MULTIPLICATIVE HOMOMORPHISMS OF MATRICES

ELIOT CHAMBERLIN AND JAMES WOLFE

G will denote a system closed under a multiplication. An element $e \in G$ is called an *identity* if $ae = ea = a$ for every $a \in G$. An element $0 \in G$ is called a *null element* if $0a = a0 = 0$ for every $a \in G$. Clearly e and 0 are unique if they exist; $e = 0$ if and only if G has just one element. A *square root* of the identity is an element $q \in G$ such that $q^2 = e$. Let $H \subset G$ be the set consisting of the square roots of the identity in G and the null element if it exists. We assume throughout that the elements of H commute with each other. If G is a ring with identity and without divisors of zero and with ring multiplication as multiplication in G , then H consists of $0, e, -e$ and these commute with every element of G , for if $q^2 = e$, $(q - e)(q + e) = 0$ and $q = \pm e$.

R will always denote a ring with identity, and $\mathfrak{M}_n$ will denote the set of $n \times n$ matrices with elements in R . Let $M_i(c), E_{ij}, A_{ij}(c)$ ($i \neq j$) be the matrices resulting respectively from the identity matrix I by multiplying row i by c , interchanging rows i and j , and adding row i multiplied by c to row j ; these will be called *elementary matrices*. Let $\mathfrak{M}_n^*$ denote the set of matrices in $\mathfrak{M}_n$ which are products of elementary matrices.

For some rings R , $\mathfrak{M}_n^* = \mathfrak{M}_n$; if R is such a ring and θ is a homomorphism of R onto a ring R' , then $\mathfrak{M}'_n = \mathfrak{M}_n'$ where the prime refers to matrices with elements in R' . For θ induces in a natural way a homomorphism θ of $\mathfrak{M}_n$ onto $\mathfrak{M}_n'$ (merely let θ act on each element of the matrix) in which the image of an elementary matrix is elementary. Suppose that a nonnegative integral absolute value $|a|$ is defined in R subject only to the conditions that for every $b \neq 0$ and a in R , $a = bq + r$ and $a = q'b + r'$ where $|r|, |r'| < |b|$. Then the usual procedure can be used to reduce a matrix in $\mathfrak{M}_n$ to diagonal form by left and right multiplications by elementary matrices with inverses; see [1, vol. 2, p. 120 ff.]. A diagonal matrix is a product of elementary matrices $M_i(c)$ and the inverse of an elementary matrix is elementary if it exists, hence if R has an absolute value as above, $\mathfrak{M}_n^* = \mathfrak{M}_n$. A skew field or field or any euclidean ring admits such an absolute value. If a ring R has such an absolute value and β is a homomorphism of R onto a ring S , then for $s \in S$ define $|s| = \min |r|$ for $\beta(r) = s$; this gives S an absolute value with the above properties.

A mapping Φ of $\mathfrak{M}_n$ or $\mathfrak{M}_n^*$ into G such that $\Phi(BC) = \Phi(B)\Phi(C)$ for every $B, C \in \mathfrak{M}_n$ or $\mathfrak{M}_n^*$ respectively, will be called a *multiplica-*

Received by the editors January 7, 1952.

tive matrix homomorphism. A mapping ϕ of R into G such that $\phi(uv) = \phi(u)\phi(v)$ for every $u, v \in R$ will be called a *multiplicative homomorphism*. The following simple facts will be used ordinarily without explicit reference.

LEMMA 1. (a) If Φ is a multiplicative matrix homomorphism of $\mathfrak{M}_n$ into G , then Φ confined to $\mathfrak{M}_n^*$ is a multiplicative matrix homomorphism of $\mathfrak{M}_n^*$ onto a multiplicatively closed subset of G .

If Φ is a multiplicative matrix homomorphism of $\mathfrak{M}_n$ or $\mathfrak{M}_n^*$ onto G , then: (b) Multiplication in G is associative. (c) G has a null element. (d) G has an identity.

The proof is obvious; for example the existence of the null and identity elements in G follows from the existence in $\mathfrak{M}_n^*$ of the zero and identity matrices O and I .

LEMMA 2. Suppose Φ is a multiplicative matrix homomorphism of $\mathfrak{M}_n^*$ onto G , then: (1) $[\Phi(E_{ij})]^2 = e$. (2) $\Phi(E_{ij}) = \Phi(E_{ji})$. (3) $[\Phi(M_i(-1))]^2 = e$. (4) $[\Phi(A_{ij}(c))]^2 = e$. (5) $\Phi(A_{ij}(c)) = \Phi(A_{ij}(-c))$. (6) $\Phi(A_{ij}(c)) = \Phi(A_{rk}(c))$. (7) $\Phi(E_{ij}) = \Phi(M_i(-1))\Phi(A_{ij}(1))$. (8) If $n > 2$, $\Phi(A_{ij}(c)) = e$. (9) If $n \neq 2$ or if the elements of H commute with every element of G , then $\Phi(M_i(c)) = \Phi(M_j(c))$. (10). If $n > 2$ or if $n = 2$ and the elements of H commute with every element of G , then G is commutative.

The following identities gives these results: (1) $E_{ij}E_{ij} = I$, hence $\Phi(E_{ij})\Phi(E_{ij}) = \Phi(I) = e$. (2) $E_{ij} = E_{ri}E_{rj}E_{ri}$ and $E_{ij} = E_{ji}$ and (1). (3) $M_i(-1)M_i(-1) = I$. (4) $M_i(-1)A_{ij}(c)M_i(-1)A_{ij}(c) = I$, hence $\Phi(M_i(-1))\Phi(A_{ij}(c))$ is a square root of e and (4) follows from (3). (5) $A_{ij}(-c) = M_i(-1)A_{ij}(c)M_i(-1)$ and (3) and (4). (6) $A_{ij}(c) = E_{jk}A_{ik}(c)E_{jk}$ and $A_{ij}(c) = E_{ij}A_{ji}(c)E_{ij}$. (7) $E_{ij} = M_i(-1)A_{ij}(1)A_{ji}(-1)A_{ij}(1)$. (8) $A_{ij}(c) = A_{kj}(-1)A_{ik}(-c)A_{kj}(1)A_{ik}(c)$ if i, j, k are distinct; then use (4) and (5). (9) $M_i(c) = E_{ij}M_j(c)E_{ij}$; if elements of H commute with every element of G then (1) gives the result. If $n = 1$, the result is obvious. If $n > 2$, using (2), $\Phi(M_1(c)) = \Phi(E_{13})\Phi(M_3(c))\Phi(E_{13}) = \Phi(M_2(c))$. Also $\Phi(M_2(c)) = \Phi(E_{ij})\Phi(M_1(c))\Phi(E_{ij})$; hence $\Phi(M_1(c)) = \Phi(E_{ij})\Phi(M_1(c))\Phi(E_{ij})$ and $\Phi(M_i(c)) = \Phi(M_j(c))$. (10) If $n \geq 2$, (9) and the hypotheses of (10) give $\Phi(M_i(c)) = \Phi(M_j(c))$. But $M_1(a)M_2(b) = M_2(b)M_1(a)$, hence all elements of G of the form $\Phi(M)$ commute with each other. Every element of G is a product of elements of the form $\Phi(M)$ and elements of H , hence G is commutative if the elements of H commute with every element of G . If $n > 2$, the last part of the proof of (9) shows that $\Phi(E)$ commutes with every $\Phi(M)$, also $\Phi(A) = e$ by (8). Then every element of G is a product of elements of the forms $\Phi(E)$ and $\Phi(M)$ and these all commute with each other.

If Φ is a multiplicative matrix homomorphism of $\mathfrak{M}_n^*$ onto G and $n \neq 2$ or the elements of H commute with every element of G , then $\Phi(M_i(c)) = \Phi(M_j(c))$. Define $\phi(c) = \Phi(M_i(c))$; ϕ is clearly a multiplicative homomorphism of R into G . ϕ will be said to be associated with Φ . For $B \in \mathfrak{M}_n$ the determinant $\det B$ is defined and if R is commutative, $\det BC = \det B \det C$ for every B and C ; if $n > 1$, this identity implies R is commutative.

THEOREM 1. *If R is commutative and $n \neq 2$, every multiplicative matrix homomorphism Φ of $\mathfrak{M}_n^*$ onto G is of the form $\Phi(B) = \phi(\det B)$ where ϕ is a multiplicative homomorphism of R into G uniquely determined by Φ .*

Take ϕ to be the multiplicative homomorphism associated with Φ . The result is clear if $n = 1$; assume $n > 2$. $\Phi(M_i(c)) = \phi(c) = \phi(\det M_i(c))$. By Lemma 2 part 8, $\Phi(A_{ij}(c)) = e = \phi(1) = \phi(\det A_{ij}(c))$ and by Lemma 2 part 7, $\Phi(E_{ij}) = \Phi(M_i(-1)) = \phi(-1) = \phi(\det E_{ij})$. Hence $\Phi(B) = \phi(\det B)$ for any elementary matrix, consequently for any matrix in $\mathfrak{M}_n^*$. If $\Phi(B) = \psi(\det B)$ for every $B \in \mathfrak{M}_n^*$, $\psi = \phi$ since $\psi(c) = \psi(\det M_i(c)) = \Phi(M_i(c)) = \phi(c)$.

COROLLARY. *If F is a commutative multiplicative system or a ring without divisors of zero, and if R is a field and Φ is a multiplicative matrix homomorphism of $\mathfrak{M}_n$ ($n \neq 2$) into F , then $\Phi = \phi(\det)$ where ϕ is a multiplicative homomorphism of R into F ; $\Phi(B) = \Phi(O)$ if $\det B = 0$. If $F = R$ and $\Phi(M_1(c)) = c$, $\Phi = \det$.*

For if F is commutative or a ring without divisors of zero, every multiplicatively closed subsystem of F is a system of type G . Then Lemma 1 and Theorem 1 give the result.

We shall use G^* to denote a system G with the properties: (i) The elements of H commute with every element of G . (ii) If $ab = 0$, $a = 0$ or $b = 0$. (iii) If $q \in H$ and $qa = a$ for some $a \neq 0$, then $q = e$. A ring without divisors of zero, under multiplication, and a group with a null element adjoined are examples of systems G^* . In a system G^* , $p = q$ if $p, q \in H$ and $pa = qa$ for some $a \neq 0$.

A multiplicative matrix homomorphism Ω of $\mathfrak{M}_2^*$ into G^* will be called *simple* if Ω maps $\mathfrak{M}_2^*$ into H , and the associated multiplicative homomorphism ω maps R into the set $\{0, e\} \subset G^*$.

THEOREM 2. *If R is commutative and Φ is a multiplicative matrix homomorphism of $\mathfrak{M}_2^*$ onto G^* , then $\Phi(B) = \Omega(B)\phi(\det B)$ where ϕ is a multiplicative homomorphism of R into G^* and Ω is simple and vanishes simultaneously with $\phi(\det)$. Such Ω and ϕ are uniquely determined by Φ .*

Let ϕ be the multiplicative homomorphism associated with Φ . By Lemma 2 parts (1) and (4), $\Phi(E)$ and $\Phi(A)$ are in H and are zero only if $\Phi \equiv 0$, similarly for $\phi(-1)$ and $\phi(1)$. Also $\Phi(M) = \phi(\det M)$, hence for any $B \in \mathfrak{M}_2^*$, $\Phi(B) = b\phi(\det B)$ where $b \in H$ and b can be taken to be zero if and only if $\phi(\det B) = 0$. Then such b is uniquely determined according to condition (iii) on G^* ; let $\Omega(B) = b$. Then $\Omega(B)\Omega(C)\phi(\det B)\phi(\det C) = \Phi(B)\Phi(C) = \Phi(BC) = \Omega(BC)\phi(\det B)\phi(\det C)$. If $\phi(\det B)$ or $\phi(\det C)$ is zero, $\Omega(B)\Omega(C) = 0$ and $\phi(\det BC) = 0$ hence $\Omega(BC) = 0$. If neither $\phi(\det B)$ nor $\phi(\det C)$ is zero, the product is not zero and $\Omega(B)\Omega(C) = \Omega(BC)$, hence Ω is multiplicative. $\Omega(M) \in \{0, e\}$, hence Ω is simple. If $\Phi(B) \equiv \Omega'(B)\phi'(\det B)$ where Ω' and $\phi'(\det)$ vanish simultaneously, replacing B by $M_1(c)$ shows $\phi' \equiv \phi$; clearly then $\Omega' \equiv \Omega$.

If Φ in Theorem 2 is simple, $\Omega = \Phi$. Every multiplicatively closed subset of a ring without divisors of zero is a system of type G^* , hence Theorem 2 holds for multiplicative matrix homomorphisms Φ into a ring without divisors of zero. If Ω is simple and ψ is an arbitrary multiplicative homomorphism of R into G^* , then $\Psi(B) = \Omega(B)\psi(\det B)$ is a multiplicative matrix homomorphism.

Let Ω be a simple multiplicative matrix homomorphism, let ω be the multiplicative homomorphism associated with Ω , and let $\sigma(c) = \Omega(A_{12}(c)) = \Omega(A_{21}(c))$. Clearly Ω is determined by ω and σ ; for $\Omega(E)$, see the proof of Lemma 2 part 7.

LEMMA 3. *Suppose Ω is simple and ω and σ are as above, then:*
 (1) $\omega(ab) = \omega(a)\omega(b)$. (2) $\sigma(a+b) = \sigma(a)\sigma(b)$. (3) $\omega(a) = 0$ or e . (4) If $\Omega \neq 0$ and $ab = 1 \in R$, then $\omega(a) = \omega(b) = e$. (5) $[\sigma(a)]^2 = e$ if $\Omega \neq 0$. (6) If $\omega(a) \neq 0$, $\sigma(ar) = \sigma(r)$. (7) If $\sigma(r) \equiv e$, $\Omega \equiv \omega(\det)$. (8) $\omega(1+1) = 0$ or $\Omega \equiv \omega(\det)$.

These facts are derived from the following identities. (1) $M_1(a)M_1(b) = M_1(ab)$. (2) $A_{12}(a+b) = A_{12}(a)A_{12}(b)$. (3) Ω is simple. (4) If $ab = 1$, $M_1(a)M_1(b) = I$ and $\Omega(I) = e \neq 0$ since $\Omega \neq 0$. (5) Follows from Lemma 2 part 4. (6) $M_1(a)A_{12}(ar) = A_{12}(r)M_1(a)$, then use (5) and the properties of G^* . (7) By Lemma 2 part 7 and by Lemma 3 part 4, $\omega(-1) = e$ and $\Omega(E_{ij}) = \Omega(M_i(-1))\Omega(A_{ij}(1)) = e = \omega(\det E_{ij})$. Also $\Omega(A_{ij}(r)) = e = \omega(\det A_{ij}(r))$ and $\Omega(M_i(c)) = \omega(c) = \omega(\det M_i(c))$. Hence $\Omega(B) = \omega(\det B)$ for every $B \in \mathfrak{M}_2^*$. (8) If $\omega(1+1) \neq 0$, $e = \sigma(r)\sigma(r) = \sigma((1+1)r) = \sigma(r)$ by (6). Then use (7).

THEOREM 3. *If R is commutative and $1/2 \in R$, then all multiplicative matrix homomorphisms Φ of $\mathfrak{M}_2^*$ onto G^* are of the form $\psi(\det)$ where ψ is a multiplicative homomorphism of R into G^* .*

For by Theorem 2, $\Phi(B) \equiv \Omega(B)\phi(\det B)$ where Ω is simple. Then by Lemma 3 part 4, $\Omega \equiv 0$ or $\omega(2) = e$, and by part 8, $\Omega \equiv 0$ or $\Omega \equiv \omega(\det)$. In either case Φ is of the form $\psi(\det)$.

Theorem 3 holds for multiplicative matrix homomorphisms Φ into a ring without divisors of zero; this is easily seen from a remark following the proof of theorem 2.

Let

$$\begin{aligned} P_1 &= \begin{pmatrix} 10 \\ 01 \end{pmatrix}, & P_2 &= \begin{pmatrix} 01 \\ 11 \end{pmatrix}, & P_3 &= \begin{pmatrix} 11 \\ 10 \end{pmatrix}, \\ N_1 &= \begin{pmatrix} 01 \\ 10 \end{pmatrix}, & N_2 &= \begin{pmatrix} 10 \\ 11 \end{pmatrix}, & N_3 &= \begin{pmatrix} 11 \\ 01 \end{pmatrix} \end{aligned}$$

be matrices with elements in $R = \mathfrak{I}_2$, the field of integers modulo two. Define $\Omega_0(P_i) = e \in G^*$, $\Omega_0(N_i) = q \in H \subset G^*$ ($q \neq 0$, $i = 1, 2, 3$) and $\Omega_0(B) = 0$ for other 2×2 matrices with elements in $\mathfrak{I}_2$. Computation of the multiplication table for the group of matrices P_i and N_i shows Ω_0 to be a multiplicative matrix homomorphism.

THEOREM 4. *If $\mathfrak{M}_2$ is the set of 2×2 matrices over a field R , all multiplicative matrix homomorphisms Φ of $\mathfrak{M}_2$ onto G^* , except the homomorphism Ω_0 above, are of the form $\psi(\det)$ where ψ is a multiplicative homomorphism of R into G^* . In particular, if R has more than two elements, Φ is of the form $\psi(\det)$.*

By Theorem 2, $\Phi = \Omega\phi(\det)$ where Ω is simple. If either Ω or Φ is identically 0 or identically e , the result is obvious. Suppose R is a field and neither Φ nor Ω is identically 0 or identically e . If $a \neq 0$, $\sigma(a) = \sigma(1)$ by Lemma 3 parts 4 and 6; hence if there is an $r \in R$ distinct from 0 and -1 , $\sigma(1) = \sigma(r+1) = \sigma(r)\sigma(1)$. But $\sigma(1) \neq 0$ by Lemma 3 part 5, hence $\sigma(r) = e$ by condition (iii) on G^* , and $\sigma(a) = \sigma(1) = \sigma(r) = e$. By Lemma 3 part 7, $\Omega = \omega(\det)$, and $\Phi = \omega(\det)\phi(\det)$. If $\psi(a) = \omega(a)\phi(a)$, $\Phi = \psi(\det)$; clearly ψ is a multiplicative homomorphism since $\omega(a) \in H$ and elements of H commute with every element of G^* .

If R has no element distinct from 0 and -1 , $R = \mathfrak{I}_2$. Then Lemma 2 shows that $\Phi(N_2) = \Phi(N_3)$ is in H and is not zero since $N_2 = A_{12}(1)$ and $N_3 = A_{21}(1)$. Also, since $-1 = +1$ and $N_1 = E_{12}$, $\Phi(N_1) = \Phi(N_2) = \Phi(N_3)$ using Lemma 2 part 7. It is also easy to see that $\Phi(P_i) = e$. By Theorem 2, $\Phi(B) = 0$ if $\det B = 0$; hence $\Phi(P_i) = e$, $\Phi(N_i) = q \in H$ ($q \neq 0$, $i = 1, 2, 3$) and $\Phi(B) = 0$ for other $B \in M_2$. Thus Φ is of the type Ω_0 . If $q \neq e$, Φ is not of the form $\psi(\det)$ since $\det P_i = \det N_j = 1$.

Let $\mathfrak{I}$ be the ring of integers and $\theta: \mathfrak{I} \rightarrow \mathfrak{I}_2$ be reduction modulo two

and let Θ be the induced homomorphism of integral 2×2 matrices onto 2×2 matrices with elements in $\mathfrak{F}_2$.

THEOREM 5. *All multiplicative matrix homomorphisms Φ of the set of 2×2 matrices with integral elements onto a system G^* are of the form $\Phi(B) = \psi(\det B)$ or $\Phi(B) = \Omega_0(\Theta(B))\psi(\det B)$ where Ω_0 is given in Theorem 4 and ψ is a multiplicative homomorphism of $\mathfrak{F}$ into G^* .*

Suppose Ω is a simple homomorphism of integral 2×2 matrices and is not of the form $\phi(\det)$. Then $\sigma(2n) = \sigma(n)\sigma(n) = e$ and $\sigma(2n+1) = \sigma(1) = q \in H$, $q \neq 0$. Using this q , define Ω_0 as in Theorem 4, then $\Omega(A_{ij}(m)) = \Omega_0(A_{ij}(\theta m)) = \Omega_0(\Theta A_{ij}(m))$. Also $\omega(2n) = \omega(2)\omega(n) = 0$ by Lemma 3 part 8, and $\Omega(M_i(c)) = \Omega_0(\Theta M_i(c))\omega(c)$ since $\Omega_0(\Theta M_i(c))$ vanishes only if $\Omega(M_i(c))$ vanishes and otherwise is e . Thus for matrices of type M and A (hence for arbitrary matrices), $\Omega(B) = \Omega_0(\Theta B)\omega(\det B)$. Then using Theorem 2, $\Phi \equiv \psi(\det)$ or Φ is of the form $\Omega_0(\Theta)\psi(\det)$ for some multiplicative homomorphism ψ of $\mathfrak{F}$ into G^* and Ω_0 of the type mentioned in Theorem 4.

If G^* is the set of integers under multiplication, $H = \{0, 1, -1\}$. The only homomorphisms of type Ω_0 are (taking $q=1$) $\Omega'_0(P_i) = \Omega'_0(N_i) = 1$, $\Omega'_0(B) = 0$ if $B \neq N_i, P_i$, and $\Omega''_0(P_i) = 1$, $\Omega''_0(N_i) = -1$, $\Omega''_0(B) = 0$ if $B \neq N_i, P_i$. Ω'_0 is of the form $\psi(\det)$.

COROLLARY. *Every multiplicative matrix homomorphism of integral 2×2 matrices into $\mathfrak{F}$ is of the form $\psi(\det)$ or $\Omega''_0(\Theta)\psi(\det)$ for some multiplicative homomorphism ψ of $\mathfrak{F}$ into $\mathfrak{F}$.*

REFERENCE

1. B. L. van der Waerden, *Moderne Algebra*, vols. I, II, 1931.

UNIVERSITY OF UTAH