IDEALS IN LINEAR ALGEBRAS*

BY C. C. MACDUFFEE

1. *Introduction.* In an algebraic field, and indeed in every commutative domain of integrity, the problem of the greatest common divisor and the problem of unique factorization into primes are equivalent. That is, the property that every pair of numbers in the domain of integrity have a greatest common divisor unique up to a unit factor implies the property that factorization be unique save for unit factors and order of multiplication. In those commutative domains of integrity in which these properties do not hold, the introduction of Dedekind ideals gives an extended system in which they do hold.

In a domain of integrity of a non-commutative algebra, the existence of the greatest common right divisor and of the greatest common left divisor does not insure unique factorization. The two problems have diverged and it seems very improbable to the writer that the same type of ideal system will handle both problems.

The Dedekind ideal is by its very definition connected with the problem of the greatest common divisor. This theory, including the theory of the class number, seems to extend practically intact to the non-commutative case. From this standpoint the theory of ideals in linear algebras is successful.

Several writers have attempted to apply Dedekind ideals to the problems of unique factorization, and in every case the result has been of dubious value. The difficulty has always been in finding an adequate definition for ideal multiplication. In every case so many important properties of ideals have failed to generalize that the theory is practically without substance. It would seem that the enlargement of the domain to permit unique factorization will have to be accomplished through other agencies than the Dedekind ideal.

2. *Domains of Integrity.* The elements of a rational algebra $\mathfrak{A}$ of order n are given by

---

$$a_1\epsilon_1 + a_2\epsilon_2 + \cdots + a_n\epsilon_n,$$

where the basis numbers ϵ_1, ϵ_2, $\cdots$, ϵ_n are linearly independent with respect to the rational field $\mathfrak{R}$ and the a's range over $\mathfrak{R}$. The algebra is closed under multiplication, so that there exist numbers c_{ijk} of $\mathfrak{R}$, called the constants of multiplication, such that

$$\epsilon_i\epsilon_j = \sum_{k=1}^{n} c_{ijk}\epsilon_k, \qquad (i, j = 1, 2, \cdots, n).$$

We assume that multiplication is associative but not that it is commutative. We further assume that $\mathfrak{A}$ contains a principal unit or modulus.

It is evident that if $\epsilon_i = \theta^{i-1}$, where θ is a root of an irreducible equation of degree n, $\mathfrak{A}$ is an algebraic field. Thus the rational algebra is a natural extension of the algebraic field.

While the term *algebraic integer* is well defined, *integral number* of a rational algebra is not. The concept of *domain of integrity* is capable of generalization, however. An algebra $\mathfrak{A}$ may possess several such domains of integrity.

The most satisfactory definition for domain of integrity has been given by Dickson* by means of the five postulates:

R: For every element of the set, the coefficients of the rank equation are rational integers.

C: The set is closed under addition, subtraction and multiplication.

U: The set contains the modulus 1.

M: The set is maximal.

O: The set is of order n.

It is proved that if $\mathfrak{A}$ is not semi-simple,[2] it can be written as a sum of a semi-simple algebra and a nilpotent algebra, and that the arithmetic of $\mathfrak{A}$ is associated with that of the semi-simple component.[1] We shall therefore devote attention only to semi-simple algebras.

For a domain of integrity $\mathfrak{D}$ of a semi-simple rational algebra $\mathfrak{A}$, it is always possible to choose a basis ϵ_1, ϵ_2, $\cdots$, ϵ_n so that $\epsilon_1 = 1$, every number of $\mathfrak{D}$ is given by

---

* See the bibliography on p. 853; the reference here is to No. 1 of that list. Hereafter, references will be by a small numeral corresponding to the number in the list.

$$a_1\epsilon_1 + a_2\epsilon_2 + \cdots + a_n\epsilon_n,$$

where the a's are now rational integers, and such that the constants of multiplication c_{ijk} are likewise rational integers.

The general number satisfies an equation of minimum degree called the *rank equation*. The constant term of this equation is called the *norm* of the number. Numbers of norm 0 are called *divisors of zero*, those of norm ± 1 are called *units*. The norm of the product is equal to the product of the norms of the factors. Those numbers, neither divisors of zero nor units, which can be represented as a product of two numbers neither of which is a unit are called *composite*, and in the contrary case *prime*. Every composite number can be represented as a product of a finite number of primes, but not always uniquely.

Due to the failure of the commutative law, the concept of greatest common divisor must be replaced by the concepts of *greatest common right divisor* (g.c.r.d.) and *greatest common left divisor* (g.c.l.d.). We shall say that δ is a g.c.r.d. of α and β if there are numbers λ, μ of $\mathfrak{D}$ such that

$$(1) \qquad\qquad \alpha = \lambda\delta, \quad \beta = \mu\delta,$$

and if also there are numbers ρ, σ of $\mathfrak{D}$ such that

$$(2) \qquad\qquad \delta = \rho\alpha + \sigma\beta.$$

It is immediately evident that every c.r.d. of α and β divides δ. A similar definition holds for g.c.l.d. Of course two numbers α and β do not have to possess either a g.c.r.d. or a g.c.l.d.

3. *Ideals.* As a criterion for evaluating the various modifications of the Dedekind ideal theory which have been put forward in connection with the problem of unique factorization, we take the definition given by Dickson.[3] This demands of an ideal system merely the following properties:

(i) Each integer (not a divisor of zero) and its associates shall correspond to the same unique ideal.

(ii) There shall be a subset of principal ideals which shall be isomorphic with the numbers of $\mathfrak{D}$.

(iii) The ideal corresponding to the units shall be the identity element of multiplication and shall have no factor different from itself.

It will be interesting to see how far the ideal systems which have been advanced come from meeting these conditions.

Dedekind ideals, modified to fit non-commutative domains, may be defined as follows: A *left ideal** is an infinite set of numbers of $\mathfrak{D}$ which is closed under addition and subtraction, and closed under multiplication on the left by the numbers of $\mathfrak{D}$. If not every number of the ideal is a divisor of zero, the ideal is called *non-singular*.

The set of numbers

$$\xi_1\alpha_1 + \xi_2\alpha_2 + \cdots + \xi_k\alpha_k,$$

where the $\alpha_1, \cdots, \alpha_k$ are fixed and the $\xi_1, \cdots, \xi_k$ variable numbers of $\mathfrak{D}$, obviously constitutes a left ideal $(\alpha_1, \cdots, \alpha_k]$. In fact, there are no others. If $k=1$, the ideal is principal, written $\mathfrak{a}=(\alpha]$.

That Dedekind ideals are fundamentally connected with the problem of the g.c.d. is evident from the fact that *a necessary and sufficient condition that α and β have a g.c.r.d. is that the left ideal $(\alpha, \beta]$ be principal*. For if $(\alpha, \beta]$ is principal, there exists a number δ such that the sets

$$\xi\delta, \quad \eta\alpha + \zeta\beta, \qquad (\xi, \eta, \zeta \text{ variable}),$$

are equal. Thus in particular for $\eta=1$, $\zeta=0$ there is a number ξ_1 such that $\alpha=\xi_1\delta$, and for $\eta=0$, $\zeta=1$ there is a number ξ_2 such that $\beta=\xi_2\delta$. Furthermore, for $\xi=1$ there are numbers η_1, ζ_1 such that $\delta=\eta_1\alpha+\zeta_1\beta$. Thus δ is a g.c.r.d. of α and β. The converse is evident, for by (2) every number $\xi\delta$ is a linear combination of α and β, and by (1) every linear combination of α and β is a multiple of δ.

It is easily proved that every ideal has a basis $\omega_1, \omega_2, \cdots, \omega_n$ such that the numbers of the ideal are given by the linear combinations of these basis numbers with rational integral coefficients. An ideal is *non-singular* if any one of the following properties holds:

(a) The numbers $\omega_1, \omega_2, \cdots, \omega_n$ are linearly independent.

(b) The ideal contains rational integers.

(c) Not every element is a divisor of zero.

(d) The norm $|g_{rs}|$ is not zero, where $\omega_i=\sum g_{ij}\epsilon_j$.

---

* Probably it would have been more logical to have reversed the definitions of left and right ideals as was done by Hurwitz[4] for quaternions, for the essential property of $(\alpha]$ is not that it is closed under multiplication on the left, but that α is a right divisor of every number in it.

4. *The Early Literature.* In first introducing ideals Kummer was interested only in establishing the unique factorization law in certain algebraic fields. The existence of the g.c.d. *together with the commutative law* implies unique factorization. Without the commutative law it does not, as was shown by Hurwitz[4] in what seems to be the earliest use of ideals in a non-commutative algebra. Unique factorization does not hold for all integral quaternions, yet every quaternion ideal is principal, and every pair of integral quaternions has a g.c.r.d. and a g.c.l.d. unique up to unit factors.

From this example it is evident that too much is not to be expected from the ideal theory in the non-commutative case. In the generalization from algebraic fields to rational algebras, the problem of the greatest common divisor and the problem of unique factorization follow divergent paths, and the Dedekind ideal theory is fundamentally connected with the former problem.

Beginning about 1906, L. G. du Pasquier[5] wrote a series of papers investigating domains of integrity in rational algebras. He did not use Wedderburn's theory of linear algebras, however, and his work consisted principally of investigations of particular algebras. He recognized the advisability of working in maximal domains of integrity, and knew that maximal domains according to his definition of domain do not exist in all algebras. We now know that his difficulties were encountered with algebras which were not semi-simple. His conjecture that the ideal theory is helpless to introduce unique factorization into domains which are not maximal was definitely proved by Dickson.[3]

Probably the most important of the algebras considered in detail by du Pasquier[6] is the complete matric algebra over the rational field. He called a matrix *integral* if all its elements were rational integers. He developed a euclidean algorithm for such matrices and proved that a set of integral matrices $M_1, M_2, \cdots, M_k$, not all singular, possess a g.c.r.d. unique up to a left factor A which is integral and of determinant ± 1. Conversely, if D is a g.c.r.d., so is AD for every unimodular integral matrix A. Similar results hold for the g.c.l.d.

Du Pasquier defined right and left ideals for this algebra and showed that in virtue of the existence of the euclidean algo-

rithm every ideal not composed exclusively of divisors of zero is principal. He also discussed two-sided ideals and found that they are never singular.

5. *Speiser's Theory.* The first paper dealing exclusively with ideals in domains of linear algebras was written by Andreas Speiser[7] in 1926. The first part of the paper is devoted to ideals in commutative domains, that is, rings. In a maximal domain of integrity the ideal product is defined in the usual way as the totality of sums of products consisting of a number of the first ideal by a number of the second. Unique factorization into prime ideals holds. For the commutative case Speiser's results are interesting and very satisfactory.

For non-commutative domains of integrity, however, Speiser does not seem to have been so successful. A one-sided ideal, defined in the usual way, is determined by its residue classes, which in turn are represented by matrices with elements in a Galois field. The intersection of two ideals is called their least common multiple (l.c.m.). The ideal formed by adding every number of the first to every number of the second is called their g.c.d. If the g.c.d. of two ideals is the unit ideal, they are relatively prime, and their product is defined to be their l.c.m. Thus multiplication of prime ideals is commutative in a non-commutative domain of integrity. Dickson's second requirement (ii) for an ideal is violated.

If the norm of a right ideal $[\mathfrak{b}]$ is $p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$, then $[\mathfrak{b}]$ can be written as $[q_1][q_2] \cdots [q_l]$, where the factors are prime in pairs (so that their product is defined as above) and each is a divisor of a power of a two-sided prime ideal which divides the norm. The factors are commutative and define $[\mathfrak{b}]$ uniquely.

The factorization of each $[q]$ is treated somewhat after the manner of the series of composition of a finite group. Suppose that $[q]$ is an ideal divisor of p^a, where p is a natural prime. By adjoining p to $[q]$ there results an ideal divisor $[\mathfrak{P}_1]$ of p. The quotient of $[q]$ by $[\mathfrak{P}_1]$ is obtained by taking those residue classes in $[q]$ which are divisible by p and dividing them by p. This new ideal is called $[q_1]$. Now adjoin p to $[q_1]$ and obtain $[\mathfrak{P}_2]$ which is similarly a divisor of $[\mathfrak{P}_1]$. This process ends in a steps, and then by definition

$$[q] = [\mathfrak{P}_1][\mathfrak{P}_2] \cdots [\mathfrak{P}_a].$$

Each factor is a divisor of the same two-sided prime ideal, and each divides the preceding. The factors are uniquely determined, but *the product is not in general uniquely determined by the factors*. Ideal multiplication is not uniquely defined.

Speiser regrets that a number of the most interesting concepts of algebraic number theory do not carry over. He mentions in particular the failure of the theorem that the ideal product can be defined through the products of the basis numbers. He also remarks upon the lack of a definition of ideal class, and the consequent vacuousness of the theorem that the class number is finite. He admits the belief that these concepts and theorems are essentially restricted to the algebraic number theory.

6. *Krull's Theory.* In a recent paper *Zur Theorie der zwei-seitigen Ideale in nichtkommutativen Bereichen*,[8] the ideal theory is treated from a postulational point of view. The essential difficulty of a definition of ideal product is avoided by laying down a set of postulates which ideal multiplication is to obey.

This paper of Krull seems to touch only slightly upon ideals in rational algebras, so we shall not discuss it in detail. The concept of *halbkommutativ* is introduced for those domains in which every pair of prime ideals are commutative. The two-sided ideals are not isomorphic with the integral numbers, and the result which he emphasizes is that the ideals are not as a rule either commutative or *halbkommutativ*.

7. *Present Status of the Unique Factorization Problem.* This year Miss Grace Shover[9] in collaboration with the writer advanced a theory of ideal multiplication using integral matrices. Ideal multiplication is defined through the product of its basis numbers, but as Speiser noted, this definition is not as fruitful as one could wish. The norm of the product is not always equal to the product of the norms, and consequently Dickson's second requirement is not always complied with.

The conclusion seems to be that all attempts up to the present to apply Dedekind ideals to the problem of unique factorization in a non-commutative domain of integrity have been wrecked because of the lack of a satisfactory definition of ideal multiplication. Perhaps one is justified in hazarding the opinion that the theory will not extend.

8. *The Matric Theory.* In 1929 the writer[10] attempted to see

how far the ideal theory would extend without the use of ideal multiplication. It was surprising that so much of the ideal theory as regards the greatest common divisor carried over intact. The right and left class numbers were satisfactorily defined, and Miss Shover[11] has just proved them finite and equal. A necessary and sufficient condition that every pair of numbers of $\mathfrak{D}$ possess a g.c.r.d. unique up to a unit left factor is that the class number of $\mathfrak{D}$ be 1. In this case they also possess a g.c.l.d. unique up to a unit right factor. Moreover, a method for finding these greatest common divisors will be developed in §9.

The use of integral matrices in the theory of ideals in an algebraic field was not entirely new, but it had not been thoroughly exploited. Of course a correspondence between ideals and quadratic forms was known to Dedekind. Poincaré[12] used the matrix (g_{rs}) to represent the ideal with basis $\omega_i = \sum g_{ij}\epsilon_j$ but he did nothing with the matrix except to consider it as an aggregate of n^2 numbers.

Another result of Poincaré[13] was of more significance. He showed essentially that every associative algebra is isomorphic with a matric algebra, and it is but a step to see that when the basis numbers of the algebra form a basis for the domain of integrity $\mathfrak{D}$, the elements of every matrix corresponding to an integral number are rational integers, and conversely. Whether Poincaré knew that this correspondence could be extended to ideals is problematical.[14] His statements on this point have justly been termed "obscure."*

A correspondence between ideals and integral matrices different from that of Poincaré was set up by A. Chatelet.[15] Let an algebraic number θ satisfy an irreducible equation whose roots are $\lambda_1, \lambda_2, \cdots, \lambda_n$. Denote the diagonal matrix $(\delta_{rs}\lambda_s)$ by $[\lambda_i]$. There exists a matrix $T = A[\lambda_i]A^{-1}$ with rational integral elements if and only if the first column of A apart from a constant factor constitutes a basis for an ideal, the other columns of A being the conjugates of the first. By keeping A fixed and letting θ vary over the numbers of $\mathfrak{D}$, matrices corresponding to all numbers of the ideal are obtained. If A corresponds to the unit ideal, the corresponding T's represent the numbers of

---

* National Research Council, *Bulletin on Algebraic Numbers*, I, p. 26, footnote 4.

$\mathfrak{D}(\theta)$, and the representation is an isomorphism with respect to addition and multiplication.

Let D be a g.c.d. of the matrices representing the n numbers whose ideal g.c.d. we seek. Then DA has as its first column this base. Chatelet calls D an ideal factor. In a brief account in the Comptes Rendus[16] he states that "to the divisibility of ideals corresponds naturally the divisibility of ideal factors." Upon consulting a book[17] published by him in the following year it appears that his investigations had not been carried as far as one might be inclined to suppose from a reading of the former article. He does, however, give a method for calculating the product of two ideals.

9. *The Problem of the Greatest Common Divisor.* Since matrices are in general non-commutative, the matric theory seemed a natural tool to apply to ideals in non-commutative domains of integrity. Suppose we have a domain of the type described in §2 with basis $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$. To the number

$$\xi = x_1\epsilon_1 + x_2\epsilon_2 + \cdots + x_n\epsilon_n,$$

we make correspond its first matrix

$$R(\xi) = \left(\sum x_i c_{isr} \right).$$

The first matrices give a matric representation of the algebra. So do the second matrices

$$S(\xi) = \left(\sum x_i c_{ris} \right).$$

This is the correspondence of Poincaré.[13]

Let $\mathfrak{j}$ be a left ideal with basis $\omega_1, \omega_2, \cdots, \omega_n$, where

$$\omega_i = \sum g_{ij}\epsilon_j.$$

The matrix $G = (g_{rs})$ is said to *correspond* to the ideal. The matrices AG, where A is integral and unimodular, give all matrices corresponding to the same ideal.

The fundamental theorem[10] is that a necessary and sufficient condition that a matrix G correspond to an ideal is that there exist n integral matrices $D_1, D_2, \cdots, D_n$ such that

$$(3) \qquad\qquad GR_i^{\mathrm{T}} = D_iG, \qquad\qquad (i = 1, 2, \cdots, n),$$

where R_i^{T} denotes the transpose of $R(\epsilon_i)$. Thus if G is non-

singular it transforms the transposed first matrix of every num-
ber of $\mathfrak{D}$ into an integral matrix.

It so happens that under this definition of correspondence
the second matrix $S(\xi)$ corresponds to the principal left ideal
$(\xi]$. Then (3) becomes

$$S(\xi)R^{\mathsf{T}}(\eta) = R^{\mathsf{T}}(\eta)S(\xi),$$

that is, the second matrices of every given number ξ are com-
mutative with the transposed first matrices of every number
η of $\mathfrak{D}$. The converse is also true, namely, that every integral
matrix commutative with every $R^{\mathsf{T}}(\eta)$ is the second matrix of
some number of $\mathfrak{D}$.

The concept of equivalence of ideals is introduced in a manner
analogous to that in algebraic number theory. If $\omega_1, \omega_2, \cdots, \omega_n$
constitute a basis for an ideal $\mathfrak{f}$, and if s is a number of $\mathfrak{D}$, then
$\omega_1 s, \omega_2 s, \cdots, \omega_n s$ is a basis for an ideal which we denote by $\mathfrak{f}s$.
This is essentially a definition of scalar multiplication for ideals.
If $\mathfrak{f}_1$ and $\mathfrak{f}_2$ are two non-singular ideals, they are called *equiva-
lent* if there exist numbers s_1 and s_2 of $\mathfrak{D}$ such that $\mathfrak{f}_1 s_1 = \mathfrak{f}_2 s_2$. It
is shown that if G_1 corresponds to $\mathfrak{f}_1$ and G_2 to $\mathfrak{f}_2$, a necessary
and sufficient condition that $\mathfrak{f}_1$ and $\mathfrak{f}_2$ be equivalent is that the
matrices D_{1i}, D_{2i} defined by

$$G_1 R_i^{\mathsf{T}} = D_{1i} G_1, \quad G_2 R_i^{\mathsf{T}} = D_{2i} G_2,$$

be connected by a relation

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

where A is integral and unimodular.

The (left) class number h is defined as the number of non-
equivalent non-singular ideals in $\mathfrak{D}$. A necessary and sufficient
condition that every pair of numbers in $\mathfrak{D}$ possess a g.c.r.d.
unique up to a unit left factor is that this class number be 1.
The left and right class numbers are finite and equal.[11]

One of the interesting by-products of the theory is the proof
that every ideal class possesses a basis composed of n integral
matrices $B_1, B_2, \cdots, B_n$ such that every matrix corresponding
to an ideal of the class is of the form AG, where A is integral
and unimodular and G is of the form

$$h_1 B_1 + h_2 B_2 + \cdots + h_n B_n,$$

where the h's are rational integers. If the class is non-singular, that is, contains at least one non-singular ideal, the B's are linearly independent. Every ideal of the class is given by this form not once but exactly p times, where p is the (cardinal) number of units in $\mathfrak{D}$.

It is also of interest that the matric theory is able to provide for all domains of integrity $\mathfrak{D}$ of semi-simple rational algebras an effective euclidean algorithm, something which has been developed previously for only a few algebraic fields. Let α and β be two numbers of $\mathfrak{D}$ not divisors of zero. Let P be a matric g.c.r.d. of $S(\alpha)$ and $S(\beta)$. Then P corresponds* to a basis of the ideal $(\alpha, \beta]$ composed of the numbers $\xi\alpha + \eta\beta$, and consequently the matrices

$$PR_i^T P^{-1} = T_i, \qquad (i = 1, 2, \cdots, n),$$

are all integral.

Now $(\alpha, \beta]$ is principal if and only if there exists a unimodular integral matrix A such that $AP = S(\delta)$, where δ is a g.c.r.d. of α and β. Since every second matrix is commutative with R_i^T, we can find whether A exists, and determine it if it does exist, from the relations $APR_i^T = R_i^T AP$, which are equivalent to

$$R_i^T A = A T_i, \qquad (i = 1, 2, \cdots, n).$$

By determining A^A (adjoint of A) we determine A. But

(4) $$A^A R_i^T = T_i A^A, \qquad (i = 1, 2, \cdots, n),$$

so the matrices A^A constitute a minor class of ideal matrices.[10] This class has a basis $B_1, B_2, \cdots, B_n$ such that every matrix satisfying (4) is of the form

$$x_1 B_1 + x_2 B_2 + \cdots + x_n B_n.$$

Hence the n^3 equations resulting from (4) are in fact equivalent to but $n(n-1)$ equations in n parameters provided the matrix A^A exists. The condition $A^A = \pm 1$ leads to the generalized Pell equation

$$\left| x_1 B_1 + x_2 B_2 + \cdots + x_n B_n \right| = \pm 1,$$

---

* Proved by the writer for algebraic fields but readily extensible to domains of integrity $\mathfrak{D}$.[18]

the solution of which is the same type of problem as the determination of the units of $\mathfrak{D}$. This was to have been expected, since δ is unique only up to a unit factor. Every determination of A leads to a determination of δ.

Since

$$AP = x_1S_1 + x_2S_2 + \cdots + x_nS_n,$$

the x's are readily found by the method of undetermined coefficients. By the same method we can find the numbers λ, μ of $\mathfrak{D}$ such that $\delta = \lambda\alpha + \mu\beta$.

I hope to convince you of the practicability of this generalized euclidean algorithm in a future paper.

10. *Conclusion*. In some respects the attempts to extend the ideal theory to non-commutative domains of integrity have failed, for the unique factorization problem has not been solved. On the other hand, much light has been thrown on the structure of systems of ideals, and on the relationship between the unique factorization problem and the problem of the greatest common divisor.

Then, too, the attempts to solve this problem have led to the use of new instruments in the ideal theory, and these in turn have led to the discovery of new results in algebraic number theory—the basis of an ideal class, the generalized euclidean algorithm, and direct methods for multiplying ideals[9] and for finding the canonical basis of an ideal.[18] A new connection between integral matrices and ideals, in no way dependent upon the preceding results, is the following theorem of C. G. Latimer.[19] If $p(x) = 0$ is the irreducible equation defining the integral number θ, the class number of $\mathfrak{F}(\theta)$ is the number of dissimilar integral matrices satisfying $p(x) = 0$.

In closing, I rather timidly put forward the suggestion that perhaps the unique factorization problem has been solved for some time and that this fact has not been properly appreciated. We have been so intent on generalizing Dedekind ideals that we have refused to consider other possible solutions. Let us consider the domain of integrity $\mathfrak{D}'$ composed of *all* integral matrices of order n. This domain of integrity contains a subdomain, consisting of the second matrices of the numbers of $\mathfrak{D}$, which is isomorphic with $\mathfrak{D}$ not only under multiplication but under addition as well. All of the units of $\mathfrak{D}$ are contained among

the units of $\mathfrak{D}'$, all the divisors of zero of $\mathfrak{D}$ are contained among the divisors of zero of $\mathfrak{D}'$. The class number of $\mathfrak{D}'$ is 1, and every number of $\mathfrak{D}'$ can be expressed as a product of prime matrices[6] in one and only one way apart from unit factors. Is there any reason for pursuing this problem further?

BIBLIOGRAPHY

1. L. E. Dickson, *Algebras and Their Arithmetics*, Chicago, 1923. *Algebren und ihre Zahlentheorie*, Zürich, 1927.

2. J. H. M. Wedderburn, Proceedings of the London Mathematical Society, (2), vol. 6 (1908), pp. 77–118.

3. L. E. Dickson, Journal de Mathématiques, (9), vol. 2 (1923), pp. 281–326.

4. A. Hurwitz, Göttinger Nachrichten, 1896, pp. 313–340. *Zahlentheorie der Quaternionen*, Berlin, 1919.

5. L. G. du Pasquier, Nouvelles Annales de Mathématiques, (4), vol. 18 (1918), p. 448; Bulletin de la Société Mathématique de France, vol. 48 (1920), p. 109; Comptes Rendus du Congrès International des Mathématiciens, Strasbourg, 1920, pp. 164–175.

6. L. G. du Pasquier, Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich, 1906, p. 90.

7. A. Speiser, Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich, vol. 71 (1926), pp. 8–48.

8. W. Krull, Mathematische Zeitschrift, vol. 28 (1928), pp. 481–503.

9. Grace Shover and C. C. MacDuffee, this Bulletin, vol. 37 (1931), pp. 434–438.

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

11. Grace Shover, dissertation, not yet published.

12. H. Poincaré, Bulletin de la Société Mathématique de France, vol. 13 (1885), pp. 162–194.

12. H. Poincaré, Bulletin de la Société Mathématique de France, vol. 13 (1885), pp. 162–194.

13. H. Poincaré, Comptes Rendus, vol. 99 (1884), p. 740.

14. H. Poincaré, Journal de l'École Polytechnique, vol. 28, Cah. 47 (1880), p. 238; Comptes Rendus, vol. 80 (1879), pp. 344–346.

15. A. Chatelet, Annales de l'École Normale, (3), vol. 28 (1911), pp. 105–202.

16. A. Chatelet, Comptes Rendus, vol. 154 (1912), p. 502.

17 A. Chatelet, *Théorie des Nombres*, Paris, 1913.

18. C. C. MacDuffee, to appear in the Mathematische Annalen, vol. 195 (1931).

19. C. G. Latimer, to appear in the Annals of Mathematics, vol. 32 (1932).

THE OHIO STATE UNIVERSITY