ON THE INDEPENDENCE OF THE FIRST AND SECOND MATRICES OF AN ALGEBRA*

BY C. C. MACDUFFEE

1. *Introduction.* It is well known† that every linear associative algebra with a principal unit (modulus) is isomorphic with the algebra of its first matrices, and also with the algebra of its transposed second matrices. If the algebra has no principal unit, it can be represented as a matric algebra of $(n+1)$th order matrices.

The condition that the algebra have a principal unit is not, however, necessary in order that the algebra be isomorphic with the algebra of its first or second matrices, as can readily be seen from examples. In this paper necessary and sufficient conditions for this isomorphism are obtained.

2. *The Correspondence of Poincaré.* Consider a linear associative algebra $\mathfrak{A}$ over a field $\mathfrak{F}$ with n basal numbers $e_1, e_2, \cdots, e_n$, the constants of multiplication being c_{ijk}. Let us denote by R_i the matrix‡ (c_{isr}), and by S_i the matrix (c_{ris}), where r determines the row and s the column in which an element stands.

The conditions for associativity in $\mathfrak{A}$ may be written§

$$(1) \qquad \sum_k c_{ikr}c_{jsk} = \sum_k c_{ijk}c_{ksr}, \quad (i,j,r,s = 1,2, \cdots, n).$$

If we form the matrices in which the respective members of the above equation stand in the rth row and sth column, we have

$$R_iR_j = \sum_k c_{ijk}R_k.$$

* Presented to the Society, Chicago, March 30, 1929.

† L. E. Dickson, *Algebras and their Arithmetics*, Chicago, 1923, p. 96.

‡ R_i and S_i are the first and transposed second matrices, respectively, of e_i. Dickson, loc. cit., p. 95.

§ Dickson, loc. cit., p. 92.

We may also write conditions (1) in the form

$$\sum_k c_{rik}c_{kjs} = \sum_k c_{ijk}c_{rks},$$

whence it follows that

$$S_iS_j = \sum_k c_{ijk}S_k.$$

Thus both R_i and S_i are isomorphic under multiplication with the basal numbers e_i.

Every number a of $\mathfrak{A}$ can be written

$$a = a_1e_1 + a_2e_2 + \cdots + a_ne_n,$$

where the a_i are in $\mathfrak{F}$. We define the *first matrix* $R(a)$ of a by the equation

$$R(a) = a_1R_1 + a_2R_2 + \cdots + a_nR_n,$$

and the *second matrix* $S(a)$ by

$$S(a) = a_1S_1 + a_2S_2 + \cdots + a_nS_n.$$

Thus the algebra $\mathfrak{A}$ is isomorphic with the algebra of matrices $R(a)$ if and only if $R_1, R_2, \cdots, R_n$ are linearly independent, and isomorphic with the algebra of matrices $S(a)$ if and only if $S_1, S_2, \cdots, S_n$ are linearly independent.

3. *Two Invariants.* If we apply to the basal numbers $e_1, e_2, \cdots, e_n$ the linear transformation

$$(2) \qquad e_i = \sum_j a_{ij}e_j', \qquad a = |a_{rs}| \neq 0,$$

with coefficients in $\mathfrak{F}$, the constants of multiplication are subject to the induced transformation*

$$(3) \qquad \sum_i c_{rsi}a_{ij} = \sum_{p,q} a_{rp}a_{sq}c_{pqj}', \qquad (r,s,j = 1,2,\cdots,n).$$

This may be written

$$ac_{isr} = \sum_{p,q,t} A_{rt}a_{ip}c_{pqt}'a_{sq},$$

* For example, see MacDuffee, Transactions of this Society, vol. 31 (1929), p. 81.

where A_{rt} denotes the cofactor of a_{rt} in $A=(a_{rs})$. Then

$$(4)\qquad R_i = \bar{A}^{-1}(\Sigma_p a_{ip} R_p')\bar{A}, \qquad (i=1,2,\cdots,n),$$

where $\bar{A}$ is the transpose of A.

If we denote by

$$(5)\qquad \sum_j k_{ij} R_j = 0, \qquad (i=1,2,\cdots,\rho),$$

a maximal set of linearly independent linear relations among the R_j, we have

$$\bar{A}^{-1}\sum_{h,j} k_{ij} a_{jh} R_h' \bar{A} = 0,$$

so that

$$\sum_h \left(\sum_j k_{ij} a_{jh}\right) R_h' = 0, \qquad (i=1,2,\cdots,\rho).$$

Since

$$\left(\sum_j k_{rj} a_{js}\right) = (k_{rs})A,$$

and the matrix (k_{rs}) of ρ rows and n columns is of rank ρ, we see that there are at least ρ linearly independent linear relations among the matrices $R_1', R_2', \cdots, R_n'$. Since (2) has an inverse, there are just ρ such relations. Hence ρ is invariant under transformation of coordinates.

Similarly we find that the number σ of linearly independent linear relations among the matrices $S_1, S_2, \cdots, S_n$ is likewise invariant.

4. *A Condition for the Independence of the Matrices.* Suppose that exactly ρ independent relations (5) hold among the matrices R_j. Form a matrix $B\equiv(b_{rs})$ so that $b_{ij}=k_{ij}$ for $i=n-\rho+1,\cdots,n$, and take for the remaining b_{ij} any convenient numbers of $\mathfrak{F}$ so that B is non-singular. Apply a transformation (2) using $A=B^{-1}$. From (4) we have

$$R_i' = \bar{B}^{-1}\sum_j b_{ij} R_j \bar{B}, \qquad (i=1,2,\cdots,n).$$

Hence $R'_{n-\rho+1}= \cdots =R'_n =0$ while $R'_1, R'_2, \cdots, R'_{n-\rho}$ are linearly independent. We drop primes.

We now have

$$(6) \qquad c_{ijk} = 0, \qquad (i > n - \rho\,;\; j,k = 1,2,\cdots,n).$$

The associativity conditions (1) may be written

$$\sum_{k=1}^{n} c_{ijk}c_{ksr} = \sum_{k=1}^{n} c_{ikr}c_{jsk}.$$

We consider only those equations in which $j>n-\rho$, and pass to matrices, obtaining

$$\sum_{k=1}^{n-\rho} c_{ijk}R_k = 0.$$

Since $R_1, R_2, \cdots, R_{n-\rho}$ are linearly independent,

$$(7) \quad c_{ijk} = 0, \quad (j > n - \rho\,;\; k \leqq n - \rho\,;\; i = 1,2,\cdots,n).$$

Consider the linear set $\mathfrak{Z}$ composed of all numbers

$$z = z_{n-\rho+1}e_{n-\rho+1} + \cdots + z_n e_n.$$

We see readily from (6) and (7) that

$$(8) \qquad \mathfrak{Z}\mathfrak{A} = 0, \qquad \mathfrak{A}\mathfrak{Z} \leqq \mathfrak{Z},$$

so that $\mathfrak{Z}$ is an invariant zero subalgebra of $\mathfrak{A}$ which has the additional property that $\mathfrak{Z}\mathfrak{A}=0$.

Conversely, let us suppose that $\mathfrak{A}$ has an invariant zero subalgebra $\mathfrak{Z}$ of order ρ such that $\mathfrak{Z}\mathfrak{A}=0$. We take the basis numbers of $\mathfrak{Z}$ for $e_{n-\rho+1}, \cdots, e_n$ of a basis for $\mathfrak{A}$. Since $\mathfrak{Z}\mathfrak{A}=0$, we have (7) and therefore $R_{n-\rho+1}= \cdots =R_n=0$.

Similar results hold for the second matrix.

THEOREM 1. *A necessary and sufficient condition in order that there be exactly $\rho(\sigma)$ linearly independent linear relations among the matrices $R_1, R_2, \cdots, R_n$ $(S_1, S_2, \cdots, S_n)$ is that $\mathfrak{A}$ have an invariant zero subalgebra $\mathfrak{Z}(\mathfrak{W})$ of order $\rho(\sigma)$ such that $\mathfrak{Z}\mathfrak{A}=0$, $(\mathfrak{A}\mathfrak{W}=0)$, and no such subalgebra of order greater than $\rho(\sigma)$.*

It is known that in every algebra with a principal unit (including every semi-simple algebra) both the first and second matrices are independent.*

It can be seen directly that if $\mathfrak{A}$ is nilpotent or the direct sum of a nilpotent algebra and another algebra, the first matrices and also the second matrices are dependent. For we may choose normalized† basis numbers e_i for the nilpotent algebra such that

$$e_ie_n = e_ne_i = 0, \qquad (i = 1,2, \cdots , n).$$

Hence e_n serves both as $\mathfrak{Z}$ and $\mathfrak{W}$ for Theorem 1.

That ρ is not necessarily equal to σ is shown by the following example:

$$e_1^2 = e_1, \quad e_1e_2 = 0, \quad e_2e_1 = e_2, \quad e_2^2 = 0.$$

We have

$$R_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad R_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad S_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad S_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Here R_1 and R_2 are linearly independent and give a representation of the algebra, while S_1 and S_2 are dependent. Thus $\rho = 0$, $\sigma = 1$, and $\mathfrak{W}$ is composed of multiples of e_2.

5. *The Characteristic Equations.* Let

$$x = x_1e_1 + x_2e_2 + \cdots + x_ne_n$$

be the general number of an algebra $\mathfrak{A}$, and define

$$\delta(\omega) = \left| R(x) - \omega I \right| , \quad \delta'(\omega) \equiv \left| S(x) - \omega I \right| .$$

It is well known‡ that $x\delta(x) = 0$ and $x\delta'(x) = 0$, and if $\mathfrak{A}$ has a principal unit, also $\delta(x) = 0$ and $\delta'(x) = 0$.

It is possible, however, for $\delta(x) = 0$ or $\delta'(x) = 0$ even though $\mathfrak{A}$ has no principal unit.

THEOREM 2. *A sufficient condition in order that* $\delta(x) = 0$ ($\delta'(x) = 0$) *is that* $R_1, R_2, \cdots , R_n$ ($S_1, S_2, \cdots , S_n$) *be linearly independent.*

* Dickson, loc. cit., p. 95.

† Dickson, loc. cit., p. 176.

‡ Dickson, loc. cit., p. 100.

The proof is immediate, for by the Hamilton-Cayley theorem

$$\delta(R(x)) = 0, \qquad \delta'(S(x)) = 0.$$

Since $\mathfrak{A}$ is isomorphic with the algebra of matrices $R(x)$ (or $S(x)$), we have $\delta(x)=0$ (or $\delta'(x)=0$).

For the example of §4 we have

$$\delta(\omega) = \omega^2 - \omega x_1, \qquad \delta'(\omega) = \omega^2 - 2\omega x_1 + x_1^2 .$$

Hence $\delta(x)=0$, while $\delta'(x)=x_1^2-x_1^2e_1-x_1x_2e_2$.

OHIO STATE UNIVERSITY

ON THE NUMBER $(10^{23}-1)/9$

D. H. LEHMER

The purpose of this note is to save any further effort* in trying to factor the number $N=(10^{23}-1)/9=111$, 11111, 11111, 11111, 11111 which in a previous paper was found to be composite.† This assertion was based on a negative result giving $3^{N-1}\not\equiv 1 \pmod{N}$.

On the basis of this conclusion Kraitchik‡ attempted to factor N arriving at another negative result that N had no factors and therefore was a prime. This conflict of results led us to recompute the value of $3^{N-1} (\text{mod } N)$ which shows clearly a mistake in the original calculation arising from the choice of 3 for a base instead of another number prime to $10^{23}-1$. Such another base would have furnished the extra check which would have detected the error.

* A recent letter from Mr. R. E. Powers informs us that he has been to the trouble of finding 150 quadratic residues of N.

† This Bulletin, vol. 33 (1927), p. 338.

‡ Mathesis, vol. 42 (1928), p. 386.