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 $M_n$ 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 $M_n^*$ denote the set of matrices in $M_n$ which are products of elementary matrices.

For some rings $R$, $M_n^* = M_n$; if $R$ is such a ring and $\theta$ is a homomorphism of $R$ onto a ring $R'$, then $M_n^{*'} = M_n'$ where the prime refers to matrices with elements in $R'$. For $\theta$ induces in a natural way a homomorphism $\theta$ of $M_n$ onto $M_n'$ (merely let $\theta$ 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 $M_n$ 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, $M_n^* = M_n$. A skew field or field or any euclidean ring admits such an absolute value. If a ring $R$ has such an absolute value and $\beta$ 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 $\Phi$ of $M_n$ or $M_n^*$ into $G$ such that $\Phi(BC) = \Phi(B)\Phi(C)$ for every $B, C \in M_n$ or $M_n^*$ respectively, will be called a multiplica-

Received by the editors January 7, 1952.
tive matrix homomorphism. A mapping \( \phi \) 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 \( \Phi \) is a multiplicative matrix homomorphism of \( \mathbb{M}_n \) into \( G \), then \( \Phi \) confined to \( \mathbb{M}_n^* \) is a multiplicative matrix homomorphism of \( \mathbb{M}_n^* \) onto a multiplicatively closed subset of \( G \).

If \( \Phi \) is a multiplicative matrix homomorphism of \( \mathbb{M}_n \) or \( \mathbb{M}_n^* \) 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 \( \mathbb{M}_n^* \) of the zero and identity matrices \( 0 \) and \( I \).

**Lemma 2.** Suppose \( \Phi \) is a multiplicative matrix homomorphism of \( \mathbb{M}_n^* \) onto \( G \), then: (1) \( \Phi(E_{ij})^2 = e \). (2) \( \Phi(E_{ij}) = \Phi(E_{ji}) \). (3) \( \Phi(M_i(-1)) = e \). (4) \( \Phi(A_{ij}(c))^2 = e \). (5) \( \Phi(A_{ij}(c)) = \Phi(A_{ij}(-c)) \). (6) \( \Phi(A_{ij}(c)) = \Phi(A_{jk}(c)) \). (7) \( \Phi(E_{ij}) = \Phi(M_i(-1))\Phi(A_{ij}(1)) \). (8) If \( n > 2 \), then \( \Phi(A_{ij}(c)) = e \). (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 give these results: (1) \( E_{ij}E_{ij} = I \), hence \( \Phi(E_{ij})\Phi(E_{ij}) = \Phi(I) = e \). (2) \( E_{ij} = E_{ij}E_{ij}E_{ij} \) and \( E_{ij} = E_{ij} \) 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) \( A_{ij}(c) = E_{ij}A_{ij}(c)E_{ij} \) and \( A_{ij}(c) = E_{ij}A_{ij}(c)E_{ij} \). (7) \( E_{ij} = E_{ij} \) and (4) and (5). (8) \( A_{ij}(-c) = A_{jk}(-1)A_{ik}(-c)A_{jk}(1)A_{ik}(c) \) if \( i, j, k \) are distinct; then use (4) and (5). (9) \( M_i(c) = E_{ij}M_i(c)E_{ij} \) 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), \( \Phi(M_1(c)) = \Phi(E_{13})\Phi(M_3(c))\Phi(E_{13}) = \Phi(M_3(c)) \). Also \( \Phi(M_2(c)) = \Phi(E_{13})\Phi(M_1(c))\Phi(E_{13}) \); hence \( \Phi(M_1(c)) = \Phi(M_2(c)) \). (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 \( \Phi \) is a multiplicative matrix homomorphism of \( M_n^* \) 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 \( \phi(c) = \Phi(M_i(c)) \); \( \phi \) is clearly a multiplicative homomorphism of \( R \) into \( G \). \( \phi \) will be said to be associated with \( \Phi \). For \( B \in M_n \) 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 \( \Phi \) of \( M_n^* \) onto \( G \) is of the form \( \Phi(B) = \phi(\det B) \) where \( \phi \) is a multiplicative homomorphism of \( R \) into \( G \) uniquely determined by \( \Phi \).

Take \( \phi \) to be the multiplicative homomorphism associated with \( \Phi \). 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, \( \Phi(A_{ii}(c)) = e = \phi(1) = \phi(\det A_{ii}(c)) \) and by Lemma 2 part 7, \( \Phi(E_{ii}) = \Phi(M_i(-1)) = \phi(-1) = \phi(\det E_{ii}) \). Hence \( \Phi(B) = \phi(\det B) \) for any elementary matrix, consequently for any matrix in \( M_n^* \). If \( \Phi(B) = \psi(\det B) \) for every \( B \in M_n^* \), \( \psi = \phi(\psi(c) = \psi(\det M_i(c)) = \Phi(M_i(c)) = \phi(c) \).

**Corollary.** If \( F \) is a commutative multiplicative system or a ring without divisors of zero, and if \( R \) is a field and \( \Phi \) is a multiplicative matrix homomorphism of \( M_n^* \) into \( F \), then \( \Phi = \phi(\det) \) where \( \phi \) is a multiplicative homomorphism of \( R \) into \( F \); \( \Phi(B) = \Phi(O) \) if \( \det B = 0 \). If \( F = R \) and \( \Phi(M_i(c)) = c, \Phi = \det \).

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 \( \Omega \) of \( M_n^* \) into \( G^* \) will be called simple if \( \Omega \) maps \( M_n^* \) into \( H \), and the associated multiplicative homomorphism \( \omega \) maps \( R \) into the set \( \{0, e\} \subset G^* \).

**Theorem 2.** If \( R \) is commutative and \( \Phi \) is a multiplicative matrix homomorphism of \( M_n^* \) onto \( G^* \), then \( \Phi(B) = \Omega(B)\phi(\det B) \) where \( \phi \) is a multiplicative homomorphism of \( R \) into \( G^* \) and \( \Omega \) is simple and vanishes simultaneously with \( \phi(\det) \). Such \( \Omega \) and \( \phi \) are uniquely determined by \( \Phi \).
Let \( \phi \) be the multiplicative homomorphism associated with \( \Phi \).
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 \( B \in \mathbb{M}^*_R \), \( \Phi(B) = b\phi(\det B) \) 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 \( \Omega \) is multiplicative.
If \( \Phi \) 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 \( \Phi \) into a ring without divisors of zero. If \( \Omega \) is simple and \( \psi \) is an arbitrary multiplicative homomorphism of \( R \) into \( G^* \), then \( \Psi(B) = \Omega(B)\psi(\det B) \) is a multiplicative matrix homomorphism.
Let \( \Omega \) be a simple multiplicative matrix homomorphism, let \( \omega \) be the multiplicative homomorphism associated with \( \Omega \), and let \( \sigma(c) = \Omega(A_{12}(c)) = \Omega(A_{12}(c)) \). Clearly \( \Omega \) is determined by \( \omega \) and \( \sigma \); for \( \Omega(\mathcal{E}) \), see the proof of Lemma 2 part 7.

**Lemma 3. Suppose \( \Omega \) is simple and \( \omega \) and \( \sigma \) are as above, then:**
1. \( \omega(ab) = \omega(a)\omega(b) \).
2. \( \sigma(a+b) = \sigma(a)\sigma(b) \).
3. \( \omega(a) = 0 \) or \( \epsilon \).
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 \( \sigma(r) \equiv e \), \( \Omega = \omega(\det) \).
8. \( \omega(1+1) = 0 \) or \( \Omega = \omega(\det) \).

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. \( \Omega \) is simple.
4. If \( ab = 1 \), \( M_1(a)M_1(b) = I \) and \( \Omega(I) = \epsilon \neq 0 \) since \( \Omega \neq 0 \). (5) Follows from Lemma 2 part 4.
6. \( M_1(a)A_{12}(ar) = A_{12}(ar)M_1(a) \), then use (5) and the properties of \( G^* \).
7. (By Lemma 2 part 7 and by Lemma 3 part 4, \( \omega(-1) = e \) and \( \Omega(E_{ii}) = \Omega(M_i(-1)) = e = \omega(\det E_{ii}) \).
   Also \( \Omega(A_{ij}(r)) = e = \omega(\det A_{ij}(r)) \) and \( \Omega(M_{ij}(c)) = \omega(c) = \omega(\det M_{ij}(c)) \).

Hence \( \Omega(B) = \omega(\det B) \) for every \( B \in \mathbb{M}^*_R \).
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 \( \Phi \) of \( \mathbb{M}^*_R \) onto \( G^* \) are of the form \( \psi(\det) \) where \( \psi \) is a multiplicative homomorphism of \( R \) into \( G^* \).
For by Theorem 2, $\Phi(B) = \Omega(B) \phi(\det B)$ where $\Omega$ is simple. Then by Lemma 3 part 4, $\Omega = 0$ or $\omega(2) = e$, and by part 8, $\Omega = 0$ or $\Omega = \omega(\det)$. In either case $\Phi$ is of the form $\psi(\det)$.

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

Let

$$P_1 = \begin{pmatrix} 10 \\ 01 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 01 \\ 11 \end{pmatrix}, \quad P_3 = \begin{pmatrix} 11 \\ 10 \end{pmatrix},$$

$$N_1 = \begin{pmatrix} 01 \\ 10 \end{pmatrix}, \quad N_2 = \begin{pmatrix} 10 \\ 11 \end{pmatrix}, \quad N_3 = \begin{pmatrix} 11 \\ 01 \end{pmatrix}$$

be matrices with elements in $R = \mathbb{Z}_2$, 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 $2 \times 2$ matrices with elements in $\mathbb{Z}_2$. Computation of the multiplication table for the group of matrices $P_i$ and $N_i$ shows $\Omega_0$ to be a multiplicative matrix homomorphism.

**Theorem 4.** If $M_2$ is the set of $2 \times 2$ matrices over a field $R$, all multiplicative matrix homomorphisms $\Phi$ of $M_2$ onto $G^*$, except the homomorphism $\Omega_0$ above, are of the form $\psi(\det)$ where $\psi$ is a multiplicative homomorphism of $R$ into $G^*$. In particular, if $R$ has more than two elements, $\Phi$ is of the form $\psi(\det)$.

By Theorem 2, $\Phi = \Omega \phi(\det)$ where $\Omega$ is simple. If either $\Omega$ or $\Phi$ is identically 0 or identically $e$, the result is obvious. Suppose $R$ is a field and neither $\Phi$ nor $\Omega$ 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 $-1$, $\sigma(r) = \sigma(r+1) = \sigma(r)\sigma(1)$. 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 $\psi$ 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 $-1$, $R = \mathbb{Z}_2$. 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 $N_3 = A_{11}(1)$. 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 $\Phi$ is of the type $\Omega_0$. If $q \neq e$, $\Phi$ is not of the form $\psi(\det)$ since $\det P_i = \det N_j = 1$.

Let $\mathfrak{Z}$ be the ring of integers and $\theta: \mathfrak{Z} \to \mathbb{Z}_2$ be reduction modulo two.
and let $\Theta$ be the induced homomorphism of integral $2 \times 2$ matrices onto $2 \times 2$ matrices with elements in $\mathcal{I}$.

**Theorem 5.** All multiplicative matrix homomorphisms $\Phi$ of the set of $2 \times 2$ 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 $\Omega_0$ is given in Theorem 4 and $\psi$ is a multiplicative homomorphism of $\mathcal{I}$ into $G^*$.

Suppose $\Omega$ is a simple homomorphism of integral $2 \times 2$ matrices and is not of the form $\phi(\det)$. Then $\sigma(2n) = \sigma(n)\sigma(n) = h$ and $\sigma(2n + 1) = \sigma(1) = q \in H$, $q \neq 0$. Using this $q$, define $\Omega_0$ 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 $h$. 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, $\Phi = \psi(\det)$ or $\Phi$ is of the form $\Omega_0(\Theta)\psi(\det)$ for some multiplicative homomorphism $\psi$ of $\mathcal{I}$ into $G^*$ and $\Omega_0$ 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 $\Omega_0$ 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 $B \neq N_i$, $P_i$. $\Omega_0'$ is of the form $\psi(\det)$.

**Corollary.** Every multiplicative matrix homomorphism of integral $2 \times 2$ matrices into $\mathcal{I}$ is of the form $\psi(\det)$ or $\Omega_0'(\Theta)\psi(\det)$ for some multiplicative homomorphism $\psi$ of $\mathcal{I}$ into $\mathcal{I}$.

**Reference**


**University of Utah**