Matric criteria for the uniqueness of basis number and the equivalence of algebras over a ring.

Dedicated to the memory of Tibor Szele.

By ROSS A. BEAUMONT in Seattle, Washington.

1. Introduction.

C. J. EVERETT [1] has proved that a right free R-module over a ring R with identity has a unique basis number if the right ideals of R satisfy the ascending chain condition. By giving a symmetric form of one of EVERETT's theorems, we derive in Sec. 2, Theorem 2, a necessary and sufficient condition for the uniqueness of the basis number of a left (right) free R-module. By using results of BAER [2] and McCOY [3], we prove that any one of the following conditions on R is sufficient for the uniqueness of the basis number.

1. R satisfies the ascending chain condition either for right or for left ideals.

2. R is commutative.

Since R has an identity, the descending chain conditions imply the ascending chain conditions.

In Sec. 3, algebras over a non-commutative ring are discussed, and a necessary and sufficient condition (Theorem 5) is obtained for equivalence in terms of a matrix transformation of the multiplication tables of the algebras. In Sec. 4, matrix conditions for the classification of groupoids are given and a necessary and sufficient condition for isomorphism (Theorem 9) in the form of a matrix transformation of the multiplication tables is derived.

2. Units for rectangular matrices.

Let $R \neq 0$ be a ring with identity 1. We denote by ${}_mR_n$ the set of all $m \times n$ matrices and by R_n the set of all $n \times n$ matrices with elements in R.

DEFINITION. A matrix $A \in {}_mR_n$ is a *unit* if there exists a matrix $B \in {}_nR_m$ such that $AB = I_m$ and $BA = I_n$. We call B an *inverse* of A.

Let A be a unit in ${}_mR_n$ with inverse B. Then if either $AX=I_m$ or $XA=I_n$ for $X\in {}_nR_m$, it follows that $X=B$. In particular, a unit has a unique inverse.

DEFINITION. A ring R is *regular for* n if $C, D\in R_n$ and $CD=I_n$ implies $DC=I_n$.

Lemma 1. *If R is regular for m and n, $m\neq n$, then there are no units in ${}_mR_n$*

PROOF. Assume that $A\in {}_mR_n$ is a unit. Suppose first that $n<m$, and let $B\in {}_nR_m$ be the inverse of A. Then $A=\begin{pmatrix}A_1\\A_2\end{pmatrix}$ where $A_1\in R_n$ and $B=(B_1B_2)$ where $B_1\in R_n$. $AB=I_m$ gives $A_1B_1=I_n$, and since R is regular for n, we have $B_1A_1=I_n$. But $AB=I_m$ gives $A_1B_2=0$ and $A_2B_2=I_{m-n}$. Since $0=B_1A_1B_2=B_2$, this contradicts $A_2B_2=I_{m-n}$.

Similarly, if $m<n$, the equation $BA=I_n$ and the fact that R is regular for m leads to a contradiction.

By the lemma, there are no units in ${}_mR_n$ for every $m, n, m\neq n$ if R is regular for n for every $n>0$. It follows from BAER's result ([2], p. 635), that any ring which satisfies the ascending chain condition either for left ideals or for right ideals is regular for n for every $n>0$. (Since $1\in R$, the descending chain condition implies the ascending chain condition).

Lemma 2. *If R is commutative, then there are no units in ${}_mR_n$ for every $m, n, m\neq n$.*

PROOF. Assume that $A\in {}_mR_n$ is a unit, $m\neq n$, and suppose $n<m$. There exists $B\in {}_nR_m$ such that $AB=\begin{pmatrix}A_1\\A_2\end{pmatrix}(B_1B_2)=\begin{pmatrix}A_1B_1 & A_1B_2\\ A_2B_1 & A_2B_2\end{pmatrix}=I_m$, where $A_1, B_1\in R_n$. Since $A_1B_1=I_n$, A_1 has rank n, as defined by McCOY ([3], p. 159). For $|A_1|\,|B_1|=1$, and if there exists $a\neq 0$ in R such that $a|A_1|=0$, we would have $0=a|A_1|\,|B_1|=a$. Now suppose $B_2\neq 0$. Then there is a column $\begin{pmatrix}b_1\\b_2\\\vdots\\b_n\end{pmatrix}\neq\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}$ of B_2 such that $A_1\begin{pmatrix}b_1\\b_2\\\vdots\\b_n\end{pmatrix}=\begin{pmatrix}0\\0\\\vdots\\0\end{pmatrix}$, since $A_1B_2=0$. But by McCOY's theorem ([3], page 159), this implies that A_1 has rank less than n, which is a contradiction. Hence $B_2=0$. But this contradicts $A_2B_2=I_{m-n}$, so that the assumption of the existence of a unit leads to contradiction.

If $m<n$, the assumption of the existence of a unit in ${}_mR_n$ and the equation $BA=I_n$, gives a contradiction in the same way.

Lemma 2 may also be obtained as a corollary of Lemma 1 by noticing that a commutative ring is regular for n for every $n>0$.

Let $N(R)$ be a free left R-module with basis $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$. Throughout, we will consider left modules. There are, of course, corresponding statements of the results for right modules. A theorem of EVERETT ([1] p. 313) states that $\begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_m \end{pmatrix} = A \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{pmatrix}$, $m < n$, is a basis of $N(R)$ if and only if $A \in {}_mR_n$ satisfies

1. The $n \times n$ matrix $\begin{pmatrix} A \\ 0 \end{pmatrix}$ has a left inverse $B \in R_n$, that is $B \begin{pmatrix} A \\ 0 \end{pmatrix} = I_n$.

2. For $v \in {}_1R_m$, $vA = 0$ implies $v = 0$.

If $n \leqq m$, conditions 1. and 2. would be replaced by

1.' The $m \times m$ matrix $(A\ 0)$ has a right inverse $B \in R_m$, that is, $(A\ 0)B = I_m$.

2.' For $v \in {}_nR_1$, $Av = 0$ implies $v = 0$.

A symmetric statement of EVERETT's theorem can be given in terms of the concept of a unit in ${}_mR_n$.

Theorem 1. *Let $N(R)$ be a free R-module with basis $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$. Then $\eta_1, \eta_2, \ldots, \eta_m$ is a basis of $N(R)$ if and only if there exists a unit $A \in {}_mR_n$ such that* $\begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_m \end{pmatrix} = A \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{pmatrix}$.

PROOF. Elements $\eta_1, \eta_2, \ldots, \eta_m$ are in $N(R)$ if and only if there exists a matrix $A \in {}_mR_n$ such that $\begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_m \end{pmatrix} = A \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{pmatrix}$. If $\eta_1, \eta_2, \ldots, \eta_m$ is a basis of $N(R)$, there exists $B \in {}_nR_m$ such that $\begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{pmatrix} = B \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_m \end{pmatrix}$, and it is a consequence of the definition of a basis that $AB = I_m$ and $BA = I_n$. Conversely, if A is a unit, there exists $B \in {}_nR_m$ such that $B \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_m \end{pmatrix} = \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{pmatrix}$, so that $\eta_1, \eta_2, \ldots, \eta_m$ spans $N(R)$. Further, we have that

$$0 = \sum_{i=i}^{m} r_i \eta_i = (r_1, r_2, \ldots, r_m) \begin{pmatrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_m \end{pmatrix} = (r_1, r_2, \ldots, r_m) A \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{pmatrix}$$

implies $(r_1, r_2, \ldots, r_m) A = 0$. Since $AB = I_m$, $(r_1, r_2, \ldots, r_m) = 0$, so that $\eta_1, \eta_2, \ldots, \eta_m$ is a basis.

An explicit statement of the equivalence of the above result to EVERETT's theorem is given in the following lemma.

Lemma 3. *A matrix $A \in {}_mR_n$ is a unit if and only if A satisfies 1. and 2. above when $m < n$ (1'. and 2'. when $n \leqq m$).*

PROOF. The proofs are entirely similar for the two cases. We assume $m < n$. Let A be a unit in ${}_mR_n$ with inverse $B \in {}_nR_m$. Then $(B\ 0) \in R_n$ and $(B\ 0)\begin{pmatrix} A \\ 0 \end{pmatrix} = BA = I_n$, satisfying 1. If $vA = 0$ for $v \in {}_1R_m$, then $0 = vA = vAB = vI_m = v$, so that 2. is satisfied.

Conversely, let $A \in {}_mR_n$ satisfy 1. and 2. Then by 1., $I_n = B\begin{pmatrix} A \\ 0 \end{pmatrix} = (B_1 B_2)\begin{pmatrix} A \\ 0 \end{pmatrix} = B_1 A$, where $B_1 \in {}_nR_m$. Further, we have $(AB_1 - I_m) A = 0$, and by 2. this implies $AB_1 - I_m = 0$. Hence A is a unit with inverse $B_1 \in {}_nR_m$.

Using the fact that for every ring R with identity, there exists a free R-module with n basis elements for every $n > 0$, the following result is an immediate consequence of Theorem 1.

Theorem 2. *Every free R-module with a finite basis has a unique basis number if and only if there are no units in ${}_mR_n$ for every $m, n, m \neq n$.*

It is a consequence of Lemma's 1 and 2 that the only rings R for which there exists a free R-module which has a basis of m elements and n elements $m \neq n$ are non-commutative rings which satisfy neither chain condition for left ideals or for right ideals. EVERETT ([1], p. 313) has given an example of such a module over a ring of infinite matrices.

3. Algebras over R.

As in Sec. 2., let $R \neq 0$ be a ring with identity, and let $N(R)$ be a free left R-module with basis $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$. If R is commutative, then $N(R)$ is an algebra over R if and only if there exist elements $\gamma_{jk}^{(i)} \in R$ such that multiplication (denoted by x) in $N(R)$ is defined by

$$(*) \qquad \alpha \times \beta = \left(\sum_{i=1}^{n} r_i \varepsilon_i \right) \times \left(\sum_{j=1}^{n} s_j \varepsilon_j \right) = \sum_{k=1}^{n} \left(\sum_{i,j=1}^{n} r_i s_j \gamma_{jk}^{(i)} \right) \varepsilon_k .$$

If R is not commutative the multiplication rule $(*)$ does not imply the identity $\alpha \times r\beta = r(\alpha \times \beta)$ for α, $\beta \in N(R)$, $r \in R$. However the weaker identity $\varepsilon_i \times r\varepsilon_j = r(\varepsilon_i \times \varepsilon_j)$ holds. This suggests the following definition.

DEFINITION. $N(R)$ is a (left) algebra of order n over R if

i) $N(R)$ is a (left) free R-module with a finite basis $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$.

ii) $N(R)$ is a ring (not necessarily associative) with respect to module addition, $+$, and a multiplication, x.

iii) $(r\alpha)\mathrm{x}\beta = r(\alpha\mathrm{x}\beta)$ for $r \in R, \alpha, \beta \in N(R)$.

iv) $\varepsilon_i\mathrm{x}(r\varepsilon_j) = r(\varepsilon_i\mathrm{x}\varepsilon_j)$ for $r \in R, i, j, = 1, 2, \ldots, n$.

As in the commutative case, a routine calculation yields the following theorem.

Theorem 3. *A free R-module $N(R)$ with basis $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ is an algebra over R if and only if there exist elements $\gamma_{jk}^{(i)} \in R$ such that multiplication is defined by* $(*)$.

Let E be the ring of endomorphisms of $N(R)$ as an additive abelian group and let $\mathfrak{L}$ be the subring of linear transformations of the R-module $N(R)$. E is an R-module which satisfies $(r\varphi)\psi = r(\varphi\psi)$ for $r \in R$, $\varphi, \psi \in E$. If $N(R)$ is an algebra over R, then E contains:

i) the scalar multiplications defined by $S_r(\alpha) = r\alpha$, $r \in R, \alpha \in N(R)$.

ii) the right component multiplications defined by $R_t(\alpha) = R_t\left(\sum_{i=1}^{n} r_i\varepsilon_i\right) = \sum_{i=1}^{n} r_i t\varepsilon_i$, $t \in R$, $\alpha \in N(R)$.

iii) the right multiplications defined by $\beta_R(\alpha) = \alpha\mathrm{x}\beta$, $\alpha, \beta \in N(R)$.

iv) the left multiplications defined by $\beta_L(\alpha) = \beta\mathrm{x}\alpha$, $\alpha, \beta \in N(R)$.

With the above definitions, iii) in the definition of an algebra becomes $\beta_R S_r = S_r\beta_R$ for $r \in R, \beta \in N(R)$. Hence $\beta_R \in \mathfrak{L}$ for all $\beta \in N(R)$. Similarly iv) becomes $\varepsilon_{iL}S_r = S_r\varepsilon_{iL}$, and $\varepsilon_{iL} \in \mathfrak{L}$ for $i = 1, 2, \ldots, n$. It is also evident that $R_t \in \mathfrak{L}$ for all $t \in R$.

Theorem 3 can now be restated in the following way.

Theorem 4. *A free R-module $N(R)$ with basis $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ is an algebra over R if and only if there exists an R-homomorphism Φ: $N(R) \to E$ with the property that $\Phi[\varepsilon_i] \in \mathfrak{L}$ for $i = 1, 2, \ldots, n$, such that multiplication is defined by $\beta\mathrm{x}\alpha = \Phi[\beta](\alpha)$.*

Proof. If $N(R)$ is an algebra, let Φ be defined by $\Phi[\beta] = \beta_L$. It follows from the right distributive law and iii) in the definition of an algebra that Φ is an R-homomorphism. It has already been noted that iv) implies $\Phi[\varepsilon_i] = \varepsilon_{iL} \in \mathfrak{L}$. By the definition of Φ, $\beta\mathrm{x}\alpha = \Phi[\beta](\alpha)$.

Conversely, if an R-homomorphism Φ is given satisfying the stated conditions, multiplication is defined by $\beta\mathrm{x}\alpha = \Phi[\beta](\alpha)$. Since $\Phi[\beta] \in E$ and since Φ is a homomorphism, both distributive laws are satisfied. Since Φ is an R-homomorphism, $(r\beta)\mathrm{x}\alpha = \Phi[r\beta](\alpha) = \{r\Phi[\beta]\}(\alpha) = r\{\Phi[\beta](\alpha)\} = r(\beta\mathrm{x}\alpha)$. Since $\Phi[\varepsilon_i] \in \mathfrak{L}$,

$$\varepsilon_i\mathrm{x}r\varepsilon_j = \Phi[\varepsilon_i](r\varepsilon_j) = r\{\Phi[\varepsilon_i](\varepsilon_j)\} = r(\varepsilon_i\mathrm{x}\varepsilon_j).$$

This completes the proof.

If R is commutative, then $\varepsilon_i\mathrm{x}r\varepsilon_j = r(\varepsilon_i\mathrm{x}\varepsilon_j)$ is equivalent to $\alpha\mathrm{x}r\beta = r(\alpha\mathrm{x}\beta)$ for all $\alpha, \beta \in N(R)$, in the presence of the other postulates for an algebra.

In this case, $R_t = S_t$, and S_t, β_R, and β_L are in $\mathfrak{L}$.

Since an R-homomorphism Φ of a free R-module is completely determined by the images of the basis elements, the algebra $N(R)$ is completely determined by the choice of the $\Phi[\varepsilon_i] \in \mathfrak{L}$. Moreover an arbitrary choice of the $\Phi[\varepsilon_i] \in \mathfrak{L}$ defines an R-homomorphism Φ. Let $\Gamma_i = (\gamma_{jk}^{(i)}), i = 1, 2, \ldots, n$ be the matrix of the linear transformation $\Phi[\varepsilon_i]$. Then $\varepsilon_i \times \varepsilon_j = \sum_{k=1}^{n} \gamma_{jk}^{(i)} \varepsilon_k$, and the $n^2 \times n$ matrix $\Gamma = \begin{pmatrix} \Gamma_1 \\ \Gamma_2 \\ \vdots \\ \Gamma_n \end{pmatrix}$ is the multiplication table of the algebra, which we will denote by $[N(R), \varepsilon_i, \Gamma]$.

Let $M(R)$ be a free R-module with basis $\eta_1, \eta_2, \ldots, \eta_m$, and let $[M(R), \eta_i, \Delta]$ be an algebra, where $\Delta_i = (\delta_{jk}^{(i)}), i = 1, 2, \ldots, m$.

Theorem 5. *The algebra $[M(R), \eta_i, \Delta]$ is isomorphic to the algebra $[N(R), \varepsilon_i, \Gamma]$ if and only if there exists a unit $A \in {}_mR_n$ such that $\Delta = (A \otimes A)\Gamma B$, where $B \in {}_nR_m$ is the inverse of A and $\otimes$ denotes the left Kronecker product of matrices.*

PROOF. Suppose first that $[M(R), \eta_i, \Delta]$ and $[N(R), \varepsilon_i, \Gamma]$ are isomorphic. Then under the given R-isomorphism the basis $\eta_1, \eta_2, \ldots, \eta_m$ of $M(R)$ corresponds to a basis $\eta_1^1, \eta_2^1, \ldots, \eta_m^1$ of $N(R)$. By Theorem 1, there exists a unit $A = (a_{ij}) \in {}_mR_n$ such that $\begin{pmatrix} \eta_1^1 \\ \eta_2^1 \\ \vdots \\ \eta_m^1 \end{pmatrix} = A \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{pmatrix}$. We have:

$$(\eta_i \times \eta_j)^1 = \left(\sum_{k=1}^{m} \delta_{jk}^{(i)} \eta_k\right)^1 = \sum_{k=1}^{m} \delta_{jk}^{(i)} \eta_k^1 = \sum_{k=1}^{m} \delta_{jk}^{(i)} \left(\sum_{l=1}^{n} a_{kl} \varepsilon_l\right) = \sum_{l=1}^{n} \left(\sum_{k=1}^{m} \delta_{jk}^{(i)} a_{kl}\right) \varepsilon_l .$$

$$\eta_i^1 \times \eta_j^1 = \left(\sum_{t=1}^{n} a_{it} \varepsilon_t\right) \times \left(\sum_{s=1}^{n} a_{js} \varepsilon_s\right) = \sum_{l=1}^{n} \left(\sum_{s,t=1}^{n} a_{it} a_{js} \gamma_{sl}^{(t)}\right) \varepsilon_l .$$

Therefore, since $(\eta_i \times \eta_j)^1 = \eta_i^1 \times \eta_j^1$, we have

$$\sum_{k=1}^{m} \delta_{jk}^{(i)} a_{kl} = \sum_{s,t=1}^{n} a_{it} a_{js} \gamma_{sl}^{(t)} = \sum_{t=1}^{n} a_{it} \left(\sum_{s=1}^{n} a_{js} \gamma_{sl}^{(t)}\right)$$

for $i = 1, 2, \ldots, n, j = 1, 2, \ldots, n$, and $l = 1, 2, \ldots, n$. For i fixed, this gives

$$\Delta_i A = \sum_{t=1}^{n} a_{it} A \Gamma_t = (a_{i1} A, a_{i2} A, \ldots, a_{in} A) \begin{pmatrix} \Gamma_1 \\ \Gamma_2 \\ \vdots \\ \Gamma_n \end{pmatrix} .$$

Therefore $\begin{pmatrix} \Delta_1 \\ \Delta_2 \\ \vdots \\ \Delta_m \end{pmatrix} A = (A \otimes A) \begin{pmatrix} \Gamma_1 \\ \Gamma_2 \\ \vdots \\ \Gamma_n \end{pmatrix}$, or $\Delta = (A \otimes A) \begin{pmatrix} \Gamma_1 \\ \Gamma_2 \\ \vdots \\ \Gamma_n \end{pmatrix} B$, where $B \in {}_nR_m$ is the inverse of A.

Conversely, let A be a unit in ${}_mR_n$ and suppose $\Delta = (A \otimes A)\Gamma B$. Then by Theorem 1, $\eta_1^1, \eta_2^1, \dots, \eta_m^1$ defined by $\begin{pmatrix} \eta_1^1 \\ \eta_2^1 \\ \vdots \\ \eta_m^1 \end{pmatrix} = A \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \\ \vdots \\ \varepsilon_n \end{pmatrix}$ is a basis of $N(R)$.

Then the mapping λ defined by $\lambda\left(\sum_{i=1}^{m} r_i \eta_i\right) = \sum_{i=1}^{m} r_i \eta_i^1$ is a $(+, \mathrm{x})$ R-isomorphism of $M(R)$ onto $N(R)$. It is clear that λ is an R-isomorphism of the module $M(R)$ onto the module $N(R)$, and the equation $\Delta = (A \otimes A)\Gamma B$ is just the condition that $\lambda(\eta_i \mathrm{x} \eta_j) = \lambda(\eta_i) \mathrm{x} \lambda(\eta_j)$.

Theorem 6. *The algebra $[N(R), \varepsilon_i; \Gamma]$ is associative if and only if $\varepsilon_{jR} R_t \varepsilon_{iL} = \varepsilon_{iL} \varepsilon_{jR} R_t$ for $i, j = 1, 2, \dots, n$ and for every $t \in R$.*

PROOF. If $[N(R), \varepsilon_i, \Gamma]$ is associative, then

$$(\varepsilon_i \mathrm{x} \alpha) \mathrm{x} (t\varepsilon_j) = \varepsilon_i \mathrm{x} (\alpha \mathrm{x} t\varepsilon_j)$$

for $i, j = 1, 2, \dots, n, t \in R$, and $\alpha \in N(R)$.

Using the trivial identity $(t\varepsilon_j)_R = \varepsilon_{jR} R_t$, we have

$$(\varepsilon_i \mathrm{x} \alpha) \mathrm{x} (t\varepsilon_j) = (t\varepsilon_j)_R \varepsilon_{iL}(\alpha) = \varepsilon_{jR} R_t \varepsilon_{jL}(\alpha),$$
$$\varepsilon_i \mathrm{x} (\alpha \mathrm{x} t\varepsilon_j) = \varepsilon_{iL} (t\varepsilon_j)_R(\alpha) = \varepsilon_{iL} \varepsilon_{jR} R_t(\alpha).$$

Conversely if the identity $\varepsilon_{jR} R_t \varepsilon_{iL} = \varepsilon_{iL} \varepsilon_{jR} R_t$ holds in $\mathfrak{L}$, we have with $\beta = \sum_{i=1}^{n} r_i \varepsilon_i$ and $\gamma = \sum_{j=1}^{n} t_j \varepsilon_j$

$$(\beta \mathrm{x} \alpha) \mathrm{x} \gamma = \left(\sum_{i=1}^{n} r_i \varepsilon_i \mathrm{x} \alpha\right) \mathrm{x} \sum_{j=1}^{n} t_j \varepsilon_j - \left[\sum_{i=1}^{n} r_i (\varepsilon_i \mathrm{x} \alpha)\right] \mathrm{x} \sum_{j=1}^{n} t_j \varepsilon_j =$$
$$= \sum_{j=1}^{n} \left\{ \left[\sum_{i=1}^{n} r_i (\varepsilon_i \mathrm{x} \alpha)\right] \mathrm{x} (t_j \varepsilon_j) \right\} = \sum_{j=1}^{n} \left\{ \sum_{i=1}^{n} r_i [(\varepsilon_i \mathrm{x} \alpha) \mathrm{x} (t_j \varepsilon_j)] \right\} =$$
$$= \sum_{j=1}^{n} \left\{ \sum_{i=1}^{n} r_i [\varepsilon_{jR} R_{t_j} \varepsilon_{iL}(\alpha)] \right\} = \sum_{i=1}^{n} \left\{ \sum_{j=1}^{n} r_i [\varepsilon_{iL} \varepsilon_{jR} R_{t_j}(\alpha)] \right\} =$$
$$= \sum_{i=1}^{n} \left\{ \sum_{j=1}^{n} r_i [\varepsilon_i \mathrm{x} (\alpha \mathrm{x} t_j \varepsilon_j)] \right\} = \sum_{i=1}^{n} \left\{ \sum_{j=1}^{n} [(r_i \varepsilon_i) \mathrm{x} (\alpha \mathrm{x} t_j \varepsilon_j)] \right\} =$$
$$= \sum_{i=1}^{n} \left\{ (r_i \varepsilon_i) \mathrm{x} \left[\sum_{j=1}^{n} \alpha \mathrm{x} (t_j \varepsilon_j)\right] \right\} = \left(\sum_{i=1}^{n} r_i \varepsilon_i\right) \mathrm{x} \left[\sum_{j=1}^{n} \alpha \mathrm{x} (t_j \varepsilon_j)\right] =$$
$$= \left(\sum_{i=1}^{n} r_i \varepsilon_i\right) \mathrm{x} \left(\alpha \mathrm{x} \sum_{j=1}^{n} t_j \varepsilon_j\right) = \beta \mathrm{x} (\alpha \mathrm{x} \gamma).$$

The matrix of the linear transformation ε_{iL} is $\Gamma_i=(\gamma_{jk}^{(i)})$. The matrix of the linear transformation ε_{jR} is the submatrix of Γ whose l-th row is the j-th row of Γ_l, that is the matrix $\Lambda_j=(\lambda_{lk}^{(j)})$, where $\lambda_{lk}^{(j)}=\gamma_{jk}^{(l)}$. The condition for associativity given in Theorem 6 can be written as the matrix identity.

1. $\Gamma_i(tI_n)\Lambda_j=(tI_n)\Lambda_j\Gamma_i$, $i,j=1,2,\dots,n$ and every $t\in R$.

If R is commutative, 1. is equivalent to

2. $\Gamma_i\Lambda_j=\Lambda_j\Gamma_i$ for $i,j=1,2,\dots,n$

which is the usual associativity condition for the multiplication constants in matrix form. More generally, 1. and 2. are equivalent whenever the ε_{iL} commute with the right component multiplications R_t. In this connection the following statement is of some interest.

Theorem 7. *Let $[N(R),\varepsilon_i,\Gamma]$ be an associative algebra such that for some j, ε_{jR} is a non-singular linear transformation. Then each ε_{iL} commutes with every R_t.*

Proof. Since $[N(R),\varepsilon_i,\Gamma]$ is associative, 1. and 2. are both satisfied. Now 2. implies

$$(tI_n)\Gamma_i\Lambda_j=(tI_n)\Lambda_j\Gamma_i \text{ for } i,j=1,2,\dots,n, \text{ and every } t\in R.$$

This identity combined with 1. gives

$$\Gamma_i(tI_n)\Lambda_j=(tI_n)\Gamma_i\Lambda_j.$$

By hypothesis, for some j, the matrix Λ_j has an inverse. Hence $\Gamma_i(tI_n)=(tI_n)\Gamma_i$ for $i=1,2,\dots,n$ and every $t\in R$. This is the matrix form of the statement of the theorem.

Let B be the set of basis elements $\{\varepsilon_1,\varepsilon_2,\dots,\varepsilon_n\}$ of the algebra $[N(R),\varepsilon_i,\Gamma]$. Then B is a groupoid if $\varepsilon_{iL}(B)\subset B$ for $i=1,2,\dots,n$. An algebra over R is a groupoid algebra if it possesses a basis B which is a groupoid. When $[N(R),\varepsilon_i,\Gamma]$ is said to be a groupoid algebra, we will mean that the basis $\{\varepsilon_1,\varepsilon_2,\dots,\varepsilon_n\}$ is a groupoid.

Theorem 8. *If $[N(R),\varepsilon_i,\Gamma]$ is a groupoid algebra, then conditions 1. and 2. are equivalent.*

Proof. Since $\{\varepsilon_1,\varepsilon_2,\dots,\varepsilon_n\}$ is a groupoid, the matrix Γ_i of the linear transformation ε_{iL} has $1\in R$ in exactly one position in each row and zeros elsewhere. Hence the matrices Γ_i commute with the scalar matrices tI_n, and therefore 2. implies 1. On the other hand 1. always implies 2.

4. Groupoids.

If $N=\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n\}$ is a groupoid, then a multiplication table for N can be given by an $n^2\times n$ incidence matrix $=\begin{pmatrix}\Gamma_1\\ \Gamma_2\\ \vdots\\ \Gamma_n\end{pmatrix}$ where $\Gamma_i=(\gamma_{jk}^{(i)})$ is an $n\times n$ matrix, $i=1,2,\ldots,n$ and $\gamma_{jk}^{(i)}=\begin{cases}1\in R & \text{if } \varepsilon_i\varepsilon_j=\varepsilon_k\\ 0\in R & \text{otherwise.}\end{cases}$

Γ_i has $1\in R$ in exactly one position in each row and zeros elsewhere. We will denote a groupoid, defined for the ordered set of elements $\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n\}$ by $[\varepsilon_i, \Gamma]$. It is convenient to classify groupoids $N=[\varepsilon_i, \Gamma]$ according to the properties of the matrix Γ. Some of the properties are trivial consequences of the definitions previously given for the submatrices Γ_i and Λ_j of Γ.

I. N is a semigroup if and only if $\Gamma_i\Lambda_j=\Lambda_j\Gamma_i$, $i,j=1,2,\ldots,n$.

II. N is commutative if and only if $\Gamma_j=\Lambda_j$, $j=1,2,\ldots,n$.

III. N is a right quasi-group if and only if each Γ_i, $i=1,2,\ldots,n$ is a permutation matrix.

PROOF. If N is a right quasi-group, then for every i and k, there exists a j such that $\varepsilon_i x=\varepsilon_k$ has a solution $x=\varepsilon_j$. Hence for every k, the matrix Γ_i must have $\gamma_{jk}^{(i)}=1$ for some j. Since there is exactly one 1 in each row of Γ_i, Γ_i is a permutation matrix. Conversely, if each Γ_i is a permutation matrix, the equation $\varepsilon_i x=\varepsilon_k$ has a solution for every i and k.

By an argument similar to the above we have

IV. N is a left quasi-group if and only if each Λ_j, $j=1,2,\ldots,n$ is a permutation matrix.

V. N is a loop if and only if Γ satisfies the following conditions:

i) Γ_i is a permutation matrix, $i=1,2,\ldots,n$.

ii) $\sum_{i=1}^{n}\Gamma_i=\mathfrak{J}_n$ where $\mathfrak{J}_n$ is a matrix with 1 in every position.

iii) For some j, $\Gamma_j=\Lambda_j=I_n$.

PROOF. If N is a loop, then by III, i) is satisfied. By IV, each Λ_j is a permutation matrix, so that the sum of the j-th rows of the matrices Γ_i is the row vector $(1,1,\ldots,1.)$ Hence $\sum_{i=1}^{n}\Gamma_i=\mathfrak{J}_n$. Since N has an identity ε_j, $\Gamma_j=I_n$ and $\Lambda_j=I_n$. Conversely, suppose that i), ii), and iii) are satisfied. Then N is a right quasi-group by III. Together, i) and ii) imply that each Λ_j is a permutation matrix, so that N is a left quasi-group by IV. Finally, iii) implies that ε_j is an identity element of N.

Since an associative quasi-group is a group, we combine the above results to obtain

VI. N is a group if and only if Γ satisfies the conditions:

i) Each Γ_i is a permutation matrix, $i=1,2,\ldots,n$.

ii) $\sum_{i=1}^{n} \Gamma_i = \mathfrak{J}_n$.

iii) $\Gamma_i \Delta_j = \Delta_j \Gamma_i$, $i=1,2,\ldots,n$, $j=1,2,\ldots,n$.

Theorem 9. *The groupoid $N=[\varepsilon_i, \Gamma]$ is isomorphic to the groupoid $M=[\eta_i, \Delta]$ if and only if there exists a permutation matrix I_Ω such that $(I_\Omega \otimes I_\Omega)\Gamma I'_\Omega = \Delta$.*

Proof. The groupoids N and M are isomorphic if and only if for a suitable ordering of the elements $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ of N, the incidence matrices of N and M are identical, that is, if and only if there exists a permutation Ω of $(1,2,\ldots,n)$ such that $N=\{\varepsilon_{\Omega(1)}, \varepsilon_{\Omega(2)}\ldots, \varepsilon_{\Omega(n)}\}$ and $M=\{\eta_1, \eta_2, \ldots, \eta_n\}$ have identical incidence matrices. Let I_Ω be the permutation matrix associated with Ω. Then the theorem follows when we observe that $(I_\Omega \otimes I_\Omega)\Gamma I'_\Omega$ is the incidence matrix of $N=\{\varepsilon_{\Omega(1)}, \varepsilon_{\Omega(2)}, \ldots, \varepsilon_{\Omega(n)}\}$. Since $\Omega=(ij)(kl)\ldots(st)$, $I_\Omega = I_{(ij)} I_{(kl)} \ldots I_{(st)}$, and $I_\Omega \otimes I_\Omega = (I_{(ij)} \otimes I_{(ij)})(I_{(kl)} \oplus I_{(kl)}) \ldots (I_{(st)} \otimes I_{(st)})$, it suffices to prove this latter result for the case where $\Omega=(ij)$ is a transposition. But if ε_i and ε_j are interchanged, then the submatrices Γ_i and Γ_j are interchanged in Γ after which the i-th and j-th rows and the i-th and j-th columns are interchanged in each Γ_l, $l=1,2,\ldots,n$. This operation is accomplished by the matrix product

$$(I_{(ij)} \otimes I_{(ij)})\Gamma I'_{(ij)} = \begin{array}{cc} & \begin{array}{ccccccccc} & & & i & & j & & & \end{array} \\ \begin{array}{c} \\ \\ \\ i \\ \\ j \\ \\ \\ \\ \end{array} & \begin{pmatrix} I_{(ij)} & & & & & & & & \\ & \ddots & & & & & & & \\ & & I_{(ij)} & & & & & & \\ & & & 0 & \cdots & I_{(ij)} & & & \\ & & & \vdots & & \vdots & & & \\ & & & I_{(ij)} & \cdots & 0 & & & \\ & & & & & & I_{(ij)} & & \\ & & & & & & & \ddots & \\ & & & & & & & & I_{(ij)} \end{pmatrix} \end{array} \begin{pmatrix} \Gamma_1 \\ \vdots \\ \Gamma_i \\ \vdots \\ \Gamma_j \\ \vdots \\ \Gamma_n \end{pmatrix} I'_{(ij)} = \begin{pmatrix} I_{(ij)}\Gamma_1 I'_{(ij)} \\ \vdots \\ I_{(ij)}\Gamma_j I'_{(ij)} \\ \vdots \\ I_{(ij)}\Gamma_i I'_{(ij)} \\ \vdots \\ I_{(ij)}\Gamma_n I'_{(ij)} \end{pmatrix}.$$

It should be recalled that for permutation matrices, $I' = I^{-1}$.

Example. Using the results of III, IV, and V, a quasi-group (both a right and left quasi-group) must have either an incidence matrix $\Gamma = \begin{pmatrix} \Gamma_1 \\ \Gamma_2 \\ \Gamma_3 \end{pmatrix}$

where $\Gamma_1, \Gamma_2, \Gamma_3$ are the matrices $\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix}, \begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix}$ in some order, or an incidence matrix $\bar{\Gamma} = \begin{pmatrix}\bar{\Gamma}_1\\\bar{\Gamma}_2\\\bar{\Gamma}_3\end{pmatrix}$ where $\bar{\Gamma}_1, \bar{\Gamma}_2, \bar{\Gamma}_3$ are the matrices $\begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix}$, $\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}, \begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix}$ in some order. Using Theorem 9 it is easy to check that there are exactly five non-isomorphic quasi-groups among the possible twelve. They are given by:

$$\Gamma = \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\\0&1&0\\0&0&1\\1&0&0\\0&0&1\\1&0&0\\0&1&0\end{pmatrix}, \text{ the group of order 3.}$$

$$\Gamma = \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\\1&0&0\\0&1&0\\0&0&1\\0&0&1\\1&0&0\\0&1&0\end{pmatrix}, \text{ a quasi-group with left identity.}$$

$$\Gamma = \begin{pmatrix}1&0&0\\0&0&1\\0&1&0\\0&1&0\\1&0&0\\0&0&1\\0&0&1\\0&1&0\\1&0&0\end{pmatrix}, \text{ a quasi-group with right identity.}$$

$$\Gamma = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \text{ a quasi-group without identity.}$$

$$\Gamma = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \text{ a quasi-group without identity.}$$

The second and third quasi-groups exhibited above are anti-isomorphic.

Bibliography.

[1] C. J. Everett, Vector spaces over rings, *Bull. Amer. Math. Soc.* **48** (1942), 312—316.
[2] R. Baer, Inverses and zero divisors, *Bull. Amer. Math. Soc.* **48** (1942), 630—638.
[3] N. H. McCoy, *Rings and ideals*, Baltimore, 1948.

(Received November 19, 1955.)