IDEAL MULTIPLICATION IN A LINEAR ALGEBRA*

BY GRACE SHOVER AND C. C. MACDUFFEE

1. *Introduction.* A recent approach† to the theory of ideals through matrices with rational integral elements proved to be successful for domains of integrity of linear associative algebras over the rational field as well as for domains of algebraic fields. The great weakness of this method was the lack of an adequate treatment of ideal multiplication.

In the present paper it is shown that ideal multiplication can be treated in a satisfactory manner by means of the matric theory. The way now seems to open for considerable development of the theory of ideals in rational algebras.

It is particularly to be noted that the classical theory of ideals in an algebraic field is a special case of the present theory. By way of illustration it is shown that the method of this paper can be applied to find by a straightforward, rational process the canonical form of the product of two ideals.

2. *Definitions and References.* Let $\mathfrak{A}$ be a rational semi-simple algebra of order n, and $\mathfrak{S}$ a set of integral elements of order n in $\mathfrak{A}$.‡ We suppose that the basal numbers $e_1, e_2, \cdots, e_n$ of $\mathfrak{A}$ form a basis for $\mathfrak{S}$, e_1 being the principal unit.

If the constants of multiplication are c_{ijk}, that is, if

$$e_i e_j = \sum_k c_{ijk} e_k \qquad (i, j = 1, 2, \cdots, n),$$

then the matrices

$$R_i = (c_{isr}), \quad S_i = (c_{ris})$$

are called the *first* and *second matrices*§ of e_i. If $\xi = \sum x_i e_i$ is the general number, then

$$R(\xi) = \sum x_i R_i, \quad S(\xi) = \sum x_i S_i$$

form sets of matrices each of which gives a matric representation of the algebra.

---

* Presented to the Society, December 30, 1930.

† C. C. MacDuffee, Transactions of this Society, vol. 31 (1929), pp. 71–90.

‡ Dickson, *Algebren und ihre Zahlentheorie*, 1927, p. 155.

§ MacDuffee, this Bulletin, vol. 35 (1929), p. 344.

A left (right) ideal $\mathfrak{R}$ is a set of numbers of $\mathfrak{S}$ which is closed under addition and subtraction, and under multiplication on the left (right) by the numbers of $\mathfrak{S}$. If not every number of $\mathfrak{R}$ is of norm* 0, $\mathfrak{R}$ is non-singular. We shall speak only of left ideals, as the theory of right ideals is obviously parallel.

Let $\mathfrak{R}_\alpha$ be an ideal with basis $(\alpha_1, \alpha_2, \cdots, \alpha_n)$. Then

$$\alpha_i = \sum_{j=1}^{n} g_{ij} e_j,$$

where the g_{ij} are rational integers. We shall call $G_\alpha = (g_{rs})$ an *ideal matrix* corresponding* to the ideal $\mathfrak{R}_\alpha$. If $|g_{rs}| \neq 0$, then $\mathfrak{R}_\alpha$ is non-singular. If G_α corresponds to the non-singular ideal $\mathfrak{R}_\alpha$, then the totality of ideal matrices corresponding to $\mathfrak{R}_\alpha$ is given by AG_α, where A is a matrix with rational integral elements (in brief, an integral matrix) of determinant ± 1.

If $\mathfrak{R}_\alpha$ and $\mathfrak{R}_\beta$ are two ideals, we define the ideal product $\mathfrak{R}_\alpha \mathfrak{R}_\beta$ to be the set of numbers

$$\delta = \sum_{i,j=1}^{n} d_{ij} \alpha_i \beta_j,$$

where the d_{ij} range over all rational integers. That this set is an ideal follows immediately, for if ξ is a number of $\mathfrak{S}$,

$$\xi\delta = \sum_{i,j} d_{ij} \xi \alpha_i \beta_j.$$

But

$$\xi\alpha_i = \sum_{h} e_{ih} \alpha_h,$$

where the e_{ih} are rational integers, since $\alpha_1, \cdots, \alpha_n$ form a basis for the ideal $\mathfrak{R}_\alpha$. Thus

$$\xi\delta = \sum_{i,j,h} d_{ij} e_{ih} \alpha_h \beta_j,$$

which is again a member of the set. We shall denote this product ideal by $\mathfrak{R}_\pi$. Note that ideal multiplication is not always commutative.

---

* MacDuffee, Transactions of this Society, loc. cit., p. 74.

Du Pasquier* has proved that if M and N are two integral square matrices of order n, not both singular, they possess a greatest common right divisor

$$D = PM + QN,$$

and that every g. c. r. d. of M and N is given by AD where A is an integral matrix of determinant ± 1. Thus the g. c. r. d. has the same latitude of definition as an ideal matrix. The theorem extends readily to n matrices, and du Pasquier shows how D may be readily computed.

3. THEOREM. *If the ideals K_α and K_β are represented by the matrices G_α and G_β respectively, then every matrix representing the product $K_\pi = K_\alpha K_\beta$ is a greatest common right divisor of the n matrices*

$$G_\alpha S(\beta_i), \qquad (i = 1, 2, \cdots, n),$$

and also of the matrices

$$G_\beta \overline{R}(\alpha_i), \qquad (i = 1, 2, \cdots, n),$$

where $\overline{R}$ is the transpose of R.

Suppose that

$$\alpha_i = \sum a_{ij}e_j,\ \beta_i = \sum b_{ij}e_j,\ \pi_i = \sum p_{ij}e_j,\ (i, j = 1, 2, \cdots, n).$$

Since every number of $K_\alpha K_\beta$ is in K_π, there exist in particular rational integers h_{ijk} such that

$$\alpha_i\beta_j = \sum_{k=1}^{n} h_{ijk}\pi_k, \quad (i, j = 1, 2, \cdots, n).$$

That is,

$$\sum_{k,l,m} a_{ik}b_{jl}c_{klm}e_m = \sum_{k,m} h_{ijk}p_{km}e_m.$$

On account of the linear independence of the basal numbers,

$$\sum_{k,l} a_{ik}b_{jl}c_{klm} = \sum_{k} h_{ijk}p_{km}, \quad (i, j, m = 1, 2, \cdots, n),$$

* Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich, vol. 51 (1906), p. 89.

which can be written in either of the two forms

$$\sum_k a_{rk}\left(\sum_l b_{jl}c_{kls}\right) = \sum_k h_{rjk}p_{ks},$$

$$\sum_l b_{rl}\left(\sum_k a_{ik}c_{kls}\right) = \sum_k h_{irk}p_{ks}.$$

In matric notation the first of these equations is

$$G_\alpha S(\beta_j) = H_{1j}G_\pi, \qquad H_{1j} = (h_{rjs}),$$

and the second is

$$G_\beta \overline{R}(\alpha_i) = H_{2i}G_\pi, \qquad H_{2i} = (h_{irs}).$$

Thus G_π is a common right divisor of the matrices $G_\alpha S(\beta_j)$, and also of the matrices $G_\beta \overline{R}(\alpha_i)$.

Since every number of K_π is in $K_\alpha K_\beta$, there exist rational integers k_{ijh} such that

$$\pi_i = \sum_{j,h} k_{ijh}\alpha_j\beta_h, \qquad (i = 1, 2, \cdots, n).$$

That is,

$$\sum_t p_{it}e_t = \sum_{j,h,l,m,t} k_{ijh}a_{jl}b_{hm}c_{lmt}e_t,$$

whence

$$p_{it} = \sum_{j,h,l,m} k_{ijh}a_{jl}b_{hm}c_{lmt}, \quad (i, t = 1, 2, \cdots, n).$$

This may be written in either of the forms

$$p_{rs} = \sum_{j,h,l} k_{rjh}a_{jl}\sum_m b_{hm}c_{lms},$$

$$p_{rs} = \sum_{j,h,m} k_{rjh}b_{hm}\sum_l a_{jl}c_{lms}.$$

In matric form these equations are, respectively,

$$G_\pi = \sum_h K_{1h}G_\alpha S(\beta_h), \qquad K_{1h} = (k_{rsh}),$$

$$G_\pi = \sum_j K_{2j}G_\beta \overline{R}(\alpha_j), \qquad K_{2j} = (k_{rjs}).$$

Thus G_π is a greatest common right divisor of the matrices $G_\alpha S(\beta_h)$ and also of the matrices $G_\beta \overline{R}(\alpha_j)$.

If the ideals K_α and K_β are non-singular, we may assume that not every α_i and not every β_i is of norm 0. In particular K_α and K_β may have canonical bases, in which case α_1 and β_1 are the smallest positive integers in the respective ideals. Thus not every $S(\beta_i)$ and not every $\overline{R}(\alpha_i)$ is singular. Since G_α and G_β are non-singular matrices, the matrix G_π is unique up to a left factor A which is an integral matrix of determinant ± 1.

4. *Canonical Form of an Ideal Product.* We shall indicate just one application of the preceding theorem. The problem of obtaining the canonical form of the product ideal from the canonical forms of the factors has been discussed for quadratic fields,* but not for the general case.

By the method of §3 the matrix G_π is obtained directly by du Pasquier's method when G_α and G_β are non-singular, that is, in the only case considered for algebraic fields. Then by a theorem due to Hermite† we can, by multiplying G_π on the left by an integral matrix A of determinant ± 1, obtain the canonical matrix

$$\begin{Vmatrix} g_{11} & 0 & 0 & \cdots & 0 \\ g_{12} & g_{22} & 0 & \cdots & 0 \\ g_{13} & g_{23} & g_{33} & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ g_{1n} & g_{2n} & g_{3n} & \cdots & g_{nn} \end{Vmatrix}$$

in which every $g_{ij} \geqq 0$, $g_{ii} > 0$, and each element in the ith column below the main diagonal is reduced modulo g_{ii}. Moreover this canonical form is unique.

All the steps in this reduction are mechanical and involve working only with rational integers.

CONNECTICUT COLLEGE, and OHIO STATE UNIVERSITY

---

* W. B. Carver, American Mathematical Monthly, vol. 18 (1911), pp. 81–87.

† Journal für Mathematik, vol. 41 (1851), p. 193.