AN INTRODUCTION TO THE THEORY OF IDEALS IN LINEAR ASSOCIATIVE ALGEBRAS*

BY

C. C. MACDUFFEE

1. Introduction. With the development of the number theory of linear algebras, it was natural that attempts should be made to extend to these domains of integrity the theory of ideal numbers. But it is evident from the few domains which have been examined that one cannot expect an extension of this theory in its entirety. For instance, Hurwitz† has investigated the number theory of quaternions by using right and left ideals, and has found that they are powerless to introduce unique factorization into this algebra. Moreover, Speiser‡ has recently investigated the properties of right, left and two-sided ideals in semi-simple algebras, remarking in the introduction to his paper that some of the most remarkable properties of ideals are "but foreign adjuncts which are essentially restricted to algebraic number fields."

Although it is historically true that ideals were introduced into algebraic number theory to establish unique factorization, it should be observed that this is a secondary function of ideals. Primarily they establish the property that every two numbers have a greatest common divisor expressible linearly in terms of the numbers. In algebraic fields this property implies unique factorization but in the general linear algebra it does not—hence the success of the ideal theory in algebraic fields and its partial failure in the more general domain.

The method which is here used in developing the theory of ideals is different from the usual one. It depends upon a correspondence§ between ideals and matrices whose elements are rational integers, and the only kind of multiplication which is employed is ordinary matric multiplication. Ideal multiplication, which plays such an important rôle in the usual treatment of ideals in algebraic fields, but which causes so much difficulty in non-commutative domains, is not employed in this paper.

---

* Presented to the Society, September 9, 1926; received by the editors in September, 1927.

† A. Hurwitz, *Vorlesungen über die Zahlentheorie der Quaternionen*, Berlin, Springer, 1919.

‡ A. Speiser, Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich, vol. 71 (1926), pp. 8–49.

§ Applied to quadratic ideals in a recent paper by the author, Annals of Mathematics, (2), vol. 29 (1927–28), pp. 199–214.

The fundamental theorem in the present development (Theorem 4) serves as a substitute for the commutative law in the multiplication of these ideal matrices. From this starting point we proceed to establish for general algebras many of the properties which ideals in algebraic fields are known to possess, including the important concept of class number. Furthermore, we obtain some properties of ideals in all semi-simple algebras which have not previously been found even in the special case of algebraic fields.

The writer is indebted to his colleague Professor Blumberg for helpful suggestions.

2. **Definition of ideal.** We suppose that $\mathfrak{A}$ is a rational semi-simple algebra of order n with a principal unit, and that $\mathfrak{S}$ is a set of integral elements of order n in $\mathfrak{A}$ according to the definition of Dickson.* 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.† We shall define a left (right) ideal $\mathfrak{R}$ to be 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 $\mathfrak{S}$.‡

We shall develop only the theory of left ideals, as the theory of right ideals is obviously parallel.

In the usual manner§ we can show that every left ideal $\mathfrak{R}$ has a basis composed of $r \leqq n$ linearly independent numbers $\omega_1, \omega_2, \cdots, \omega_r$. That is, the numbers of $\mathfrak{R}$ are represented by the form

$$k_1\omega_1 + k_2\omega_2 + \cdots + k_r\omega_r$$

where $k_1, k_2, \cdots, k_r$ are rational integral variables. In particular the ω_i may be chosen in the form

$$\begin{aligned}
\omega_1 &= a_{11}e_1, \\
\omega_2 &= a_{21}e_1 + a_{22}e_2, \\
&\cdots\cdots\cdots\cdots \\
\omega_r &= a_{r1}e_1 + a_{r2}e_2 + \cdots + a_{rr}e_r
\end{aligned}$$

where each $a_{ii} > 0$.

---

* L. E. Dickson, *Algebras and their Arithmetics*, University of Chicago Press, 1923, p. 141. *Algebren und ihre Zahlentheorie*, Zürich, 1927, p. 155. These books will be referred to as Dickson I and Dickson II, respectively.

† Dickson I, p. 163, II, p. 212.

‡ This is more general than the definition of Speiser, which further specifies that the set $\mathfrak{R}$ be of order n, thus excluding what we shall call singular ideals. See Dickson II, p. 270.

§ Dickson II, p. 270. Landau, *Theorie der algebraischen Zahlen und der Ideale*, Leipzig, 1918, p. 29, Theorem 99.

This number r, which is evidently the number of linearly independent numbers in every basis of $\mathfrak{R}$, is called the *rank* of the ideal. The ideal is called *singular* or *non-singular* according as $r<n$ or $r=n$.

3. **Some properties of ideals.** Every number a satisfies its rank equation*

$$\omega^r + c_1\omega^{r-1} + \cdots + c_{r-1}\omega + N(a) = 0.$$

From the definition of ideal it follows that if a is in $\mathfrak{R}$, then

$$N(a) = (-a^{r-1} - c_1a^{r-2} - \cdots - c_{r-1})a$$

is also in $\mathfrak{R}$. Hence $\mathfrak{R}$ contains rational integers unless every number of $\mathfrak{R}$ is of norm 0.

Let p be the smallest positive integer in the ideal $\mathfrak{R}$. Let c be any rational integer in $\mathfrak{R}$. Then we may write $c=kp+r$ where $0\leqq r<p$. Since c and p are in $\mathfrak{R}$, so is $c-kp=r$. But p was minimal, so $r=0$ and $c=kp$. Hence *if not every number of $\mathfrak{R}$ is of norm* 0, *$\mathfrak{R}$ contains infinitely many rational integers, each an integral multiple of a smallest positive integer. If a is a number of $\mathfrak{R}$, so is $N(a)$.*

Let $\mathfrak{R}$ be an ideal containing a positive integer p. Since $\mathfrak{S}$ is of order n, it contains n linearly independent numbers $s_1, s_2, \cdots, s_n$. Then $\mathfrak{R}$ contains the linearly independent numbers $s_1p, s_2p, \cdots, s_np$. It follows that *if $\mathfrak{R}$ contains a positive integer, the numbers $\omega_1, \omega_2, \cdots, \omega_n$ of every basis are linearly independent and $\mathfrak{R}$ is of rank n.*

Let $\omega_1', \omega_2', \cdots, \omega_n'$ constitute a second basis for an ideal $\mathfrak{R}$ of rank n. There are rational integers a_{ij} and b_{ij} such that

$$\omega_i = \sum_k a_{ik}\omega_k', \qquad \omega_i' = \sum_k b_{ik}\omega_k \qquad (i = 1,2, \cdots, n). \tag{3.1}$$

Then

$$\omega_i = \sum_{j,k} a_{ij}b_{jk}\omega_k,$$

and since the basal numbers are linearly independent,

$$\sum_j a_{ij}b_{jk} = \delta_{ik} \qquad (i,k = 1,2, \cdots, n)$$

so that (a_{rs}) is an integral matrix of determinant ± 1.

Conversely, if (a_{rs}) is an integral matrix of determinant ± 1, its inverse is likewise an integral matrix of determinant ± 1 and will serve as the matrix (b_{rs}) in (3.1). If the ω_i' constitute a basis for $\mathfrak{R}$, so do the ω_i as determined by

* Dickson I, p. 113.

(3.1). Thus *if* $\mathfrak{R}$ *is an ideal having a basis* $\omega_1, \omega_2, \cdots, \omega_n$ *composed of linearly independent numbers, every basis of* $\mathfrak{R}$ *is given by*

$$\omega_i' = \sum_j a_{ij}\omega_j \qquad (i = 1,2, \cdots, n)$$

where (a_{rs}) *is an integral matrix of determinant* ± 1.

If $\mathfrak{R}$ has a basis $\omega_1, \omega_2, \cdots, \omega_n$, we may write

$$\omega_i = \sum_j g_{ij}e_j \qquad (i = 1,2, \cdots, n), \tag{3.2}$$

where the g_{ij} are rational integers, in terms of the basal numbers $e_1, e_2, \cdots, e_n$ of $\mathfrak{S}$. We define the *norm* $N(\mathfrak{R})$ of the ideal $\mathfrak{R}$ to be the absolute value of the determinant $|g_{rs}|$. If $N(\mathfrak{R}) = 0$, the ω_i are linearly dependent and the rank r of $\mathfrak{R}$ is less than n; i.e., $\mathfrak{R}$ is singular.

Suppose that $\omega_1, \omega_2, \cdots, \omega_n$ constitute a linearly independent basis for $\mathfrak{R}$. If $\omega_1', \omega_2', \cdots, \omega_n'$ is any basis for $\mathfrak{R}$, we have

$$\omega_i' = \sum_j a_{ij}\omega_j = \sum_{j,k} a_{ij}g_{jk}e_k \equiv \sum_k g_{ik}'e_k \qquad (i = 1,2, \cdots, n)$$

where $|a_{rs}| = \pm 1$. Hence

$$(a_{rs})(g_{rs}) = (g_{rs}'),$$

which implies that

$$\text{absolute value } |g_{rs}'| = \text{absolute value } |g_{rs}| \neq 0,$$

so that the value of $N(\mathfrak{R})$ is independent of the basis chosen. In other words, $N(\mathfrak{R})$ is an invariant under change of basis and is therefore a positive integer intrinsically connected with the ideal $\mathfrak{R}$.

Let us now suppose that $\mathfrak{R}$ is an ideal for which $N(\mathfrak{R}) \neq 0$. From (3.2) we have

$$N(\mathfrak{R})e_i = \sum_j d_{ij}\omega_j \qquad (i = 1,2, \cdots, n)$$

where the d_{ij} are rational integers. Since e_1 is a principal unit, we see that $N(\mathfrak{R})$ is a positive integer in $\mathfrak{R}$. The norm of this positive integer is a non-zero integer in $\mathfrak{R}$, so that $\mathfrak{R}$ contains elements of norm not zero.

We may summarize the results of this paragraph in

THEOREM 3. *The following five statements are equivalent*:

(a) *Not every element of the ideal* $\mathfrak{R}$ *is of norm* 0.
(b) $\mathfrak{R}$ *contains rational integers.*
(c) *The numbers* $\omega_1, \omega_2, \cdots, \omega_n$ *of every basis of* $\mathfrak{R}$ *are linearly independent.*
(d) *The ideal* $\mathfrak{R}$ *is non-singular, i.e., of rank* n.
(e) *The norm* $N(\mathfrak{R})$ *of* $\mathfrak{R}$ *is not zero.*

We have shown that each statement implies the next following and that the last implies the first. Thus each of the five statements implies them all.

To see that ideals of norm zero actually exist, we need only to consider the principal ideal $(b]^*$ where $N(b)=0$, i.e., where b is a divisor of zero or zero itself. Then $\Delta(b)=0$, and for every number λ in $\mathfrak{S}$,

$$\Delta(\lambda b) = \Delta(\lambda)\cdot\Delta(b) = 0$$

so that $N(\lambda b)=0$ for every number λb in the ideal. Such ideals have none of the properties described in Theorem 3.

4. **A condition that n numbers constitute a basis for an ideal.** While it is true that every left ideal has a basis $\omega_1, \omega_2, \cdots, \omega_n$ composed of integral numbers, it does not follow that every n numbers of $\mathfrak{S}$ constitute a basis for a left ideal. We shall find necessary and sufficient conditions that n numbers $\omega_1, \omega_2, \cdots, \omega_n$ of $\mathfrak{S}$ shall form a basis for a left ideal.

Let us assume that $\omega_1, \omega_2, \cdots, \omega_n$ constitute a basis for a left ideal $\mathfrak{R}$, and that

$$\omega_i = \sum_j g_{ij}e_j \qquad (i = 1,2,\cdots,n). \tag{4.1}$$

Every number k of $\mathfrak{R}$ is of the form

$$k = \sum_i k_i\omega_i = \sum_{i,j} k_i g_{ij} e_j.$$

Every number s of $\mathfrak{S}$ is of the form

$$s = \sum_l s_l e_l.$$

Since sk is in $\mathfrak{R}$, there exist rational integers d_r such that

$$sk = \sum_{l,i,j} s_l k_i g_{ij} e_l e_j = \sum_{l,i,j,h} s_l k_i g_{ij} c_{ljh} e_h = \sum_{r,t} d_r g_{rt} e_t.$$

Since the basal numbers are linearly independent, this implies

$$\sum_{l,i,j} s_l k_i g_{ij} c_{ljt} = \sum_r d_r g_{rt} \qquad (t = 1,2,\cdots,n).$$

In particular there must exist rational integers d_r, which we shall call d_{pqr}, when $s_l = \delta_{lp}$ and $k_i = \delta_{iq}$. For these values we have

$$\sum_j g_{qj} c_{pjt} = \sum_r d_{pqr} g_{rt} \qquad (p,q,t = 1,2,\cdots,n). \tag{4.2}$$

---

* The notation is due to Speiser. See Dickson II, p. 271.

The existence of integers d_{pqr} satisfying (4.2) is in fact sufficient that the integral numbers $\omega_1, \omega_2, \cdots, \omega_n$ defined by (4.1) constitute a basis for a left ideal. For, let d_{pqr} and g_{qi} be any rational integers satisfying (4.2). Define the ω_i by (4.1). The set of numbers

$$k = \sum_i k_i \omega_i$$

where the k_i vary independently over $\mathfrak{S}$ is evidently closed under addition and subtraction. We can show that it is closed under multiplication on the left by any number s of $\mathfrak{S}$. In fact

$$sk = \sum_{l,i,j,r} s_l k_i g_{ij} c_{ljr} e_r = \sum_{l,i,r} s_l k_i \sum_j g_{ij} c_{ljr} e_r .$$

Hence by (4.2) we have

$$sk = \sum_{l,i,r} s_l k_i \left(\sum_s d_{lis} g_{sr} \right) e_r = \sum_{l,i,s} s_l k_i d_{lis} \omega_s ,$$

which is obviously of the form $\sum_i k_i' \omega_i$.

Let us define the matrices

$$C_p = (c_{prs}) = \text{transpose } R_p, \quad D_p = (d_{prs}), \quad G = (g_{rs}) \qquad (p = 1, 2, \cdots, n).$$

We may now state

THEOREM 4.* *A necessary and sufficient condition in order that $\omega_1, \omega_2, \cdots, \omega_n$ constitute a basis for a left ideal is that there exist integral matrices $D_1, D_2, \cdots, D_n$ such that*

$$GC_p = D_p G \qquad (p = 1, 2, \cdots, n)$$

where G is the matrix (g_{rs}) of (4.1)

5. An explicit basis for a principal ideal. In particular every principal ideal $(d]$ has a basis $\omega_1, \omega_2, \cdots, \omega_n$. We have

$$d = \sum_i d_i e_i, \qquad \omega_i = \sum_j g_{ij} e_j \qquad (i = 1, 2, \cdots, n).$$

Let $s = \sum s_i e_i$ be any number of $\mathfrak{S}$. Then

$$sd = \sum_{i,j,k} s_i d_j c_{ijk} e_k$$

is in $(d]$, and hence must be representable in the form

$$sd = \sum_i r_i \omega_i = \sum_{i,j} r_i g_{ij} e_j .$$

* Poincaré, using the same correspondence between ideals and matrices, obtained a quite different condition that a matrix in canonical form correspond to an ideal. Bulletin de la Société Mathématique de France, vol. 13 (1885), p. 167.

It follows that for all rational integers s_i there must exist rational integers r_i such that

$$\sum_{i,j} s_i d_j c_{ijk} = \sum_i r_i g_{ik} \qquad (k = 1,2, \cdots, n). \tag{5.1}$$

Conversely, since every linear combination of the ω_i is in $(d]$, it follows that for all integers r_i there must exist integers s_i such that (5.1) holds. These conditions together are necessary and sufficient in order that $\omega_1, \omega_2, \cdots, \omega_n$ form a basis for the principal left ideal $(d]$.

In particular, let us take $r_i = \delta_{hi}$, and denote the corresponding values of s_i by s_{hi}. Then (5.1) gives

$$\sum_{i,j} s_{hi} d_j c_{ijk} = \sum_i \delta_{hi} g_{ik} = g_{hk} \quad (h,k = 1,2, \cdots, n). \tag{5.2}$$

Again, let us choose $s_i = \delta_{hi}$ in (5.1) and denote the corresponding values of r_i by r_{hi}. Then we have

$$\sum_{i,j} \delta_{hi} d_j c_{ijk} = \sum_j d_j c_{hjk} = \sum_i r_{hi} g_{ik} \qquad (h,k = 1,2, \cdots, n). \tag{5.3}$$

From (5.2) we have, taking matrices,

$$G = (g_{rs}) = (s_{rs})(\sum d_j c_{rjs}) = (s_{rs}) S(d)$$

where $S(d)$ is the transposed second matrix* of d. In the same way we obtain from (5.3)

$$S(d) = (r_{rs}) G.$$

Every number of the ideal $(d]$ is of the form

$$\sum_i a_i \omega_i = \sum_{i,j} a_i g_{ij} e_j = \sum_{i,k,j} a_i s_{ik} \sigma_{kj} e_j,$$

where $S(d) = (\sigma_{rs})$, and conversely every number of the form $\sum b_i \sigma_{ij} e_j$ can be written

$$\sum_{i,j} b_i \sigma_{ij} e_j = \sum_{i,k,j} b_i r_{ik} g_{kj} e_j = \sum_{i,k} b_i r_{ik} \omega_k$$

and is therefore in $(d]$. Hence the numbers $\sum \sigma_{ij} e_j$ constitute a basis for $(d]$.

It follows from the definition of norm that $N((d]) = $ *absolute value* $S(d) = $ *absolute value* $\Delta'(d)$. We have now proved

THEOREM 5.1. *The principal left ideal* $(d]$ *has a basis* $\omega_1, \omega_2, \cdots, \omega_n$ *where*

$$\omega_i = \sum_j \sigma_{ij} e_j, \quad (\sigma_{rs}) = S(d) ;$$

the norm of $(d]$ *is the absolute value of* $\Delta'(d)$.

* Dickson I, p. 86, II, p. 35. It is easy to show that d is an integral number if and only if $S(d)$ has integral elements.

The conditions for associativity may be written

$$\sum_j c_{qkj}c_{pjs} = \sum_j c_{pqj}c_{jks}.$$

Let us multiply by d_k and sum for k:

$$\sum_{j,k} d_k c_{qkj}c_{pjs} = \sum_{j,k} c_{pqj}d_k c_{jks},$$

which may be written

$$S(d)C_p = C_pS(d) \qquad (p = 1,2,\cdots,n)$$

where $d=\sum d_ie_i$. This is exactly (4.2) with g_{ij} replaced by σ_{ij} and d_{pqr} replaced by c_{pqr}.

THEOREM 5.2. *For every number d in $\mathfrak{S}$, $S(d)$ is commutative with every matrix C_p; and if $G=S(d)$ in Theorem 4, then $D_p=C_p$ for every p.*

We shall prove later (Theorem 11) that every integral matrix commutative with every C_p is the transposed second matrix $S(d)$ of some number d of $\mathfrak{S}$.

6. **Equivalent ideals.** Let $\mathfrak{R}$ be a non-singular left ideal with basis $\omega_1, \omega_2, \cdots, \omega_n$, and let s be a number of $\mathfrak{S}$. If we set

$$\omega_i = \sum_j g_{ij}e_j, \qquad s = \sum_q s_q e_q,$$

we have

$$\omega_i s \equiv \sum_j g'_{ij}e_j = \sum_p g_{ip}e_p \sum_q s_q e_q$$
$$= \sum_{p,q,r} g_{ip}s_q c_{pqr}e_r.$$

Hence

$$g'_{ij} = \sum_{p,q} g_{ip}s_q c_{pqj} = \sum_p g_{ip} \sum_q s_q c_{pqj} = \sum_p g_{ip}\sigma_{pj}.$$

Taking matrices, we have

$$G' = GS(s).$$

But

$$GC_p = D_pG, \qquad S(s)C_p = C_pS(s),$$

so that

$$G'C_p = GS(s)C_p = GC_pS(s) = D_pGS(s) = D_pG'.$$

Therefore $\omega_1 s, \omega_2 s, \cdots, \omega_n s$ form a basis for an ideal which we may call $\mathfrak{R}'$.

Furthermore, we obtain the same ideal $\mathfrak{R}'$ irrespective of the basis of $\mathfrak{R}$ with which we start. Using any other basis for $\mathfrak{R}$, we should have obtained, instead of G',

$$G'' = AGS(s)$$

where A is an integral matrix of determinant ± 1 (§3). But $G'' = AG'$ corresponds to the same ideal $\mathfrak{R}'$ as does G'. For a non-singular ideal $\mathfrak{R}$ we may call the uniquely existing ideal having the basis $(\omega_1 s, \omega_2 s, \cdots, \omega_n s)$ where $(\omega_1, \omega_2, \cdots, \omega_n)$ is any basis for $\mathfrak{R}$, the ideal $\mathfrak{R}s$.

Two non-singular ideals $\mathfrak{R}_1$ and $\mathfrak{R}_2$ are, according to analogy with the usual definition in algebraic number theory, called *equivalent* if there exist integral numbers s_1 and s_2 of $\mathfrak{S}$, neither of norm 0, such that

$$\mathfrak{R}_1 s_1 = \mathfrak{R}_2 s_2.$$

Let G_1 and G_2 be the matrices corresponding to particular bases of $\mathfrak{R}_1$ and $\mathfrak{R}_2$ respectively. The condition for equivalence becomes

$$G_1 S(s_1) = A G_2 S(s_2)$$

where A is an integral matrix of determinant ± 1.

The following theorem is important in showing that the concept of ideal class applies to all semi-simple domains and in pointing to a more comprehensive definition which is applicable to singular ideals as well.

THEOREM 6. *A necessary and sufficient condition that two non-singular ideal matrices G_1 and G_2 be equivalent is that the corresponding sets of matrices D_{1p}, D_{2p} satisfying the equations*

$$G_1 C_p = D_{1p} G_1, \quad G_2 C_p = D_{2p} G_2 \qquad (p = 1, 2, \cdots, n)$$

respectively, be similar—i.e., that $D_{1p} = A D_{2p} A^{-1}$ for $p = 1, 2, \cdots, n$, where A is an integral matrix of determinant ± 1.

First, let us suppose that G_1 and G_2 are equivalent. We have

$$G_1 C_p = D_{1p} G_1, \qquad G_2 C_p = D_{2p} G_2,$$
$$G_1 S(s_1) = A G_2 S(s_2), \qquad |A| = \pm 1$$

where $S(s_1)$ and $S(s_2)$ are each, by Theorem 5.2, commutative with every C_p. Then

$$G_1 S(s_1) C_p = G_1 C_p S(s_1) = D_{1p} G_1 S(s_1),$$
$$A G_2 S(s_2) C_p = A G_2 C_p S(s_2) = A D_{2p} G_2 S(s_2)$$
$$= A D_{2p} A^{-1} A G_2 S(s_2).$$

Therefore

$$D_{1p} G_1 S(s_1) = A D_{2p} A^{-1} G_1 S(s_1).$$

Since both G_1 and $S(s_1)$ are non-singular, we have

$$D_{1p} = A D_{2p} A^{-1} \qquad (p = 1, 2, \cdots, n).$$

Secondly, suppose that the sets of matrices D_{1p} and D_{2p} are similar:

$$G_1C_p = D_{1p}G_1, \quad G_2C_p = D_{2p}G_2, \quad D_{1p} = AD_{2p}A^{-1}, \quad |A| = \pm 1.$$

Then

$$G_1C_pG_1^{-1} = D_{1p} = AD_{2p}A^{-1} = AG_2C_pG_2^{-1}A^{-1}.$$

We multiply on the left by $G_2^{-1}A^{-1}$ and on the right by G_1, obtaining

$$G_2^{-1}A^{-1}G_1C_p = C_pG_2^{-1}A^{-1}G_1.$$

Let T be the scalar matrix each of whose diagonal elements is $|G_2|$. Then $TG_2^{-1}A^{-1}G_1$ is an integral matrix and, since it is commutative with each C_p, it is the second matrix $S(s)$ of some element s of $\mathfrak{S}$.* Then

$$TG_2^{-1}A^{-1}G_1 = S(s),$$

and since T is commutative with every matrix,

$$G_1T = AG_2S(s).$$

Moreover, $T = S(|G_2|)$, so that the ideals $\mathfrak{R}_1$ and $\mathfrak{R}_2$ are in fact equivalent.

7. **Ideal matrices.** An essential point in our proof of Theorem 6 was that $|G_1| \neq 0$. We were therefore unable to consider equivalence of singular ideals. Moreover, the transitive character of equivalence was not apparent from its definition. We now proceed along a line suggested by this theorem but somewhat broader.

We assume a semi-simple rational algebra $\mathfrak{A}$, and a set of integral numbers $\mathfrak{S}$ of order n, the basal numbers being chosen so that the constants c_{ijk} of multiplication are rational integers. As before, we define the matrices $C_p = (c_{prs})$ for $p = 1, 2, \cdots, n$, where c_{prs} is the element in row r and column s. Let $D_p = (d_{prs})$ be any set of n integral matrices. All the integral matrices G which satisfy the equations

$$GC_p = D_pG \qquad (p = 1, 2, \cdots, n) \tag{7.1}$$

will be said to constitute a *minor class* of *ideal matrices*, and the set of matrices $D_1, D_2, \cdots, D_n$ will be called a set of corresponding *class matrices*. The zero matrix at least will satisfy (7.1) no matter how the class matrices may be chosen.

All the matrices of a minor class constitute a modul. In fact, if $G_1, G_2, \cdots, G_p$ are ideal matrices of the same minor class and if $k_1, k_2, \cdots, k_p$ are rational integers, then

$$G = k_1G_1 + k_2G_2 + \cdots + k_pG_p$$

* Theorem 11, to follow.

is an ideal matrix of the same minor class. We shall show that if $\mathfrak{A}$ is semi-simple there exist $r \leqq n$ linearly independent matrices $B_1, B_2, \cdots, B_r$ which constitute a basis for the ideal matrices of the minor class.

LEMMA 7. *If $\mathfrak{A}$ is a semi-simple algebra, new basal numbers for $\mathfrak{S}$ and new constants of multiplication c'_{ijk} can be so chosen that $|c'_{rs1}| \neq 0$.*

Let us suppose that our basal numbers are chosen as in §2, and that the c_{ijk} are defined by

$$e_i e_j = \sum_k c_{ijk} e_k \qquad (i,j = 1,2, \cdots, n). \tag{7.2}$$

Since e_1 is a principal unit, $c_{1jk} = c_{j1k} = \delta_{jk}$. If we apply to the basal numbers the transformation

$$e_i = \sum_j a_{ij} e'_j, \qquad a = |a_{rs}| \neq 0, \tag{7.3}$$

we get from (7.2):

$$\sum_{p,q} a_{ip} a_{jq} e'_p e'_q = \sum_{r,s} c_{ijr} a_{rs} e'_s = \sum_{p,q,t} a_{ip} a_{jq} c'_{pqt} e'_t$$

so that

$$\sum_{p,q} a_{rp} a_{sq} c'_{pqj} = \sum_i c_{rsi} a_{ij} \qquad (r,s,j = 1,2, \cdots, n), \tag{7.4}$$

where the c'_{pqs} are defined as in (7.2) with each letter primed. For a fixed j, let us form the determinant whose element in row r and column s is (7.4):

$$a^2 |c'_{rsj}| = \left| \sum_i a_{ij} c_{rsi} \right| \qquad (j = 1,2, \cdots, n). \tag{7.5}$$

In (7.3) let us now choose

$$a_{ij} = \tau_{ij} \equiv \sum_{r,k} c_{ijr} c_{rkk}.$$

If $\mathfrak{A}$ is semi-simple, $a = |\tau_{rs}| \equiv d \neq 0$,* and

$$a_{r1} = \sum_{h,k} c_{r1h} c_{hkk} = \sum_{h,k} \delta_{hr} c_{hkk} \equiv \sum_k c_{rkk}$$

so that

$$\sum_r a_{r1} c_{ijr} = \sum_{r,k} c_{ijr} c_{rkk} = \tau_{ij}.$$

---

* Dickson I, p. 108.

From (7.5) with $j=1$ we obtain

$$d^2 \left| c'_{rs1} \right| = d$$

so that $|c'_{rs1}| \neq 0$.

In making this transformation we may have lost the property that the basal numbers of $\mathfrak{A}$ form a basis for the set $\mathfrak{S}$ of integral numbers. We must now restore this property.

Bring* the fractions c'_{ijk} to a common denominator δ, write $\delta c'_{ijk} = h_{ijk}$ where the h_{ijk} are all integers. Set $\epsilon_i = \delta e'_i$. Then

$$\epsilon_i \epsilon_j = \delta^2 e'_i e'_j = \delta^2 \sum_k c'_{ijk} e'_k = \sum_k h_{ijk} \epsilon_k .$$

We use the new basal numbers ϵ_i whose constants h_{ijk} of multiplication are rational integers. We note that

$$\left| h_{rs1} \right| = \left| \delta c'_{rs1} \right| = \delta^n \left| c'_{rs1} \right| \neq 0.$$

Proceeding according to the method of Dickson,† we see that every element x of $\mathfrak{S}$ can be put into the form

$$x = \frac{x_1}{D}\epsilon_1 + \frac{x_2}{D}\epsilon_2 + \cdots + \frac{x_n}{D}\epsilon_n \tag{7.6}$$

where

$$D = \left| \sum_{i,k} h_{rsi} h_{ikk} \right| \neq 0,$$

and where the x_i are rational integers. Of all numbers x in $\mathfrak{S}$ having $x_1 = x_2 = \cdots = x_{r-1} = 0$ but $x_r \neq 0$, choose one having $x_r > 0$ and minimal for ϵ'_r. If there is no x of this type having $x_r \neq 0$, choose $\epsilon'_r = 0$. We have

$$\begin{aligned} D\epsilon'_1 &= b_{11}\epsilon_1 + b_{12}\epsilon_2 + \cdots + b_{1n}\epsilon_n , \\ D\epsilon'_2 &= \qquad b_{22}\epsilon_2 + \cdots + b_{2n}\epsilon_n , \\ &\cdots\cdots\cdots\cdots \\ D\epsilon'_n &= \qquad\qquad\qquad b_{nn}\epsilon_n . \end{aligned} \tag{7.7}$$

Now $(\epsilon'_1, \epsilon'_2, \cdots, \epsilon'_n)$ form a basis for $\mathfrak{S}$. For, let

$$x = \frac{1}{D}(x_1\epsilon_1 + x_2\epsilon_2 + \cdots + x_n\epsilon_n)$$

---

* Dickson I, pp. 161–162.

† Dickson I, p. 162.

be any number of $\mathfrak{S}$. Set

$$x_1 = q_1 b_{11} + r_1 \qquad (0 \leqq r_1 < b_{11}).$$

Then

$$x - q_1\epsilon_1' = \frac{1}{D}(r_1\epsilon_1 + x_2'\epsilon_2 + \cdots + x_n'\epsilon_n)$$

has its coefficient of ϵ_1 less than b_{11} which was minimal, so $r_1 = 0$. Similarly, set

$$x_2' = q_2 b_{22} + r_2 \qquad (0 \leqq r_2 < b_{22}).$$

Then $x - q_1\epsilon_1' - q_2\epsilon_2'$ lacks the basal numbers ϵ_1 and ϵ_2. Proceeding in this way, we have after n steps:

$$x = q_1\epsilon_1' + q_2\epsilon_2' + \cdots + q_n\epsilon_n'$$

where the q_i are rational integers. Since $\mathfrak{S}$ is of order n, we now know that $b_{ii} \neq 0$ for every i.

Since the numbers $\epsilon_1', \epsilon_2', \cdots, \epsilon_n'$ form a basis for $\mathfrak{S}$, we know that the new constants h'_{ijk} of multiplication are rational integers. Transformation (7.7) can be written

$$\epsilon_i = \frac{D}{b}\sum_j B_{ji}\epsilon_j' \qquad (i = 1, 2, \cdots, n)$$

where $b = |b_{rs}|$ and B_{rs}, the cofactor of b_{rs}, is zero for $r < s$. From (7.5) we have

$$a^2 |h'_{rs1}| = \left| \sum_i a_{i1} h_{rsi} \right|$$

with $a_{ij} = (1/b)DB_{ji} = 0$ for $i > j$. Hence

$$a^2 |h'_{rs1}| = a_{11}^n |h_{rs1}| \neq 0,$$

and therefore $|h'_{rs1}| \neq 0$.

Since the basal numbers $e_1, e_2, \cdots, e_n$ with which we started and the numbers $\epsilon_1', \epsilon_2', \cdots, \epsilon_n'$ each form a basis for the set $\mathfrak{S}$, we know that there are transformations with rational integral coefficients and of determinants ± 1 carrying each set of basal numbers into the other set.

8. Effect of change of basis on the fundamental matrices. Let us make a change of basis (7.3) where the a_{rs} are rational integers of determinant ± 1. By (7.4) we have

$$\sum_r c_{pir} a_{rt} = \sum_{s,q} a_{ps} a_{iq} c'_{sqt}.$$

Multiply by the cofactor A_{jt} of a_{jt} and sum for t. Then

$$ac_{pij} = \sum_{q,t} a_{iq}\left[\sum_{s} a_{ps}c'_{sqt}\right]A_{jt}.$$

Passing to matrices, we have

$$C_p = A\left[\sum_{s} a_{ps}C'_s\right]A^{-1} \qquad (p = 1,2,\cdots,n)$$

where $A \equiv (a_{rs})$ as our induced transformation on the matrices C_p.

We shall more generally define the matrices D'_p, which will be said to correspond to the matrices D_p under transformation (7.3) of determinant ± 1, as the solutions of the equations

$$D_p = A\left[\sum_{s} a_{ps}D'_s\right]A^{-1} \qquad (p = 1,2,\cdots,n). \tag{8.1}$$

The matrices D'_p are evidently integral if the matrices D_p are integral. Our definition is justified by the following result:

LEMMA 8.1. *If G is an ideal matrix satisfying the equations*

$$GC_p = D_pG \qquad (p = 1,2,\cdots,n),$$

then $G' = A^{-1}GA$ satisfies the equations

$$G'C'_p = D'_pG' \qquad (p = 1,2,\cdots,n)$$

where C'_p and D'_p are given by (8.1).

From (8.1) and the equations $GC_p = D_pG$, we have

$$GA\left[\sum_{s} a_{ps}C'_s\right]A^{-1} = A\left[\sum_{s} a_{ps}D'_s\right]A^{-1}G,$$

and therefore

$$A^{-1}GA\left[\sum_{s} a_{ps}C'_s\right] = \left[\sum_{s} a_{ps}D'_s\right]A^{-1}GA.$$

If we multiply by the cofactor A_{pr} of a_{pr} and sum for p, we obtain

$$A^{-1}GAC'_r = D'_rA^{-1}GA,$$

which proves the lemma.

LEMMA 8.2. *If the basis of $\mathfrak{S}$ is so chosen that $|c_{r\cdot 1}| \neq 0$, then an ideal matrix G whose first column consists exclusively of zeros is a zero matrix.*

From our definition of ideal matrix we have

$$\sum_k g_{rk}c_{pks} = \sum_k d_{prk}g_{ks} \qquad (p,r,s = 1,2,\cdots,n).$$

If $g_{k1}=0$ for every k, then

$$\sum_k g_{rk}c_{pk1} = 0 \qquad (r,p = 1,2,\cdots,n).$$

Taking matrices, we have

$$G(c_{sr1}) = 0.$$

Since the second matrix is non-singular, G must be of rank 0.

9. A fundamental theorem. Let $\mathfrak{A}$ be a semi-simple algebra, and let $e_1, e_2, \cdots, e_n$ be a basis for a set $\mathfrak{S}$ of integral numbers of $\mathfrak{A}$, where e_1 is a principal unit. We transform by a matrix A of determinant ± 1 to another basis $e_1', e_2', \cdots, e_n'$ for which $|c'_{rs1}| \neq 0$. Every ideal matrix G is thereby transformed into an ideal matrix $G'=A^{-1}GA$, and inversely $G=AG'A^{-1}$, so that there is a one-to-one correspondence between the ideal matrices G and G'.

If G' is an ideal matrix of a certain minor class, so is $-G'$. If in the minor class defined by the class matrices $D_1', D_2', \cdots, D_n'$ (§7), there are ideal matrices $G'=(g_{rs})$ in which $g_{11}\neq 0$, define as B_1' one such matrix in which $g_{11}>0$ and is minimal. If no such matrix exists, set $B_1'=0$, which surely is in the minor class. If there are in the minor class matrices for which $g_{11}=g_{21}=\cdots=g_{k-1,1}=0$ but $g_{k1}\neq 0$, define as $B_k'=(b_{krs})$ one such matrix in which $g_{k1}=b_{kk1}>0$ and is minimal, otherwise set $B_k'=0$. Then B_1', $B_2', \cdots, B_n'$ form a basis for the matrices of the minor class.

For, let $G'=(g_{rs})$ be any matrix of the minor class. Set

$$g_{11} = h_1 b_{111} + r_1 \qquad (0 \leqq r_1 < b_{111}).$$

Then $G'-h_1B_1'=(g_{rs}')$ is an ideal matrix of the minor class having as its first element r_1. But b_{111} was minimal, so $r_1=0$. Now set

$$g_{21}' = h_2 b_{221} + r_2 \qquad (0 \leqq r_2 < b_{221}).$$

Similarly

$$G' - h_1B_1' - h_2B_2'$$

has two zeros in its first column. Proceeding in this way, we find after n steps that

$$G' - h_1B_1' - h_2B_2' - \cdots - h_nB_n'$$

is an ideal matrix of the minor class whose first column consists exclusively of zeros, and which by Lemma 8.2 is therefore the zero matrix. Thus

$$G' = h_1B_1' + h_2B_2' + \cdots + h_nB_n'$$

where $h_1, h_2, \cdots, h_n$ are rational integers.

Let us now transform back to our original basis. We have $G=AG'A^{-1}$, and we define $B_i \equiv AB_i'A^{-1}$, so that every ideal matrix G is expressible in the form

$$G = h_1B_1 + h_2B_2 + \cdots + h_nB_n$$

where the $h_1, h_2, \cdots, h_n$ are rational integers. Conversely, every such matrix is in the minor class. We now have

THEOREM 9. *Relative to every basis $e_1, e_2, \cdots, e_n$ for a set $\mathfrak{S}$ of integral elements of a semi-simple rational algebra $\mathfrak{A}$, every minor class of ideal matrices has a basis composed of n matrices $B_1, B_2, \cdots, B_n$ such that the totality of ideal matrices of the minor class is given by*

$$h_1B_1 + h_2B_2 + \cdots + h_nB_n$$

where $h_1, h_2, \cdots, h_n$ are independent rational integral variables.

10. **Rank of a minor class.** Suppose that as in the preceding paragraph we have a set $\mathfrak{S}$ of integral numbers with basis so chosen that $|c'_{rs1}| \neq 0$. Then we have seen that every minor class has a basis $B_1', B_2', \cdots, B_n'$ such that in each matrix $B_k' \equiv (b_{krs})$ we have $b_{kr1}=0$ for $r<k$, and either $b_{kk1}>0$ and minimal, or $B_k'=0$. Suppose that the B_k' are linearly dependent:

$$d_1B_1' + d_2B_2' + \cdots + d_nB_n' = 0,$$

where we may assume that the d_i are rational integers not all zero. Considering only elements in the first columns, we have

$$d_1b_{1r1} + d_2b_{2r1} + \cdots + d_nb_{nr1} = 0 \quad (r = 1,2, \cdots, n).$$

Suppose that $d_1=d_2=\cdots=d_{p-1}=0$ while $d_p \neq 0$. Then we have $d_pb_{pp1}=0$ so that $b_{pp1}=0$ and hence $B_p'=0$.

If there is a dependence relation among the remaining $n-1$ basal matrices B_i', we may repeat the argument and show that another one is zero. We finally reach a point where all the basal matrices which are not zero are linearly independent. The number r of linearly independent matrices in a basis is called the *rank* of the minor class, and if $r<n$ the class is called *singular*. When we transform to another basis for $\mathfrak{S}$, we see from the relation $B_i=AB_i'A^{-1}$ that the rank is preserved.

Just as in the case of change of basis of an ideal, it can be shown that, relative to the same basis for $\mathfrak{S}$, the most general transformation from one linearly independent basis to another is given by

$$B_i' = \sum_{j=1}^{r} a_{ij}B_j \qquad (i = 1,2, \cdots, r)$$

where (a_{rs}) is an integral matrix of determinant ± 1. The rank is preserved under such transformations also.

11. **The principal minor class.** All matrices commutative with the fundamental matrices C_p evidently constitute a minor class, called the *principal* minor class. The members of this class we shall call *principal* ideal matrices. We shall now prove the result required to complete the proof of Theorem 6:

THEOREM 11. *Every principal ideal matrix is the transposed second matrix $S(k)$ of some integral number k of $\mathfrak{S}$, and conversely.*

The conditions for associativity may be written*

$$\sum_h c_{rih}c_{phs} = \sum_h c_{prh}c_{his}$$

or

$$(c_{ris})C_p = C_p(c_{ris}).$$

That is, the matrices $(c_{ris}) = S_i = S(e_i)$ belong to the principal minor class. Let $k = k_1e_1 + k_2e_2 + \cdots + k_ne_n$ be any integral number. Then

$$S(k) = k_1S_1 + k_2S_2 + \cdots + k_nS_n$$

where the k_i are rational integers, and therefore $S(k)$ is in the principal minor class. This proves the converse.

We consider now the set of all matrices G which are commutative with every C_p. We have seen that every such minor class has a basis $B_1, B_2, \cdots, B_n$. Since the matrices S_i are in this set, we have

$$S_i = \sum_j a_{ij}B_j \qquad (i = 1, 2, \cdots, n)$$

where the a_{ij} are rational integers. Now $|a_{rs}| \neq 0$, since the S_i are linearly independent. Therefore we can solve these equations for the B_i, obtaining

$$B_i = \sum_j r_{ij}S_j = S(r_i) \qquad (i = 1, 2, \cdots, n)$$

where each r_{ij} is rational, and $r_i = r_{i1}e_1 + r_{i2}e_2 + \cdots + r_{in}e_n$ is a number of the algebra $\mathfrak{A}$. But $S(r_i) = B_i$ is an integral matrix, and hence by the footnote to §5 each r_i is an integral number and therefore the r_{ij} are rational integers. Then every matrix

$$G = h_1B_1 + h_2B_2 + \cdots + h_nB_n$$

can be written

$$G = S(k), \qquad k = \sum_{i,j} h_ir_{ij}e_j,$$

* Dickson I, p. 92.

where the h_i and r_{ij} are rational integers, so that k is a number of $\mathfrak{S}$. This completes the proof of the theorem.

12. **The class number.** We shall now establish a few properties of minor classes.

THEOREM 12.1. *If G is an ideal matrix of the minor class $\mathfrak{k}$, and if P is a principal ideal matrix, then GP is an ideal matrix of the minor class $\mathfrak{k}$.*

Let $D_1, D_2, \cdots, D_n$ be the class matrices defining the minor class $\mathfrak{k}$. Then

$$GC_p = D_pG, \qquad PC_p = C_pP \qquad (p = 1,2, \cdots, n).$$

Therefore

$$GPC_p = GC_pP = D_pGP,$$

which proves the theorem.

THEOREM 12.2. *If the minor class $\mathfrak{k}$ contains one non-singular ideal matrix G, then the n basal matrices of $\mathfrak{k}$ are linearly independent, and $\mathfrak{k}$ is of rank n.*

Let G be a non-singular matrix of $\mathfrak{k}$. Let $P_1, P_2, \cdots, P_n$ be linearly independent matrices of the principal class. Then $GP_1, GP_2, \cdots, GP_n$ are linearly independent matrices of class $\mathfrak{k}$, for if there were a dependence relation

$$\sum_i d_iGP_i = G\sum_i d_iP_i = 0, \tag{12.1}$$

where G is a non-singular matrix, we should have $\sum d_iP_i=0$, contrary to assumption. Let $B_1, B_2, \cdots, B_n$ be a basis for $\mathfrak{k}$. Then

$$GP_i = \sum_j b_{ij}B_j \qquad (i = 1,2, \cdots, n),$$

and since the GP_i are linearly independent, so are the basal matrices B_j. Thus the rank of $\mathfrak{k}$ is n.

THEOREM 12.3. *If $\mathfrak{A}$ is a division algebra, every minor class except the zero class is non-singular.*

Since $\sum d_iP_i$ is the transposed second matrix of a number of $\mathfrak{A}$, it is either of rank n or of rank 0. Thus in (12.1) either $G=0$, or else $d_1=d_2=\cdots=d_n=0$ and the matrices GP_i are linearly independent.

THEOREM 12.4. *If two minor classes contain the same non-singular ideal matrix, the classes coincide.*

Suppose that

$$GC_p = D_{1p}G, \quad GC_p = D_{2p}G, \quad |G| \neq 0 \quad (p = 1,2, \cdots, n).$$

Then $D_{1p}G = D_{2p}G$, and since G is non-singular, $D_{1p} = D_{2p}$ for every p. Thus the minor classes coincide.

The theorem is not true with the omission of the word "non-singular." Thus the zero matrix is common to every minor class.

In general we shall not expect the number of minor classes to be finite. Thus $D_1, D_2, \cdots, D_n$ may be taken as perfectly arbitrary integral matrices, and the equations $GC_p = D_pG$ will be satisfied by the zero matrix at least. Moreover, if there be matrices satisfying a relation $GC_p = D_pG$, then

$$AGC_p = AD_pA^{-1}AG,$$

so that the matrices AD_pA^{-1} define a minor class in general distinct from the given class.

Two minor classes whose class matrices are connected by a relation

$$D_p' = AD_pA^{-1}, \quad |A| = \pm 1 \qquad (p = 1,2, \cdots, n)$$

will be called *similar* minor classes. We now define the (left) *class number h* of the set $\mathfrak{S}$ of integral numbers of $\mathfrak{A}$ as the (cardinal) number of dissimilar non-singular minor classes of (left) ideal matrices.

It is evident from Theorem 6 that when $\mathfrak{A}$ is an algebraic field, h becomes the ordinary class number of the field. All ideal matrices corresponding to principal ideals belong to minor classes which are similar to the principal minor class. We have therefore, without using the concept of ideal multiplication, succeeded in generalizing to sets $\mathfrak{S}$ of semi-simple algebras the concept of ideal class in a satisfactory manner. For instance, we may prove in the usual manner

THEOREM 12.5. *A necessary and sufficient condition in order that every pair of numbers of $\mathfrak{S}$ may possess a greatest common right divisor expressible linearly in terms of the numbers is that the left class number h of $\mathfrak{S}$ be* 1.

13. **The density of ideal matrices.** It is recognized that the addition of Dedekind ideals cannot be defined in any useful way, because of the fact that associated numbers correspond to the same principal ideal. This is not true of ideal matrices, however, and we have a satisfactory additive theory within each minor class.

Let $B_1, B_2, \cdots, B_n$ be a set of basal matrices for a non-singular minor class $\mathfrak{k}$. Every ideal matrix of $\mathfrak{k}$ has the form

$$G = a_1B_1 + a_2B_2 + \cdots + a_nB_n$$

where the a's are rational integers, and conversely every such G is in $\mathfrak{k}$. Since the B_i are linearly independent, this representation is unique. Addition and scalar multiplication within the minor class $\mathfrak{k}$ are defined as in the theory of linear algebras, and follow the usual laws.

We have seen that $S_1, S_2, \cdots, S_n$ constitute a basis for the principal minor class (§11). The numbers

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

are in one-to-one correspondence with the principal ideal matrices

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

which in turn are in one-to-one correspondence with the ideal matrices G of each class $\mathfrak{k}$, and this correspondence is preserved under addition and scalar multiplication. Thus we have

THEOREM 13. *The ideal matrices of every non-singular minor class $\mathfrak{k}$ are in one-to-one correspondence with the numbers of the set $\mathfrak{S}$. This correspondence is preserved under addition and scalar multiplication.*

OHIO STATE UNIVERSITY,
COLUMBUS, OHIO