uvwrs),w})_{(r,s),(v,w)} \\
&= \iota(\mathcal{A})\iota(\mathcal{B}).
\end{aligned}$$

The injection ι can be used to transfer the eigenvalue theory from the square matrices to the cubes. Let us call the monic polynomial

$$\chi_{\mathcal{A}}(X) := \det\left(XE - \iota(\mathcal{A})\right) \in K[X]$$

of degree n^2 the characteristic polynomial of $\mathcal{A} \in \mathcal{W}(g,K)$. It is invariant with respect to conjugation of $\mathcal{A}$:

$$\chi_{\mathcal{B}^{-1}\mathcal{A}\mathcal{B}}(X) = \chi_{\mathcal{A}}(X).$$

The "eigenvalues" of $\mathcal{A}$ are the roots of $\chi_{\mathcal{A}}(X)$. If $\lambda \in K$ is an eigenvalue of $\mathcal{A}$, then the eigenspace $E(\mathcal{A},\lambda)$ of $\mathcal{A}$, consisting of the eigenmatrices corresponding to λ,

$$E(\mathcal{A},\lambda) := \{B \in M(G,K);\ \mathcal{A}^{\phi}(B) = \lambda B\}$$

is a non-trivial $K[G]$-submodule of $M(G,K)$. Different eigenspaces of $\mathcal{A}$ have intersection $\{o\}$. Further we call

$$\det \mathcal{A} := (-1)^{N^2}\chi_{\mathcal{A}}(o) = \det(\iota(\mathcal{A}))$$

the determinant of $\mathcal{A}$. Then $\mathcal{A}$ is invertible in $\mathcal{W}(g,K)$ if and only if $\det \mathcal{A} \neq o$.

PROPOSITION 15. *$\mathcal{A} \in \mathcal{W}(g,K)$ is diagonalizable if and only if $M(G,K)$ is the sum of the eigenspaces of $\mathcal{A}$.*

Proof. Suppose first that $\mathcal{A}$ is diagonalizable, i.e., that

$$\mathcal{B}^{-1}\mathcal{A}\mathcal{B} = \sum_{z\in G} \lambda_z \mathcal{E}_z, \quad \lambda_z \in K,$$

for some $\mathcal{B} \in \mathcal{W}(g,K)^{\times}$. Then

$$\begin{aligned} \mathcal{A}^{\phi}(p_u(\mathcal{B})) &= p_u\left(\mathcal{A}(\iota_u \circ p_u)(\mathcal{B})\right) \quad \text{by Proposition 10} \\ &= p_u(\mathcal{A}\mathcal{B}) \\ &= p_u\left(\mathcal{B}\left(\sum_z \lambda_z \mathcal{E}_z\right)\right) \\ &= \lambda_u p_u(\mathcal{B}) \end{aligned}$$

by (14), and the twisted vertical planes $p_u(\mathcal{B})$, $u \in G$, of $\mathcal{B}$ form a $K[G]$-basis of $M(G,K)$ by Corollary 12.

Conversely, if the matrices B_u, $u \in G$, form a $K[G]$-basis of $M(G,K)$ and

$$\mathcal{A}^{\phi}(B_u) = \lambda_u B_u, \quad \lambda_u \in K, \quad u \in G,$$

then with

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press

$$\begin{aligned}
\mathcal{B} &:= \sum_u \iota_u(B_u) \quad \text{and} \quad \mathcal{D} := \sum_z \lambda_z \mathcal{E}_z, \\
\mathcal{B}\mathcal{D} &= \left(\sum_u \iota_u(B_u)\right)\left(\sum_z \lambda_z \mathcal{E}_z\right) && \text{by (A2)} \\
&= \sum_u \iota_u(\lambda_u B_u) \\
&= \sum_u \iota\left(\mathcal{A}^{\phi}(B_u)\right) && \text{by Proposition 2} \\
&= \sum_u (\iota_u \circ p_u)\left(\mathcal{A}\,\iota_u(B_u)\right) && \text{by (A4)} \\
&= \sum_u (\iota_u \circ p_u)\left(\mathcal{A} \sum_v \iota_v(B_v)\right) \\
&= \mathcal{A}\mathcal{B}
\end{aligned}$$

by (15), and

$$p_v(\mathcal{B}) = p_v\left(\sum_u \iota_u(B_u)\right) = B_v, \quad v \in G,$$

is a $K[G]$-basis of $M(G, K)$, hence $\mathcal{B}$ is invertible by Corollary 12.

Technische Universität,
München, Germany

https://doi.org/10.4153/CJM-1989-024-5 Published online by Cambridge University Press