MATRICES WITH ELEMENTS IN A PRINCIPAL IDEAL RING*

BY C. C. MACDUFFEE

1. *Rings.* To attempt to distinguish between algebra and number theory is probably futile, but, speaking approximately, it may be said that algebra (in the narrowest sense of the word) is the study of fields, while number theory is the study of rings. The mathematical system which seems most satisfactory as an abstraction of the system of rational integers is the principal ideal ring. By this I mean that the basic theorems of number theory, such as unique factorization into primes, hold for a principal ideal ring, while the concept of principal ideal ring is sufficiently general to include many other instances besides the rational integers.

A *ring*† is a mathematical system composed of more than one element, an equals relation, and two operations, $+$ and $\times$, subject to the following laws. The elements form an abelian group relative to the operation $+$, the identity element being denoted by 0. The set of elements is closed under the operation $\times$, which is associative. Finally, the operation $\times$ is distributive with respect to the operation $+$.

If $a \neq 0$ and $b \neq 0$ are elements of a ring $\mathfrak{R}$ such that $ab = 0$, then a and b are called *divisors of zero.* A commutative ring without divisors of zero is called a *domain of integrity.*

Let a, b, c be elements of a domain of integrity $\mathfrak{D}$. If $ab = c$, then $a \mid c$ (a divides c), $b \mid c$, and a and b are called *divisors* of c. If $a \mid b$ and $a \mid c$, then a is called a *common divisor* of b and c. If, furthermore, every common divisor of b and c divides a, then a is a *greatest common divisor* (g. c. d.) of b and c.

If there exists a number 1 of $\mathfrak{D}$ such that $1 \cdot a = a \cdot 1 = a$ for every a, this number 1 is called a *principal unit.*‡ A domain of integrity with a principal unit in which every pair of elements

* Symposium lecture delivered at the meeting of the Society in Chicago, April 15, 1933.

† In the interest of uniformity I have used the definitions of van der Waerden, *Moderne Algebra*, Springer, 1930–31.

‡ *Einselement*, van der Waerden.

not both 0 have a greatest common divisor representable linearly in terms of the elements is called a *principal ideal ring.*

In a principal ideal ring $\mathfrak{P}$, an element which divides 1 is called a *unit.* The relation $a = ub$, where u is a unit is reciprocal, and the two numbers a and b so related are called *associates.* A set of numbers of $\mathfrak{P}$ no two of which are associated but such that every number of $\mathfrak{P}$ is associated with one of them will be called a *complete set of non-associates* for $\mathfrak{P}$. Thus the positive integers and 0 constitute a complete set of non-associates in the ring of rational integers.

A field* is an instance of a principal ideal ring, but from the standpoint of number theory it is a trivial instance, since every element except 0 is a unit. The polynomial domain of a field, that is, the set of all polynomials in one indeterminate with coefficients in the field, is a non-trivial instance. The units of this polynomial domain are the elements of the field (0 excluded), and the primes are the irreducible polynomials. Maximal domains of algebraic fields of class number unity are also non-trivial instances.

According to the definition of principal ideal ring, every two numbers a and b of $\mathfrak{P}$ have a g. c. d. d expressible in the form

$$d = pa + qb,$$

where p and q are in $\mathfrak{P}$. The determination of p and q is for most rings a practical problem of considerable difficulty. In the ring of rational integers it is handled by means of the well known Euclid algorithm. For polynomial domains and a very few algebraic rings a Euclid algorithm has been developed.

The term *euclidean ring* has been applied to a principal ideal ring with a Euclid algorithm, and it has been considered that the separation of rings into euclidean and non-euclidean rings was a fundamental separation. Recent developments have tended to question this, and to indicate that the separation into rings of class number unity (principal ideal rings) and those of higher class number is of much more importance. It is true that the well known methods of proof of the fundamental theorems of number theory carry over only to euclidean rings, but the theorems themselves are generally true for principal ideal rings.†

* *Kommutativ Körper*, van der Waerden.

† Van der Waerden, loc. cit., vol. I, §17.

Just what algebraic rings of class number unity have euclidean algorithms is not known. Only five quadratic fields of negative discriminant have an algorithm based on decreasing norms, while ten of positive discriminant are known to have such. Perron* has recently suggested that all quadratic rings of positive discriminant and class number unity may have such an algorithm, but could not prove this. Then, too, the existence of an algorithm based on some other stathm† than the norm is a possibility. Very little is known of algebraic rings of degree higher than the second.

It is thus evident that the whole matter of euclidean rings is in disorder. For practical purposes, a euclidean ring is one for which some person has discovered a Euclid algorithm.

One of the purposes of this paper is to add support to the point of view that the principal ideal ring is the important concept rather than the euclidean ring by giving a unified account of an extension to principal ideal rings of the more important results in the theory of matrices with rational integral elements.

2. *Matric Rings.* Consider a mathematical system $\mathfrak{M}$ whose elements are the arrays

$$A = \begin{Vmatrix} a_{11} & a_{12} \cdots a_{1n} \\ a_{21} & a_{22} \cdots a_{2n} \\ \cdots & \cdots \\ a_{n1} & a_{n2} \cdots a_{nn} \end{Vmatrix} = (a_{rs}),$$

where the a_{ij} belong to a ring $\mathfrak{R}$. Two arrays $A=(a_{rs})$ and $B=(b_{rs})$ are called *equal* if $a_{rs}=b_{rs}$ for every r and s.

The operation of addition $(+)$ is defined by

$$A + B = (a_{rs} + b_{rs}).$$

Evidently the arrays form an abelian group with respect to addition, since the same is true of the elements of the ring $\mathfrak{R}$. The identity for addition, composed entirely of 0's, will be denoted by O.

---

* Mathematische Annalen, vol. 107 (1932), pp. 489–495.

† See J. H. M. Wedderburn, Journal für Mathematik, vol. 167 (1931), pp. 129–141.

The operation of multiplication is defined by

$$AB = \left(\sum_i a_{ri} b_{is} \right).$$

The product is unique, and $OA = AO = O$ for every A.

It is easily seen that multiplication in $\mathfrak{M}$ is associative, and distributive with respect to addition, since the same is true in $\mathfrak{R}$.

Thus the system $\mathfrak{M}$ is a ring, which we may call the *total matric ring of order n over* $\mathfrak{R}$. Each of the arrays composing $\mathfrak{M}$ will be called a *matrix*.

If the ring $\mathfrak{R}'$ has a principal unit 1, the derived matric ring $\mathfrak{M}'$ has the principal unit $I = (\delta_{rs})$, where δ_{rs} is 1 or 0 according as $r = s$ or $r \neq s$. We shall call I the *identity matrix* of $\mathfrak{M}'$.

Further specialization of $\mathfrak{R}'$ to a commutative ring, or to a ring without divisors of zero, does not carry with it the corresponding specialization of $\mathfrak{M}'$.

If $\mathfrak{R}'$ is a ring with a principal unit, the matrices $S(k) = (k\delta_{rs})$ constitute a subring of $\mathfrak{M}'$ which is isomorphic with the numbers k of $\mathfrak{R}'$. The operation of scalar multiplication by which a matrix A of $\mathfrak{M}'$ is multiplied by a number k of $\mathfrak{R}'$ consists in replacing k by $S(k)$ and forming the matric product $S(k)A$.

The matrix $A^{\mathsf{T}} = (a_{sr})$, obtained from $A = (a_{rs})$ by changing rows to columns, is called the *transpose* of A. A matrix S such that $S^{\mathsf{T}} = S$ is called *symmetric*. A matrix Q such that $Q^{\mathsf{T}} = -Q$ is called *skew*.

If A is a matrix of $\mathfrak{M}$, then $2A$ can be represented as a sum of the symmetric matrix $A + A^{\mathsf{T}}$ and the skew matrix $A - A^{\mathsf{T}}$. If 2 is not a divisor of zero in the ring $\mathfrak{R}$, this representation is unique. For if

$$2A = S + Q,$$

where S is symmetric and Q is skew, then

$$2A^{\mathsf{T}} = S - Q,$$

so that

$$2[A + A^{\mathsf{T}} - S] = 0, \quad 2[A - A^{\mathsf{T}} - Q] = 0.$$

3. *Unimodular Matrices.* Let us now consider the total matric ring $\mathfrak{M}$ of matrices with elements in a principal ideal ring $\mathfrak{P}$.

A matrix U of $\mathfrak{M}$ is called *unimodular*, or a *unit matrix*, if there exists a matrix U' such that $UU' = I$.

Denote the determinant of U by $d(U)$. Since $UU' = I$ implies $d(U)d(U') = 1$, $d(U)$ is a unit of $\mathfrak{P}$. Conversely if U is in $\mathfrak{M}$ and $d(U)$ is a unit of $\mathfrak{P}$, then U^{-1} (the inverse of U) is in $\mathfrak{M}$, and serves as the U' of the definition. Hence also $U'U = I$, and U' is a unit.

Similarly a matrix A of $\mathfrak{M}$ is a divisor of zero if and only if $d(A) = 0$.

THEOREM 1. *Let $a_1, a_2, \cdots, a_n$, all numbers of a principal ideal ring $\mathfrak{P}$, have the greatest common divisor d_n. There exists a matrix of determinant d_n having $a_1, a_2, \cdots, a_n$ as its first row.*

This theorem was first given for rational integers, $n = 3$, by G. Eisenstein,* and for any n by C. Hermite.† The following proof (for the case of rational integers) was given by A. Bloch.‡

The theorem is evidently true for $n = 2$, for if $pa_1 + qa_2 = d_2$, then

$$\begin{Vmatrix} a_1 & a_2 \\ -q & p \end{Vmatrix} = d_2.$$

Suppose that it holds for $n-1$, and let D_{n-1} be a matrix which has $a_1, a_2, \cdots, a_{n-1}$ as its first row, and whose determinant is the g. c. d. d_{n-1} of $a_1, a_2, \cdots, a_{n-1}$. Determine p and q so that $pd_{n-1} - qa_n = d_n$. Let

$$D_n = \begin{Vmatrix} & & & a_n \\ & D_{n-1} & & 0 \\ & & & \cdots \\ & & & 0 \\ \frac{a_1 q}{d_{n-1}} & \frac{a_2 q}{d_{n-1}} & \cdots \frac{a_{n-1} q}{d_{n-1}} & p \end{Vmatrix}.$$

Then, expanding according to the elements of the last column,

$$\begin{aligned} d(D_n) &= (-1)^{n-1} a_n \frac{q}{d_{n-1}} (-1)^n d_{n-1} + pd_{n-1} \\ &= pd_{n-1} - qa_n = d_n. \end{aligned}$$

* Journal für Mathematik, vol. 28 (1884), pp. 289–374.

† Journal de Mathématiques, (1), vol. 14 (1849), pp. 21–30.

‡ Bulletin de la Société Mathématique, vol. 50 (1922), pp. 100–110.

Other proofs have been given by K. Weihrauch,* Bianchi,† and H. Hancock.‡

4. *Types of Equality in Matric Theory.* At the very basis of every mathematical system lies the notion of equality. The abstract formulation of this notion may be embodied in the following four postulates.§ The relation $A=B$ is a relation of equality if it is

(1.) *Determinative* (Either $A=B$ or $A\neq B$),
(2.) *Reflexive* ($A=A$),
(3.) *Symmetric* ($A=B$ implies $B=A$),
(4.) *Transitive* (If $A=B$ and $B=C$, then $A=C$).

Such a definition of equality constitutes a separation of the elements into classes.

The richness of the matric theory is due in large part to the number of non-isomorphic types of equality which can be defined, each having associated with it an interesting and fairly extensive theory. A few examples follow.

(1.) Let $\mathfrak{R}'$ be a ring with a principal unit. If there exists a unimodular matrix U such that $A=UB$, then A is a *left associate* of B, written $A\overset{\mathsf{L}}{=}B$.

(2.) If A is a *right associate* of B, then $A\overset{\mathsf{R}}{=}B$.

(3.) If there exist two unimodular matrices U and V such that $A=UBV$, then $A\overset{\mathsf{E}}{=}B$. ($A$ is *equivalent* to B.)

(4.) If there exists a unimodular matrix U such that $A=U^{\mathsf{T}}BU$, then $A\overset{\mathsf{C}}{=}B$. ($A$ is *congruent* with B.)

(5.) If there exists a unimodular matrix U such that $A=U^{\mathsf{I}}BU$, then $A\overset{\mathsf{S}}{=}B$. ($A$ is *similar* to B.)

(6.) If there exists an orthogonal matrix U ($U^{\mathsf{I}}=U^{\mathsf{T}}$) such that $A=U^{\mathsf{T}}BU$, then $A\overset{\mathsf{O}}{=}B$. ($A$ is *orthogonally congruent* with B.)

All of these relationships obey the four postulates stated above, and are therefore in an abstract sense relations of equality. These examples by no means exhaust the possibilities.

* Zeitschrift für Mathematik und Physik, vol. 21 (1876), pp. 134–137.

† *Lezioni sulla Teoria dei Numeri Algebrici*, pp. 1–7.

‡ American Mathematical Monthly, vol. 31 (1924), pp. 161–162.

§ See O. Ore, this Bulletin, vol. 37 (1931), p. 538. Van der Waerden (vol. I, p. 14) would call this relation *equivalence*, and say that the class C_a containing a is *equal* to the class C_b containing b if and only if a is equivalent to b. It seems to the writer that Ore has carried this idea to its logical conclusion.

An interesting example of slightly more complicated nature was given by A. Loewy.* If the elements of A, B, and P are functions of x, and P^{D} is the matrix obtained from P by replacing each element by its derivative, and if

$$A = -P^{D}P^{I} + PBP^{I},$$

then A is *similar to B in the sense of Loewy.*

5. *Associated Matrices.* The following *elementary operations* upon the rows of a matrix can be accomplished by multiplying the given matrix on the left by an *elementary matrix*, namely the unimodular matrix obtained by performing the desired elementary operation upon the identity matrix I.

(1.) The interchange of two rows.

(2.) The multiplication of the elements of a row by a unit u of $\mathfrak{P}$.

(3.) The addition to the elements of a row of k times the corresponding elements of another row, k being in $\mathfrak{P}$.

Every elementary matrix is unimodular, and its inverse is an elementary matrix of the same type. The theory of elementary matrices is due to L. Kronecker.†

If $\mathfrak{P}$ has a euclidean algorithm, every unimodular matrix is a product of elementary matrices. This appears to be not so in other rings.‡

If $UA = B$, then for every k

$$\sum u_{ij}a_{jk} = b_{ik},$$

so that every g. c. d. of the elements of the kth column of A is a common divisor of the elements of the kth column of B. If U is unimodular, the relation of A to B is reciprocal. Hence the g. c. d. of the elements of every column is invariant under transformations of this type.

These n invariants do not form a complete system, however, as the next theorem shows.

THEOREM 2. *Every matrix A with elements in $\mathfrak{P}$ is the left associate of a matrix having* 0*'s above the main diagonal, each di-*

* Mathematische Annalen, vol. 78 (1918), pp. 1–51.

† Berliner Akademie, Monatsberichte, 1866, pp. 597–612.

‡ See van der Waerden, loc. cit., vol. II, p. 122.

agonal element lying in a prescribed system of non-associates, and each element below the main diagonal lying in a prescribed residue system modulo the diagonal element above it. If, furthermore, any diagonal element is 0, *all the elements of its row can be made* 0. *This form is unique.*

This theorem was stated for a non-singular matrix with rational integral elements by C. Hermite.*

To avoid being tiresome, I shall prove this merely for a special case. It is fairly evident that the procedure is general. Let

$$A = \begin{Vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{Vmatrix}.$$

Unless every element of the last column is zero, they have a g. c. d.

$$d_3 = b_1a_{13} + b_2a_{23} + b_3a_{33}$$

lying in any prescribed system of non-associates. By Theorem 1 there is a unimodular matrix U having b_1, b_2, b_3 as its last row. Then UA has d_3 in the (3, 3)-position, and every other element of the last column is a linear combination of a_{13}, a_{23}, a_{33}, and hence a multiple of d_3. By subtracting a proper multiple of the last row from each of the other rows, a matrix is obtained whose last column consists entirely of 0's above the main diagonal. Similarly, if we work now only with the second order minor in the upper left corner, a_{12} can be made 0.

In case every element of the last column of A is 0, the procedure must be slightly modified. Let

$$d_2 = b_1a_{12} + b_2a_{22} + b_3a_{32}$$

be the desired g. c. d. of the elements of the second column. Let U be unimodular with b_1, b_2, b_3 as its second row. Then UA still has all zeros in the third column, while d_2 is in the (2, 2)-position, and d_2 divides every other element of the second column. Thus A is the left associate of

---

* Journal für Mathematik, vol. 41 (1851), pp. 191–216.

$$\begin{Vmatrix} a_{11} & 0 & 0 \\ a_{21} & d_2 & 0 \\ a_{31} & 0 & 0 \end{Vmatrix}.$$

Let $d_1 = b_1 a_{11} + b_3 a_{31}$ be a g. c. d. of a_{11} and a_{31}. Take U unimodular so that

$$U = \begin{Vmatrix} b_1 & 0 & b_3 \\ 0 & 1 & 0 \\ u_{31} & 0 & u_{33} \end{Vmatrix}.$$

Then UA has d_1 in the (1, 1)-position, and d_1 is a divisor of the other elements of the first column, while the last two columns are intact. Thus A is the left associate of

$$\begin{Vmatrix} d_1 & 0 & 0 \\ a_{21} & d_2 & 0 \\ 0 & 0 & 0 \end{Vmatrix}.$$

Let us prove the uniqueness of this form for the example

$$A = \begin{Vmatrix} a_{11} & 0 & 0 \\ 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} \end{Vmatrix}, \quad a_{11} a_{33} \neq 0.$$

Suppose

$$\begin{Vmatrix} l_{11} & l_{12} & l_{13} \\ l_{21} & l_{22} & l_{23} \\ l_{31} & l_{32} & l_{33} \end{Vmatrix} \cdot \begin{Vmatrix} a_{11} & 0 & 0 \\ 0 & 0 & 0 \\ a_{31} & a_{32} & a_{33} \end{Vmatrix} = \begin{Vmatrix} b_{11} & 0 & 0 \\ b_{21} & b_{22} & 0 \\ b_{31} & b_{32} & b_{33} \end{Vmatrix},$$

where $b_{ii} = 0$ implies $b_{ki} = 0$, $k = 1, 2, 3$ and (l_{rs}) is unimodular. Suppose that b_{ii} belongs to the same system of non-associates as a_{ii}, and that if $b_{ii} = a_{ii}$, then b_{ki} belongs to the same residue system modulo a_{ii} that a_{ki} does.

Since $l_{13} a_{33} = b_{13} = 0$ and $l_{23} a_{33} = b_{23} = 0$, and $a_{33} \neq 0$, then $l_{13} = l_{23} = 0$. Since (l_{rs}) is unimodular, l_{33} is a unit. Since a_{33} and $l_{33}\ a_{33} = b_{33}$ belong to the same system of non-associates, $l_{33} = 1$ and $b_{33} = a_{33}$.

Now $b_{22} = 0$, since $l_{23} = 0$. Hence $b_{21} = 0$ also, from the definition of canonical form. Hence $l_{21} a_{11} = b_{21} = 0$, $l_{21} = 0$. Then l_{11} and l_{22}

are units of $\mathfrak{P}$. But a_{11} and $l_{11}a_{11}=b_{11}$ are in the same system of non-associates, so $l_{11}=1$ and $b_{11}=a_{11}$. Since

$$l_{31}a_{11} + a_{31} = b_{31},$$

and a_{31} and b_{31} lie in the same residue system modulo $a_{11}=b_{11}$, it follows that $l_{31}=0$. Hence

$$(l_{rs}) = \begin{Vmatrix} 1 & l_{12} & 0 \\ 0 & u & 0 \\ 0 & l_{31} & 1 \end{Vmatrix}.$$

This matrix leaves A unaltered when used as a left factor.

6. *Greatest Common Divisors.* If A, C, and D are matrices with elements in a principal ideal ring such that $A=CD$, then D is called a *right divisor* of A, and A is a *left multiple* of D. A *greatest common right divisor* (g. c. r. d.) D of two matrices A and B is a common right divisor which is a left multiple of every common right divisor of A and B. A *least common left multiple* (l. c. l. m.) of two matrices A and B is a common left multiple which is a right divisor of every common left multiple of A and B.

THEOREM 3. *Every pair of matrices A and B with elements in a principal ideal ring have a g. c. r. d. D expressible in the form*

$$D = PA + QB.$$

This theorem was first given for matrices A and B not both singular and with rational integral elements by du Pasquier* by means of a generalized Euclid algorithm. Computation by this method is laborious. The presentation here given is not only simple and independent of the Euclid algorithm (and hence extensible to principal ideal rings) but computation by means of it is easy and rapid. It is due in essence to E. Cahen,† and in the form here presented (for rational integers) to A. Chatelet.‡

By Theorem 2 there exists a unimodular matrix U such that

$$U \begin{Vmatrix} A & O \\ B & O \end{Vmatrix} = \begin{Vmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{Vmatrix} \begin{Vmatrix} A & O \\ B & Q \end{Vmatrix} = \begin{Vmatrix} D & O \\ O & O \end{Vmatrix}.$$

* Naturforschende Gesellschaft zu Zürich, vol. 51 (1906), pp. 55–129.

† *Théorie des Nombres*, vol. I, 1914.

‡ *Groupes Abéliens Finis*, 1924,

Thus $U_{11}A + U_{12}B = D$, so that every common right divisor of A and B is a right divisor of D. Since U is unimodular, $U^{-1} = V$ has elements in $\mathfrak{P}$, and

$$V \begin{Vmatrix} D & O \\ O & O \end{Vmatrix} = \begin{Vmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{Vmatrix} \begin{Vmatrix} D & O \\ O & O \end{Vmatrix} = \begin{Vmatrix} A & O \\ B & O \end{Vmatrix}.$$

Thus $A = V_{11}D$, $B = V_{21}D$, and D is a common right divisor of A and B.

If in the $2n \times n$ array $\binom{A}{B}$ is of rank n, the matrices A and B have a non-singular g. c. r. d. D. In this case every g. c. r. d. of A and B is a left associate of D. For if $D = PD_1$ and $D_1 = QD$, $D = PQD$. If $d(D) \neq 0$, then $I = PQ$, whence P and Q are unimodular.

The above algorithm also furnishes a least common left multiple of A and B if both are non-singular. Evidently

$$U_{21}A + U_{22}B = O.$$

Let us define M by the formula

$$M = U_{21}A = -U_{22}B.$$

That is, M is a common left multiple of A and B. If M_1 is another c. l. m., their g. c. r. d. $M_2 = PM + QM_1$ is a c. l. m. such that $M = HM_2$. Suppose $M_2 = KA = LB$. Then

$$U_{21}A = HKA, \quad -U_{22}B = HLB,$$

and since A and B are non-singular,

$$U_{21} = HK, \quad U_{22} = -HL.$$

But

$$I = U_{21}V_{12} + U_{22}V_{22} = H[HV_{12} - LV_{22}],$$

so H is unimodular, and M is a right divisor of M_1.

7. *Equivalence.* Two matrices A and B with elements in a principal ideal ring $\mathfrak{P}$ are *equivalent* if there exist two unimodular matrices U and V with elements in $\mathfrak{P}$ such that $A = UBV$.

With some modification of proofs, the theory of invariant factors and elementary divisors in an ordinary polynomial ring goes over intact to a principal ideal ring. First of all, we may note that each greatest common divisor d_i of the i-rowed minor

determinants of A is associated with every greatest common divisor d_i' of the i-rowed minor determinants of B. This follows from the fact that if $A = UBV$, every i-rowed minor of A can be written as a linear combination of the i-rowed minors of B, and if U and V are unimodular, the relation is reciprocal.

THEOREM 4. *Every matrix A of rank ρ with elements in $\mathfrak{P}$ is equivalent to a diagonal matrix $h_1, h_2, \cdots, h_\rho, 0, \cdots, 0$ where $h_i \neq 0$ and $h_i \mid h_{i+1}$.*

This theorem was given for rational integers by H. J. S. Smith.*

Since the Euclid algorithm is no longer available, Theorem 1 must be used as a substitute. After shifting rows and columns so that the minor of order ρ in the upper left corner is not 0, the element in the (1, 1)-position can be made $\neq 0$ and a g. c. d. of the elements of the first column, as was shown in the proof of Theorem 2. As in the usual reduction, the element in the (1, 1)-position either divides every remaining element of the first row, or it can be replaced by a proper divisor of itself—that is, replaced by a number having fewer prime factors. Since a number of $\mathfrak{P}$ neither 0 nor a unit has but a finite number of prime factors, this process can be repeated until a_{11} divides every other element of the first row and first column.† Now, as usual, A can be reduced by a repetition of this process to a diagonal form $[g_1, g_2, \cdots, g_\rho, 0, \cdots, 0]$.

By adding column 2, column 3, $\cdots$, column ρ to column 1, the matrix is made to assume the form

$$\begin{Vmatrix} g_1 & 0 & 0 \cdots 0 \\ g_2 & g_2 & 0 \cdots 0 \\ g_3 & 0 & g_3 \cdots 0 \\ \cdots & \cdots & \cdots \end{Vmatrix}.$$

As in the proof of Theorem 2, there is a unimodular matrix U which, used as a left factor, replaces g_1 by the g. c. d. h_1 of $g_1, g_2, \cdots, g_\rho$. Every element of the new matrix UA is a homo-

* Philosophical Transactions of the Royal Society of London, vol. 151 (1861–62), p. 314.

† Van der Waerden, loc. cit., vol. II, p. 124.

geneous linear combination of $g_1, g_2, \cdots, g_\rho$, so every element is divisible by h_1. Reduce every element of the first row and column except the element h_1 in the (1, 1)-position to 0. Continue the entire process with the $(n-1)$-rowed minor in the lower right corner to obtain an h_2 in the (2, 2)-position which divides $h_3, \cdots, h_\rho$. Finally we obtain the normal form.

Let $H=[h_1, \cdots, h_\rho, 0, \cdots, 0]$ be the normal form of A. The g. c. d. d_i of the i-rowed minors of A is associated with the g. c. d. d_i' of the i-rowed minors of H. Since $h_i \mid h_{i+1}$, it follows that $d_i = h_1 h_2 \cdots h_i$ divides $d_{i+1} = h_1 h_2 \cdots h_i h_{i+1}$, the quotient being h_{i+1}. Hence these quotients are invariants (up to a unit factor in $\mathfrak{P}$), so that the normal form of A is unique when we require that the h's shall lie in a specified system of non-associates.

In a principal ideal ring every element neither 0 nor a unit can be factored uniquely (except for unit factors) into a product of powers of primes.* Suppose

$$h_i = p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_k^{e_{ik}}.$$

Since $h_i \mid h_{i+1}$, the exponents of each prime factor form a sequence

$$e_{nl} \geqq e_{n-1,l} \geqq \cdots \geqq e_{1l} \quad (l = 1, 2, \cdots, k).$$

Such of these powers $P^{e_{il}}$ as are not units are called the *elementary divisors* of A. They are defined up to unit factors.

This treatment unifies the elementary divisor theory of matrices with rational integral elements and that of the so-called λ-*matrices*, that is, matrices with elements in the polynomial domain of a field. Every polynomial domain (with one indeterminate) of a field is a principal ideal ring,† the units being the numbers $\neq 0$ of the field.

The theory of equivalent matrices is an excellent example of the interdependence of algebra and number theory. It seems to the writer that the elementary divisor theory appears simpler and more natural when it is looked upon as being fundamentally a branch of the theory of numbers.

8. *Congruence.* If there exists a unimodular matrix U such

* Van der Waerden, loc. cit., vol. I, p. 65.

† Van der Waerden, loc. cit., vol. I, p. 60.

that $A = U^{T}BU$, all matrices having elements in $\mathfrak{P}$, then A is said to be *congruent* with B.

Symmetric and skew matrices play an important role in the theory of congruence. Each of these properties is preserved under this relation. If $S+Q$ is congruent with S_1+Q_1, where S and S_1 are symmetric and Q and Q_1 are skew, then S is congruent with S_1 and Q with Q_1. Hence if $2A = S+Q$, the congruence invariants of S and Q are congruence invariants of A, and together they form a complete system for A except for rings in which 2 is a divisor of zero.

It is well known that the problem of the congruence of symmetric matrices is a problem of extreme difficulty. It is essentially the problem of the equivalence of quadratic forms in the theory of numbers. How refractory this problem is may be seen by glancing through Professor Dickson's recent book.*

It is perhaps less well known that the corresponding problem for skew matrices is capable of complete and simple solution not only for matrices with rational integral elements, but for matrices with elements in a principal ideal ring. It seems perverseness on the part of nature that an important problem should appear to be insoluble, while a similar problem of no evident importance should behave so well. Perhaps the ultimate explanation will consist in showing that the skew matrix is really important.† At present it is sufficient for the pure mathematician that the theory is elegant.

I wish at this point to call attention to a very useful notation due to A. Hurwitz.‡ If A and B are matrices, and O is a block of zeros, then

$$\left\| \begin{matrix} A & O \\ O & B \end{matrix} \right\|$$

is called the *direct sum* of A and B, and is written $A+B$.

THEOREM 5. *Every skew matrix Q is of even rank $\rho = 2\mu$, and is congruent with a matrix*

---

* L. E. Dickson, *Studies in the Theory of Numbers*, University of Chicago Press, 1930.

† Professor Albert has called my attention to the fact that skew matrices are of prime importance in the theory of pure Riemann matrices.

‡ H. Kries, *Contribution à la Théorie des Systèmes Linéaires*, Zurich, 1906.

$$H = \left\| \begin{matrix} 0 & h_1 \\ -h_1 & 0 \end{matrix} \right\| \dot{+} \left\| \begin{matrix} 0 & h_2 \\ -h_2 & 0 \end{matrix} \right\| \dot{+} \cdots \dot{+} \left\| \begin{matrix} 0 & h_\mu \\ -h_\mu & 0 \end{matrix} \right\| \dot{+} \left\| \begin{matrix} 0 & 0 \\ 0 & 0 \end{matrix} \right\| \dot{+} \cdots,$$

where $h_i \mid h_{i+1}$. *The numbers* $h_1, h_1, h_2, h_2, \cdots, h_\mu, h_\mu$ *of the canonical form* H *are the invariant factors of* Q.

This theorem for the ring of rational integers was given by E. Cahen.*

I shall not give the details of this proof, for it follows the lines of the proofs of Theorems 2 and 4. The 0's in the main diagonal of the skew matrix enable one to work successively on rows and columns. In the case of symmetric matrices the non-zero elements in the main diagonal make a similar reduction impossible.

9. *Moduls.* The set $\mathfrak{L}$ of all numbers of the form

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

where the a's range over a ring $\mathfrak{R}$ and the ϵ's are linearly independent with respect to $\mathfrak{R}$, constitute a *linear form modul.* The ϵ's constitute a *basis* for $\mathfrak{L}$.

If $U = (u_{rs})$ is unimodular with elements in $\mathfrak{R}$, then

$$\epsilon_i' = \sum u_{ij}\epsilon_j, \qquad (i = 1, 2, \cdots, n),$$

also constitute a basis for $\mathfrak{L}$, since every linear combination of the ϵ's is a linear combination of the ϵ''s, and vice versa. Conversely, every two bases of a linear form modul are so related by a unimodular transformation.

The theory of moduls over the ring of rational integers was developed along the lines which we shall follow by A. Chatelet.† The establishment of Theorems 1, 2, and 3 of this paper shows that Chatelet's results are true for every principal ideal ring.

---

* *Théorie des Nombres*, vol. I, 1914, p. 282.

† Annales de l'École Normale, (3), vol. 28 (1911), pp. 105–202; Comptes Rendus, vol. 154 (1912), p. 502; *Leçons sur la Thèorie des Nombres*, 1913; *Groupes Abêliens Finis*, 1924.

Let $\mathfrak{L}_1$ be a linear form sub-modul* of order n of $\mathfrak{L}$, and let $\mathfrak{L}_1$ have the basis $\lambda_1, \lambda_2, \cdots, \lambda_n$. Then

$$\lambda_i = \sum g_{ij}\epsilon_j, \qquad (i = 1, 2, \cdots, n),$$

where $G_1 = (g_{rs})$ is a non-singular matrix with elements in $\mathfrak{R}$. We may say that G_1 is *associated* with the basis $\lambda_1, \lambda_2, \cdots, \lambda_n$ of $\mathfrak{L}_1$. Every non-singular matrix G_1 determines in this way a basis of some linear form sub-modul of order n of $\mathfrak{L}$.

If $\mathfrak{L}_2$, with basis $\mu_1, \mu_2, \cdots, \mu_n$, is a linear form sub-modul of order n of $\mathfrak{L}_1$, every number of $\mathfrak{L}_2$ is in $\mathfrak{L}_1$, and in particular

$$\mu_i = \sum c_{ij}\lambda_j = \sum c_{ij}g_{jk}\epsilon_k, \quad (i = 1, 2, \cdots, n).$$

The matrix G_2 associated with the basis $\mu_1, \mu_2, \cdots, \mu_n$ of $\mathfrak{L}_2$ is CG_1, where C is a non-singular matrix with elements in $\mathfrak{R}$. Thus $\mathfrak{L}_1$ contains $\mathfrak{L}_2$ if and only if G_1 is a right divisor of G_2.

In particular, two moduls $\mathfrak{L}_1$ and $\mathfrak{L}_2$ are equal if and only if G_1 and G_2 are left associates. A unique canonical basis for $\mathfrak{L}_1$ may be determined in accordance with Theorem 1.

Now suppose that $\mathfrak{R}$ is a principal ideal ring $\mathfrak{P}$. The set of numbers common to two moduls $\mathfrak{L}_1$ and $\mathfrak{L}_2$ constitute a modul $\mathfrak{L}_d$ called the *greatest common sub-modul* of $\mathfrak{L}_1$ and $\mathfrak{L}_2$. It may also be defined as that common sub-modul of $\mathfrak{L}_1$ and $\mathfrak{L}_2$ which contains every common sub-modul of $\mathfrak{L}_1$ and $\mathfrak{L}_2$. If G_1, G_2, and G_d are matrices associated with $\mathfrak{L}_1$, $\mathfrak{L}_2$, and $\mathfrak{L}_d$ respectively, then G_d is a right divisor of G_1 and G_2, and every common right divisor of G_1 and G_2 is a right divisor of G_d. That is, G_d is a g. c. r. d. of G_1 and G_2. Now G_d is unique up to a unimodular left factor—the same latitude of definition as the g. c. r. d. of two matrices.

In a similar manner all numbers contained in either $\mathfrak{L}_1$, or $\mathfrak{L}_2$, together with their sums and differences, constitute a modul $\mathfrak{L}_m$ called the *least common super-modul* of $\mathfrak{L}_1$ and $\mathfrak{L}_2$. It may also be defined as that modul containing $\mathfrak{L}_1$ and $\mathfrak{L}_2$ which is contained in every modul containing $\mathfrak{L}_1$ and $\mathfrak{L}_2$. If G_m is a matrix associated with $\mathfrak{L}_m$, it is clear from this last definition that G_m is a l. c. l. m. of G_1 and G_2.

10. *Ideals.* Let $\mathfrak{S}$ be a linear form modul, with coefficients in a principal ideal ring $\mathfrak{P}$, which is also a ring, and whose elements

* If $\mathfrak{R}$ is a principal ideal ring, every sub-modul of $\mathfrak{L}$ is a linear form modul. Van der Waerden, loc. cit., vol. II, p. 121.

are commutative with those of $\mathfrak{P}^*$. If $\mathfrak{S}$ has the basis $\epsilon_1, \epsilon_2, \cdots, \epsilon_n$, then

$$\epsilon_i\epsilon_j = \sum_k c_{ijk}\epsilon_k,$$

where the constants of multiplication c_{ijk} are in $\mathfrak{P}$. Define the matrices

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

Then both of the matric rings

$$R(\xi) = x_1R_1 + x_2R_2 + \cdots + x_nR_n,$$
$$S(\xi) = x_1S_1 + x_2S_2 + \cdots + x_nS_n$$

are isomorphic under both addition and multiplication with the numbers

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

of $\mathfrak{S}$. Unless $\mathfrak{S}$ is of very special form† the R_i are linearly independent, and the S_i are also. Thus we have two representations of $\mathfrak{S}$ as a matric ring.

A sub-modul of $\mathfrak{S}$ which is closed under multiplication on the left by numbers of $\mathfrak{S}$ is called a *left ideal*.‡ Similarly *right ideals* and *two-sided ideals* may be defined.

It is known that every ideal has a *minimal basis* $\lambda_1, \lambda_2, \cdots, \lambda_n$ such that every number of the ideal is given by the form

$$h_1\lambda_1 + h_2\lambda_2 + \cdots + h_n\lambda_n,$$

where the h's are in $\mathfrak{P}$; and if the ideal does not consist exclusively of divisors of zero, the representation is unique, that is, the λ's are linearly independent with respect to $\mathfrak{P}$.§

If $\lambda_1, \lambda_2, \cdots, \lambda_n$ form a minimal basis for a left ideal $\mathfrak{J}$, where

$$\lambda_i = \sum g_{ij}\epsilon_j,$$

every number κ of $\mathfrak{J}$ is of the form

---

* An instance of such a system is a domain of integrity of a linear associative algebra in the sense of Dickson. *Algebren und ihre Zahlentheorie*, 1927, p. 154.

† This Bulletin, vol. 35 (1929), pp. 344–349.

‡ Van der Waerden, loc. cit., vol. I, p. 53.

§ Transactions of this Society, vol. 31 (1929), p. 74.

$$\kappa = k_i\lambda_i = \sum k_i g_{ij}\epsilon_j,$$

while every number σ of $\mathfrak{S}$ is of the form

$$\sigma = \sum s_l\epsilon_l.$$

Since $\sigma\kappa$ is in $\mathfrak{J}$ for all values of s_l and k_i, there exist numbers d_r of $\mathfrak{P}$ such that

$$\sigma\kappa = \sum s_l k_i g_{ij}c_{ljh}\epsilon_h = \sum d_r g_{rt}\epsilon_t.$$

Hence

$$\sum s_l k_i g_{ij}c_{ljh} = \sum d_r g_{rh}.$$

In particular, when $s_l = \delta_{lp}$ and $k_i = \delta_{iq}$, there exist values d_{pqr} of d_r. For these values

$$\sum g_{qj}c_{pjh} = \sum d_{pqr}g_{rh},$$

or

$$GR_p^{\mathsf{T}} = D_pG, \quad D_p = (d_{prs}), \quad (p = 1, 2, \cdots, n). \tag{1}$$

That is, if the modul with which G is associated is a left ideal, matrices $D_1, D_2, \cdots, D_n$ with elements in $\mathfrak{P}$ exist satisfying the above condition.

The existence of the D's in (1) is a sufficient as well as a necessary condition that G be associated with an ideal. Let d_{pqr} and g_{qj} be numbers of $\mathfrak{P}$ satisfying the above conditions. If we write, by definition,

$$\lambda_i = \sum g_{ij}\epsilon_j,$$

the modul*

$$k_1\lambda_1 + k_2\lambda_2 + \cdots + k_n\lambda_n$$

is closed under multiplication on the left by every number σ of $\mathfrak{S}$. For

$$\sigma\kappa = \sum s_l k_i g_{ij}c_{ljr}\epsilon_r = \sum s_l k_i d_{lis}\lambda_s$$

is again in the modul.

If $\mathfrak{J}_1$ and $\mathfrak{J}_2$ are two left ideals of $\mathfrak{S}$ with bases $\lambda_1, \lambda_2, \cdots, \lambda_n$ and $\mu_1, \mu_2, \cdots, \mu_n$, respectively, the set of numbers

* Transactions of this Society, vol. 31 (1929), pp. 71–90.

$$\sum d_{ij}\lambda_i\mu_j,$$

where the d's range over $\mathfrak{P}$, is a linear form modul $\mathfrak{L}$. Since $\mathfrak{J}_1$ is closed under multiplication on the left by the numbers of $\mathfrak{S}$, the same is true of $\mathfrak{L}$. Hence $\mathfrak{L}$ is an ideal. Since it generalizes the concept of ideal product in algebraic number theory, it is called the *product* of the ideals $\mathfrak{J}_1$ and $\mathfrak{J}_2$ in that order.*

If $\mathfrak{J}_1\mathfrak{J}_2 = \mathfrak{K}$, the latter with basis $\nu_1, \nu_2, \cdots, \nu_n$, set

$$\lambda_i = \sum l_{ij}\epsilon_j, \quad \mu_i = \sum m_{ij}\epsilon_j, \quad \nu_i = \sum p_{ij}\epsilon_j.$$

Then there exist numbers h_{ijk} of $\mathfrak{P}$ such that

$$\lambda_i\mu_j = \sum h_{ijk}\nu_k.$$

That is,

$$\sum_{k,r,t} l_{ik}m_{jr}c_{krt}\epsilon_t = \sum_{k,t} h_{ijk}p_{kt}\epsilon_t,$$

or

$$\sum_{k,r} l_{ik}m_{jr}c_{krt} = \sum_{k} h_{ijk}p_{kt},$$

which can be written in either of the forms

$$G_1S(\mu_j) = H_{1j}G_3, \quad H_{1j} = (h_{rjs}),$$
$$G_2R^{\mathsf{T}}(\lambda_i) = H_{2i}G_3, \quad H_{2i} = (h_{irs}),$$

where G_1 is associated with $\mathfrak{J}_1$, G_2 with $\mathfrak{J}_2$, and G_3 with their product $\mathfrak{K}$. Similarly it may be shown that

$$G_3 = \sum_h K_{1h}G_1S(\mu_h) = \sum_j K_{2j}G_2R^{\mathsf{T}}(\lambda_j),$$

where K_{1h} and K_{2j} are matrices with elements in $\mathfrak{P}$. Thus G_3 may be readily determined as the g. c. r. d. of $G_1S(\mu_1)$, $G_1S(\mu_2)$, $\cdots$, $G_1S(\mu_n)$ or (if preferred) as the g. c. r. d. of $G_2R^{\mathsf{T}}(\lambda_1)$, $G_2R^{\mathsf{T}}(\lambda_2)$, $\cdots$, $G_2R^{\mathsf{T}}(\lambda_n)$.†

11. *Determination of a Minimal Basis.* If $\alpha_1, \alpha_2, \cdots, \alpha_k$ are numbers of $\mathfrak{S}$, the set of numbers

---

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

† The problem of finding the minimal basis of the product of two quadratic ideals whose minimal bases are given was discussed by W. B. Carver, American Mathematical Monthly, vol. 18 (1911), pp. 81–87, with no simple results.

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

where the ξ's range over $\mathfrak{S}$, satisfies the definition of an ideal $\mathfrak{J}$. As stated before, this ideal is known to have a minimal basis $\lambda_1, \lambda_2, \cdots, \lambda_n$, such that the form

$$h_1\lambda_1 + h_2\lambda_2 + \cdots + h_n\lambda_n,$$

where the h's range over $\mathfrak{S}$, gives all the numbers of $\mathfrak{J}$. The proof of the existence of the minimal basis is existential, hinging upon the ability to select from an infinite set of numbers of $\mathfrak{S}$ one whose norm is minimal.

The effective determination of the minimal basis has been considered a problem of considerable difficulty. In 1917 M. Cipolla* gave a complete solution of this problem for quadratic fields, but even in this simple case both method and results are complicated.

The method of integral matrices affords a simple and easily stated solution of this problem in its general form.† Let $S(\alpha_i)$ be the second matrix of α_i, and let B be a matrix associated with the minimal basis $\lambda_1, \lambda_2, \cdots, \lambda_n$ to be found. The matrix B is a g. c. r. d. of $S(\alpha_1), S(\alpha_2), \cdots, S(\alpha_k)$.

Since $\mathfrak{J}$ is an ideal, it contains

$$\epsilon_r\alpha_i = \sum c_{rij}\beta_j, \quad (r, j = 1, \cdots, n;\ i = 1, \cdots, k).$$

That is, if $\alpha_i = \Sigma a_{ij}\epsilon_j$, $\beta_i = \Sigma b_{ij}\epsilon_j$,

$$\sum_{h,s} a_{ih}c_{rhs}\epsilon_s = \sum_{j,s} q_{rij}b_{js}\epsilon_s,$$

$$\sum_h a_{ih}c_{rhs} = \sum_j q_{rij}b_{js}, \quad (r, s, j = 1, \cdots, n;\ i = 1, \cdots, k).$$

In matric notation this is

$$S(\alpha_i) = Q_iB, \quad Q_i = (q_{ris}), \quad (i = 1, \cdots, k).$$

Hence B is a common right divisor of the matrices $S(\alpha_i)$.

Since every β_i is in $\mathfrak{J}$, there exist numbers

$$\pi_{rj} = \sum_h p_{rjh}\epsilon_h, \quad (r, h = 1, \cdots, n;\ j = 1, \cdots, k),$$

of $\mathfrak{S}$ such that

* Atti Accademia Catania, (5), vol. 10 (1917), No. 20.

† Mathematische Annalen, vol. 105 (1931), pp. 663–665.

$$\beta_r = \sum_j \pi_{rj}\alpha_j.$$

That is,

$$\sum_s b_{rs}\epsilon_s = \sum_{j,h,l,s} p_{rjh}a_{jl}c_{hls}\epsilon_s,$$

whence

$$b_{rs} = \sum_{j,h,l} p_{rjh}a_{jl}c_{hls}, \quad (r, s, h, l = 1, \cdots, n; j = 1, \cdots, k).$$

In matric notation this is

$$B = \sum P_j S(\alpha_j), \qquad P_j = (p_{rjs}).$$

Thus B is a g. c. r. d. of the matrices $S(\alpha_i)$.

It thus appears that a problem which is of great complexity when approached by the methods of elementary number theory and congruences can be given a very simple and natural treatment when the greatest common divisor theory of integral matrices is applied. Furthermore, in the case of algebraic fields at least, a constructive proof replaces an existential proof of the existence of a minimal basis of an ideal.

THE OHIO STATE UNIVERSITY