Non-commutative domains of integrity.

By *J. H. M. Wedderburn* in Princeton.

1. Introduction. The present paper forms an introduction to the study of the general properties of domains of integrity. Much old matter has had to be included in order to render the remainder intelligible. In particular § 7 was originally published in 1913[1]) but is given here in a much improved form with some extensions and additions. The first theorem of § 10 has been given by Dickson[2]) but in a somewhat less general form.

2. Definitions. A *domain of integrity* D is a set of elements $a, b, \ldots$ called integers in connection with which there are defined two functions $a + b$, ab which have a unique value in D for every pair of elements a, b in D and which satisfy the following postulates:

A1. $(a + b) + c = a + (b + c)$.

A2. There exists a unique integer 0 such that $a + 0 = a$ for every integer a.

A3. If a is an integer, there exists an integer c such that $a + c = 0$. (This c is denoted by $-a$.)

A4. $a + b = b + a$.

M1. $ab \cdot c = a \cdot bc$.

M2. There exists a unique integer 1 such that $a1 = a = 1a$ for every integer a.

M3. $ab = 0$ implies either $a = 0$ or $b = 0$.

AM. $a(b + c) = ab + ac$, $(b + c)\, a = ba + ca$.

The postulates are, as is well known, not wholly independent and contain parts which can be deduced as theorems from simpler postulates.

The domain D contains $2 = 1 + 1$, $3 = 2 + 1, \ldots$ also -2, -3, $\ldots$; and these integers form a subdomain of integrity D_1 in D. If for some integer m of the sequence $2, 3, \ldots$ we have $m + 1 = 0$, the domain is said to be modular; it is readily shown that, if m is the first of the sequence for which this is true, then $m + 1$ is a prime when regarded as a rational integer. The elements of D_1 are commutative with every element of D; moreover, the total set of elements of D which are commutative with every element of D themselves form a domain of integrity and the elements of this domain we shall call the *scalars* of D.

If $a = bc$, b is called a left factor (L. F.) of a and c a right factor (R. F.); we shall here denote these relations by bLa and cRa respectively, while if x is not a right factor of a, we write $x \widetilde{R} a$, and similarly $x \widetilde{L} a$ will mean that x is not a left factor of a.

If there exists an integer b such that $ab = 1$, then b is called the *inverse* of a; and an integer which has an inverse in D is called a *unit*. If a is an integer and u, v are units

[1]) J. H. M. Wedderburn, On continued fractions in non-commutative quantities, Ann. of Math. (2) **15** (1913—14), pp. 101—105.

[2]) L. E. Dickson, Algebras and their arithmetics, Chicago 1923, p. 173; Algebren und ihre Zahlentheorie, Zürich 1927, p. 226.

in D, all integers of the form uav are called *associates* of a; ua is called a *left associate* and av a *right associate.* An integer which is not a unit and which has no factors except itself, or an associate, and units, is said to be *irreducible* in D, that is, if a is irreducible and $a = bc$, then either b or c must be a unit.

If to a pair of integers a, b there corresponds an integer c such that (I) c is a common right factor (C. R. F.) of a and b, (II) every C. R. F. of a and b is a R. F. of c, then c, or any of its left associates, is called a highest common right factor (H. C. R. F.) of a and b; a H. C. L. F. is similarly defined. Again, if there exists an integer m such that (I) aRm, bRm, (II) if p is any integer for which aRp, bRp, then mRp, then m is called a least common right multiple (L. C. L. M.) of a and b; a L. C. R. M. is similarly defined.

3. Vectors and matrices. Vectors and matrices with non-commutative coordinates have been used by several authors but it is convenient here to give a short description of them since they are used freely in the sequel. A vector of order n in a domain of integrity D is a set of n ordered integers of the domain, say $x = (x_1, x_2, \ldots, x_n)$. If $y_i = \sum_j a_{ij} x_j$ (a_{ij} in D) the vector y is a laevolateral linear vector form in x and we write $y = Ax$; similarly, if $y_i = \sum_j x_j a_{ji}$, we set $y = xA$. Just as in ordinary scalar algebra we call $A = \| a_{ij} \|$ a matrix and addition and multiplication of A and $B = \| b_{ij} \|$ are defined by

$$A + B = \| a_{ij} + b_{ij} \|, \quad AB = \| \sum_k a_{ik} b_{kj} \|.$$

4. Elementary Transformations. If the relation between y and x is given by

(1) $$y = Ax; \quad y_i = x_i \ (i \neq p), \quad y_p = x_p + \theta x_q \ (q \neq p),$$

y is said to be derived from x by a left-hand elementary transformation of type I; or if

(2) $$z = xA; \quad z_i = x_i \ (i \neq q), \quad z_q = x_q + x_p \, \theta \ (q \neq p),$$

z is derived from x by a right-hand elementary transformation of type I. Again, if

(3) $$y = Px; \quad y_{\alpha i} = x_i,$$

where $\alpha_1, \alpha_2, \ldots, \alpha_n$ is a permutation of $1, 2, \ldots, n$, then y is said to be derived from x by a left-hand elementary transformation of type II. The corresponding right-hand transformation is

(4) $$z = xP; \quad z_{\alpha i} = x_i.$$

Finally, if $y_i = u_i x_i$ ($y_i = x_i u_i$), where each u_i is a unit, y is derived from x by a left-(right-)hand elementary transformation of type III; the corresponding matrix is $U = \| u_i \delta_{ij} \|$.

The matrices A, P, U are called elementary matrices of type I, II, and III, respectively, and any matrix which is the product of a finite number of such matrices is called an *elementary matrix* in D.

5. Examples of domains of integrity. In order to illustrate the terms introduced in the next section we shall give here a number of examples which will later be quoted by number.

Example 1. The set I of rational integers. The units are ± 1.

Example 2. The set $I(\frac{1}{2})$ of all rational numbers of the form $x 2^n$, where x is in I and $n = 0, -1, -2, \ldots$ This set is obtained by adjoining $\frac{1}{2}$ to I; the set of units is the set of numbers of the form 2^m, where m is in I.

Example 3. The set R of all rational numbers; here every element, except 0, is a unit.

Example 4. The set $I(\sqrt{k})$ of all numbers of the form $a + b\sqrt{k}$, where k is a fixed element of I and a, b arbitrary elements of I.

Example 5. The set $K(\sqrt{k})$ of quadratic integers, that is, the set of numbers of the form $x = a + b\sqrt{k}$, where k is a fixed element of I which has no square factor and a, b are elements of R such that x satisfies an equation $x^2 + \alpha x + \beta = 0$ (α, β in I). Unless $k \equiv 1 \bmod 4$, this domain is the same as $I(\sqrt{k})$.

Example 6. The set $Q = I(i, j, k)$ of quaternions $a_0 + a_1 i + a_2 j + a_3 k$ with coordinates in I.

Example 7. The set $Q(\frac{1}{2}(1 + i + j + k))$ of all quaternions of the form

$$a_1 i + a_2 j + a_3 k + a_4 \frac{1 + i + j + k}{2}, \qquad a_1, a_2, a_3, a_4 \text{ in } I.$$

Example 8. If F is a field, the set $F(x)$ of all polynomials in the variable x with coefficients in F is a domain of integrity.

Example 9. If D is any domain of integrity and $x_1, x_2, \ldots, x_n$ are scalar variables, the set $D(x_1, x_2, \ldots, x_n)$ of polynomials in the x's with coefficients in D forms a domain of integrity.

Example 10. Consider the set of all functions a_p of a variable t which possess derivatives of all orders in a given region and let D here stand for $\frac{d}{dt}$; the set of all operators of the form

$$a_0 D^n + a_1 D^{n-1} + \cdots + a_n, \qquad n = 0, 1, 2, \ldots$$

forms a domain of integrity. This domain contains a subdomain obtained by restricting the a's to be polynomials in t, which gives a purely algebraic domain since D may be defined by means of the relations

$$Da = aD + a', \; D(a_1 + a_2) = Da_1 + Da_2, \; Da_1 a_2 = a_1 Da_2 + a_1' a_2,$$

where a' is the derivative of a.

Example 11. In place of D in example 10 we may use the difference operators $\triangle$ or E for which

$$Ea(t) = a(t + 1), \; \triangle = E - 1.$$

Many other operators may be used in the same way; for instance, we may use the operator which turns t^n into t^{n-1}, the coefficients being taken to be polynomials in order to avoid non-algebraic considerations.

6. Euclidean domains. Domains of integrity in which the division transformation is possible have many important properties in common. The definition of the transformation varies somewhat in different domains, and some care is necessary in order to cover all cases in one discussion.

In Example 1 of the preceding section we know that, if p, q are any integers, we can determine (in general in two ways) integers a, b such that

$$p = aq + b, \tag{5}$$

with the condition $|b| < |q|$. In Example 2 a similar relation exists, only we must replace, if $b \neq 0$, the absolute value $|b|$ by $\sigma(b)$ where, if $b = 2^n\beta$, $\beta \not\equiv 0 \bmod 2$, then $\sigma(b) = \beta$. In Examples 4, 5 the division transformation is not always possible but in in certain cases, which we need not discuss here, the transformation exists with the

condition that, if $\sigma(z)$ stands for the absolute value of the norm of z, then in (5) we have $\sigma(b) < \sigma(q)$ or else $b = 0$. The transformation is also possible in Example 7.

In Examples 8, 10, 11 the property of the remainder b is usually stated in terms of the degree of the polynomial, but, if z is a polynomial of degree n (in x, D, or E, respectively), the characteristic property of the remainder can be brought into line with the earlier examples by putting $\sigma(z) = 2^n$. We are therefore led to formulate the existence of the division transformation in a domain as in the following postulate:

E 1. *To every non-zero integer a there exists a real positive number $\sigma(a)$, called the stathm of a, such that* (I) *any sequence of integers $a_1, a_2, \ldots$ for which $\sigma(a_1) > \sigma(a_2) > \ldots$ can contain only a finite number of members,* (II) *to any pair of integers p, q, neither of which is* 0, *there exist integers a, b, r, s such that*

$$p = aq + r = qb + s,$$

where either $r = 0$ or $\sigma(r) < \sigma(q)$ and either $s = 0$ or $\sigma(s) < \sigma(q)$.

A domain of integrity in which this postulate is satisfied will be called a *Euclidean domain.*

It follows from E 1 that $\sigma(a)$ has a minimum value for elements of the domain. If we denote this value temporarily by α, then any element b for which $\sigma(b) = \alpha$ is a unit; for the remainder on dividing any integer by b must be 0 since there is no element whose stathm is less than α. We may always set $\alpha = 1$ without real loss of generality and, except when otherwise stated we shall always suppose that this has been done. We have then the following theorem:

Theorem 6. 1. *In a Euclidean domain, if a, b are integers such that $\sigma(ab) = 1$, then both a and b are units.*

In all the examples quoted above it happens that

$$\sigma(ab) = \sigma(a)\,\sigma(b). \tag{6}$$

Any Euclidean domain in which (6) holds will be called a *proper* Euclidean domain. We have then

Theorem 6. 2. *In a proper Euclidean domain the stathm of a unit is* 1; *and every integer whose stathm is* 1 *is a unit.*

Suppose for the moment that the minimum stathm α is not necessarily 1. Since $\sigma(a) = \sigma(1a) = \sigma(1)\sigma(a)$, we have $\sigma(1) = 1$. Suppose that u is a unit for which $\sigma(u) = \alpha$. We have $\alpha \leqq 1$ since $\sigma(u^{-1}) = \alpha^{-1}$; but, if $\alpha < 1$, then $\sigma(u^2) = \alpha^2 < \alpha$, which is impossible since α is the minimum value of a stathm; hence $\alpha = 1$. Again, if u is any unit and $uv = 1$, then $1 = \sigma(1) = \sigma(uv) = \sigma(u)\sigma(v)$ whence $\sigma(u) = \sigma(v) = 1$ since neither can be less than 1. The second part of the theorem then follows as in Theorem 6. 1.

7. The Euclidean algorism. Let ξ_0, ξ_1 be a pair of integers in any domain of integrity and $a_1, a_2, \ldots$ any sequence in the same domain; we can then define another sequence $\xi_0, \xi_1, \xi_2, \ldots$ by the recurrence formula

$$\xi_{r-1} = a_r \xi_r + \xi_{r+1}. \tag{7}$$

If we set

$$x_r = (\xi_r, \xi_{r+1}) = (\xi_r, \xi_{r-1} - a_r \xi_r), \tag{8}$$

we have

$$x_r = A_r^{-1} x_{r-1}, \tag{9}$$

where

$$A_r^{-1} = \begin{Vmatrix} 0 & 1 \\ 1 & -a_r \end{Vmatrix}$$

which is an elementary matrix whose inverse is

$$A_r = \begin{Vmatrix} a_r & 1 \\ 1 & 0 \end{Vmatrix}. \tag{10}$$

From (9) we have $x_{r-1} = A_r x_r$, repeated use of which gives

$$x_0 = P_r x_r, \tag{11}$$

where

$$P_r = A_1 A_2 \cdots A_r = P_{r-1} A_r. \tag{12}$$

It follows readily that P_r has the form

$$P_r = \begin{Vmatrix} p_r & p_{r-1} \\ q_r & q_{r-1} \end{Vmatrix}, \quad P_1 = A_1, \tag{13}$$

where

$$\begin{aligned} &p_r = p_{r-1} a_r + p_{r-2}, \quad q_r = q_{r-1} a_r + q_{r-2} \\ &p_0 = 1, \quad p_1 = a_1, \quad q_0 = 0, \quad q_1 = 1. \end{aligned} \tag{14}$$

Since P_r is elementary, its inverse is integral. In fact, we have

$$P_r^{-1} = (-1)^r \begin{Vmatrix} q'_{r-1} & -p'_{r-1} \\ -q'_r & p'_r \end{Vmatrix}, \quad P_1^{-1} = \begin{Vmatrix} 0 & 1 \\ 1 & -a_1 \end{Vmatrix} \tag{15}$$

where

$$\begin{aligned} &p'_r = a_r p'_{r-1} + p'_{r-2}, \; q'_r = a_r q'_{r-1} + q'_{r-2} \\ &p'_0 = 1, \; p'_1 = a_1, \; q'_0 = 0, \; q'_1 = 1. \end{aligned} \tag{16}$$

Since $P_r P_r^{-1} = 1 = P_r^{-1} P_r$, we have

Theorem 7. 1.

$$\begin{aligned} 0 &= q'_r p_r - p'_r q_r = p_r p'_{r-1} - p_{r-1} p'_r = q_r q'_{r-1} - q_{r-1} q'_r \\ (-1)^r &= q'_{r-1} p_r - p'_{r-1} q_r = p'_r q_{r-1} - q'_r p_{r-1} \\ &= p_r q'_{r-1} - p_{r-1} q'_r = q_{r-1} p'_r - q_r p'_{r-1}. \end{aligned} \tag{17}$$

Also from $x_0 = P_r x_r$, $x_r = P_r^{-1} x_0$, we have

Theorem 7. 2.

$$\begin{aligned} &\xi_0 = p_r \xi_r + p_{r-1} \xi_{r+1}, \quad \xi_1 = q_r \xi_r + q_{r-1} \xi_{r+1} \\ &q'_{r-1} \xi_0 - p'_{r-1} \xi_1 = (-1)^r \xi_r. \end{aligned} \tag{18}$$

Using the same values of a_r as in (7) we can also define the sequence $\eta_0, \eta_1, \eta_2, \ldots$ where

$$\eta_{r-1} = \eta_r a_r + \eta_{r+1}, \; \eta_0 = \xi_0, \; \eta_1 = \xi_1. \tag{19}$$

If we set $y_r = (\eta_r, \eta_{r+1})$, this gives immediately $y_r = y_{r-1} A_r^{-1}$ whence, as before,

$$y_0 = y_r Q_r, \; Q_r = A_r A_{r-1} \cdots A_1 = A_r Q_{r-1} \tag{20}$$

with [1]) $Q_1 = A_1$. Repeating the processes used above we find that

$$Q_r = \begin{Vmatrix} p'_r & q'_r \\ p'_{r-1} & q'_{r-1} \end{Vmatrix} = (-1)^{r+1} T P_r^{-1} T^{-1}, \tag{21}$$

where

$$T = \begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix},$$

and, remembering that $\eta_0 = \xi_0$, $\eta_1 = \xi_1$, we have

[1]) In a commutative domain Q_r is the transverse of P_r.

Theorem 7.3. $\xi_0 = \eta_r p'_r + \eta_{r+1} p'_{r-1}, \quad \xi_1 = \eta_r q'_r + \eta_{r+1} q'_{r-1}$

$$\xi_0 q_{r-1} - \xi_1 p_{r-1} = (-1)^r \eta_r. \tag{22}$$

Another formal relation whose proof is readily made by induction, is

$$\xi_1 \xi_0 - \xi_0 \xi_1 = (-1)^r (\eta_{r+1} \xi_r - \eta_r \xi_{r+1}). \tag{23}$$

8. Factorization in a Euclidean domain. We now assume that all the quantities used in § 7 lie in a Euclidean domain E, and that after some value r_1 of r the relation (7) is obtained by the division transformation so that at each stage after the r_1-th we have either $\xi_{r+1} = 0$ or $\sigma(\xi_{r+1}) < \sigma(\xi_r)$. The stathms $\sigma(\xi_r)$ $(r > r_1)$ then form a decreasing sequence and hence at some point $\xi_r R \xi_{r-1}$, that is, $\xi_{r+1} = 0$; let n be the first [1]) value of r for which $\xi_{n+1} = 0$. A similar process may be carried out with left-hand division in place of right; but it is probably more convenient to continue the process with the η's defined by (19) using the division transformation after the value $r = n$. As before we must have at some stage $\eta_{r+1} = 0$; let m be the first value of r for which $\eta_{m+1} = 0$.

As a consequence of (7) we have that every C. R. F. of ξ_0 and ξ_1 is also a R. F. of ξ_n, and from Theorem 7. 2 with $r = n$ we have

$$\xi_0 = p_n \xi_n, \quad \xi_1 = q_n \xi_n, \quad q'_{n-1} \xi_0 - p'_{n-1} \xi_1 = (-1)^n \xi_n, \tag{24}$$

so that ξ_n is a R. F. of both ξ_0 and ξ_1; hence ξ_n is a H. C. R. F. of ξ_0 and ξ_1. Similarly, from (19) and Theorem 7. 3 it follows that η_m is a H. C. L. F. and

$$\xi_0 = \eta_m p'_m, \quad \xi_1 = \eta_m q'_m, \quad \xi_0 q_{m-1} - \xi_1 p_{m-1} = (-1)^m \eta_m. \tag{25}$$

We may therefore state the following theorem:

Theorem 8.1. *If p and q are integers in a Euclidean domain, we can find in a finite number of steps a H. C. R. F., r, and a H. C. L. F., l; and there exist integers a, b, c, d such that*

$$ap + bq = r, \quad pc + qd = l.$$

We have also the following corollary:

Corollary. *We can find integers a', b' such that $a'p + b'q = 0$ and such that*

$$\begin{Vmatrix} a & b \\ a' & b' \end{Vmatrix}$$

is an elementary matrix.

For in the theorem we have $a = q'_{n-1}$, $b = -p'_{n-1}$, whence $a' = -q'_n$, $b' = p'_n$ satisfy the required conditions.

When p and q have no C. R. F., then $p = p_n v$, $q = q_n v$, where v is a unit. If we set

$$\gamma_r = p_r v, \quad \delta_r = q_r v, \quad \gamma'_r = v^{-1} p'_r, \quad \delta'_r = v^{-1} q'_r,$$

the results of Theorems 7. 1, 2 still hold good when γ_r, δ_r are substituted for p_r, q_r. The difference equations satisfied by γ_r and γ'_r are

$$\begin{aligned} &\gamma_r = \gamma_{r-1} b_r + \gamma_{r-2}, \quad \gamma'_r = b_r \gamma'_{r-1} + \gamma'_{r-2}, \\ &b_r = v^{-1} a_r v, \quad \gamma_0 = v, \quad \gamma_1 = v b_1, \end{aligned} \tag{27}$$

and similar results hold good for the δ's.

The discussion just given above shows that a H. C. F. may be found by a variety of sequences of elementary transformations; the following theorems show to what extent the results at any stage are invariant. We shall deal directly only with left-hand trans-

[1]) It is permissible that n be less than r_1.

formations leaving the reader to make the necessary alterations in the statement and proof when right-hand transformations are used. We shall also assume as above that $\xi_{n+1} = 0 = \eta_{m+1}$.

Theorem 8.2. *If* $ap_r = bq_r$, $hp_r - kq_r = (-1)^r$, *then*

$$a = sq'_r, \quad b = sp'_r, \quad h = tq'_r + q'_{r-1}, \quad k = tp'_r + p'_{r-1}, \tag{28}$$

where s *and* t *are integers.*

Consider the class X of integers x for which there exists an integer y such that $xp_r = yq_r$. In X there is at least one integer, say f, which is not 0 and whose stathm has the minimum value β for the class; let $fp_r = gq_r$. By the division transformation we may set $q'_r = c_1 f + c_2$ where either $c_2 = 0$ or $\sigma(c_2) < \sigma(f) = \beta$. This gives

$$0 = q'_r p_r - p'_r q_r = c_2 p_r - (p'_r - c_1 g) q_r.$$

Hence c_2 is in X and equals 0 since otherwise $\sigma(c_2) < \beta$; therefore

$$q'_r = c_1 f, \quad p'_r = c_1 g.$$

From Theorem 7. 1 any C. L. F. of q'_r and p'_r is a unit so that, if $u = c_1^{-1}$, we may set $f = uq'_r$, $g = up'_r$. If we now set $a = a_1 f + a_2$, it follows as before that we cannot have $\sigma(a_2) < \sigma(f)$, and hence fRa; whence $q'_r Ra$, say $a = sq'_r$, and this gives $b = sp'_r$.

The second part of the theorem then follows immediately since from $hp_r - kq_r = (-1)^r$ we have (cf. Theorem 7. 1)

$$(h - q'_{r-1}) p_r - (k - p'_{r-1}) q_r = 0.$$

Corollary. *Every L. C. L. M. of* p_r *and* q_r *has the form* $uq'_r p_r$, *where* u *is a unit.*

For if w is a L. C. L. M. of p_r and q_r, then $w = ap_r = bq_r$, and hence by Theorem 8. 2, $w = sq'_r p_r$; that s is a unit follows from the definition of a L. C. L. M.

Theorem 8. 3. *If* p *and* q *are integers in a Euclidean domain, we can find in a finite number of steps a L. C. L. M.,* w_l, *and a L. C. R. M.,* w_r.

For in view of the results of § 7 we may write $p = p_n \xi_n$, $q = q_n \xi_n$. If therefore w_l is a L. C. L. M. we have

$$w_l = ap_n \xi_n = bq_n \xi_n$$

and hence $ap_n = bq_n$ and $w_l = sq'_n p_n \xi_n$, where s is a unit; conversely $q'_n p_n \xi_n$ is a C. L. M. Similarly $w_r = \eta_m q'_m p_m$ is a L. C. R. M.

A corollary of this theorem is of sufficient importance to require separate statement.

Theorem 8. 4. *If* $ap = bq$, *then* q'_n *is a R. F. of* a.

For we may set $p = p_n \xi_n$, $q = q_n \xi_n$ and hence as above $a = sq'_n$.

In many respects this theorem takes the place of the theorems regarding unique factorization which are valid in commutative domains.

Theorem 8. 5. *In a proper Euclidean domain* $\sigma(p_r) = \sigma(p'_r)$, $\sigma(q_r) = \sigma(q'_r)$; *and, if* p_r *is irreducible, so is also* p'_r, *and conversely.*

The first part of the theorem is true for $r = 1$ and, since

$$\sigma(p_r)\, \sigma(p'_{r-1}) = \sigma(p_r p'_{r-1}) = \sigma(p_{r-1} p'_r) = \sigma(p_{r-1})\, \sigma(p'_r),$$

it follows by induction that it is true for all values of r.

To prove the second part suppose that p_r is irreducible and that $p'_r = ab$, where a is irreducible, so that $q'_r p_r = abq_r$. Taking q'_r and a, which have no C. L. F. by Theorem

7. 1, we can find c and d such that

$$q_r' c = ad, \quad \sigma(c) = \sigma(a), \quad \sigma(d) = \sigma(q_r),$$

and from Theorem 8. 2 (with right and left interchanged) it follows that $p_r = cs$, $bq_r = ds$. But p_r is irreducible and $\sigma(c) = \sigma(a)$ so that c is not a unit; hence s is a unit and $\sigma(p_r) = \sigma(c) = \sigma(a)$. This gives $\sigma(b) = 1$ and b is therefore a unit.

Vectors of higher order can be treated in much the same way as those of order 2. If $x = (p_1, p_2, \ldots, p_k)$ is any vector, we can find $q_{11}, q_{12}, r_{11}, r_{12}$ such that

$$0 = q_{11} p_1 + q_{12} p_2, \quad r_1 = r_{11} p_1 + r_{12} p_2, \tag{29}$$

where r_1 is a H. C. R. F. of p_1 and p_2, and q_{11}, q_{12} have no C. R. F. Next, taking r_1 with p_3, we find $q_{21}', q_{23}, r_{21}', r_{23}$ such that, if r_2 is a H. C. R. F. of p_1, p_2, p_3, then using (29)

$$0 = q_{21}' r_1 + q_{23} p_3 = q_{21}' r_{11} p_1 + q_{21}' r_{12} p_2 + q_{23} p_3$$

or, say,

$$0 = q_{21} p_1 + q_{22} p_2 + q_{23} p_3;$$

similarly

$$r_2 = r_{21}' r_1 + r_{23} p_3 = r_{21}' r_{11} p_1 + r_{21}' r_{12} p_2 + r_{23} p_3 = r_{21} p_1 + r_{22} p_2 + r_{23} p_3.$$

Let q be a H. C. L. F. of q_{21}, q_{22}, q_{23}; q_{23} and q_{21}' have no C. L. F. and therefore, if we find q_1', q_2' such that $q_{21}' q_1' = q q_2'$ is a L. C. R. M. of q_{21}' and q, then by Theorem 8. 4 q_1' is a C. L. F. of r_{11} and r_{12} and is therefore a unit. But if u is the inverse of q_1', this gives $q_{21}' = q q_2' u$ and, since q_{21}' and q have no C. L. F., q must be a unit; hence q_{21}, q_{22}, q_{23} have no C. L. F. Similarly r_{21}, r_{22}, r_{23} have no C. L. F. Continuing this process we arrive at the first part of the following theorem; the proof of the second part is similar to that of Theorem 8. 2 and is left to the reader.

Theorem 8. 6. *If r is a H. C. R. F. of a sequence $p_1, p_2, \ldots, p_k$ of integers in a Euclidean domain, we can find integers $q_{ij} (i = 1, 2, \ldots, k-1;\ j = 1, 2, \ldots, i+1)$ and $q_{kj} (j = 1, 2, \ldots, k)$ such that, for a given value of i, $q_{i1}, q_{i2}, \ldots$ have no C. L. F. and*

$$\begin{aligned}
&q_{11} \quad p_1 + q_{12} p_2 && = 0\\
&q_{21} \quad p_1 + q_{22} \quad p_2 + q_{23} p_3 && = 0\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&q_{k-1,1} p_1 + q_{k-1,2} p_2 + \cdots + q_{k-1,k} p_k && = 0\\
&q_{k1} \quad p_1 + q_{k2} \quad p_2 + \cdots + q_{kk} \quad p_k && = r.
\end{aligned}$$

Further, if $\alpha_1, \alpha_2, \ldots, \alpha_i$ are any integers such that

$$\alpha_1 p_1 + \alpha_2 p_2 + \cdots + \alpha_i p_i = 0,$$

then there exist integers $t_i, t_{i-1}, \ldots$ such that

$$\begin{aligned}
\alpha_i &= t_i q_{i-1,i}\\
\alpha_{i-1} &= t_i q_{i-1,i-1} + t_{i-1} q_{i-2,i-1}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
\alpha_1 &= t_i q_{i-1,1} + t_{i-1} q_{i-2,1} + \cdots + t_2 q_{11}.
\end{aligned}$$

The following theorem is also of interest.

Theorem 8. 7. *If $x = (p_1, p_2, \ldots, p_k)$ is any vector and q an integer in a Euclidean domain, there exists a vector $x' = (p_1', p_2', \ldots, p_k')$ and an integer q' such that*

$$q' x = x' q;$$

and, if y and a are any vector and integer in the domain such that $ax = yq$, then there is an integer s such that $a = sq'$, $y = sx'$.

Let q_i' and p_i'' be determined so that a L. C. L. M. of p_i and q is $q_i' p_i = p_i'' q$, and et $q' = q_i'' q_i'$ be a L. C. L. M. of q_i'($i = 1, 2, \ldots, k$). Then $p_i' = q_i'' p_i''$($i = 1, 2, \ldots, k$) satisfies the first condition of the theorem; the proof that it also satisfies the second condition is similar to that already given for Theorem 8. 2.

9. Quotient algebras. In a commutative domain there is little difficulty in showing that there is always a field of which the domain is a subset; the situation is, however, not so simple in the case of non-commutative domains. We shall take first the case of Euclidean domains.

Let E be a Euclidean domain and consider all pairs of integers a, b for which $b \neq 0$. Let $a_1 b = b_1 a$ be the L. C. L. M. of a and b and let (a, b) denote the class of all pairs p, q such that

$$a_1 q = b_1 p, \quad q \neq 0. \tag{30}$$

From Theorem 8. 2 it follows that, if r is a H. C. R. F. of a and b, and $a = a_2 r$, $b = b_2 r$, then $p = a_2 s$, $q = b_2 s$, and any pair of this form belongs to (a, b). We have therefore

$$(a, b) = (as, bs), \quad s \neq 0. \tag{31}$$

If (c, d) is another class of pairs and $e = be_1 = de_2$ is a L. C. R. M. of b and d, we have

$$(a, b) = (ae_1, be_1) = (ae_1, e), \quad (c, d) = (ce_2, e)$$

so that, if we have any finite number of classes, we can always assume that the second members of the representative pairs are identical; similar reasoning shows that we may, if we please, make the first members equal instead of the second. The sum of (a, b) and (c, d) is now defined as follows.

$$(a, b) + (c, d) = (ae_1 + ce_2, e). \tag{32}$$

Again, if $f = bf_1 = cf_2$ is a L. C. R. M. of b and c, then

$$(a, b) = (af_1, bf_1) = (af_1, f), \quad (c, d) = (cf_2, df_2) = (f, df_2)$$

and the product of (a, b) into (c, d) is defined by

$$(a, b)\,(c, d) = (af_1, f)\,(f, df_2) = (af_1, df_2). \tag{33}$$

The zero element is $(0, b)$ and the identity is $(1, 1)$; also by definition $(a, b)(0, b) = (0, b)$.

We have now to show that the operations just defined lead to a division algebra (non-commutative field). We shall leave to the reader the proof that addition is uniquely defined, associative, and commutative as the proofs differ only in detail from those which we shall now give for multiplication. The definition of multiplication is independent of the pair chosen to represent the class. For, if (a, b) is replaced by (as, bs) and we set $g = bsg_1 = cg_2$, then by Theorem 8.2, we have $sg_1 = f_1 t$, $g_2 = f_2 t$ and therefore

$$(as, bs)\,(c, d) = (asg_1, dg_2) = (af_1 t, df_2 t) = (af_1, df_2) = (a, b)\,(c, d).$$

A repetition of this process shows that the product is independent of the representative pairs.

The proof of the associative law is as follows. If $k = dk_1 = ek_2$, we may replace a triad (a, b), (c, d), (e, f) in which no first member is 0 by (a, b), (ck_1, k), (k, fk_2) and then, if $h = bh_1 = ck_1 h_2$, this in tu rnmay be replaced by (ah_1, h), $(h, kh_2)(kh_2, fk_2 h_2)$; there is therefore no loss of generality in taking the triad in the form (a, b), (b, c), (c, d). We then have

$$(a, b)\,[(b, c)\,(c, d)] = (a, b)\,(b, d) = (a, d),$$

$$[(a, b)\,(b, c)]\,(c, d) = (a, c)\,(c, d) = (a, d),$$

so that multiplication is associative.

The distributive law holds good. In the first place, in $(h, k)[(a, b) + (c, d)]$ we may take $a = c$ and then $k = a$. Let $p = bp_1 = dp_2$; then

$$\begin{aligned}(h, a)[(a, b) + (a, d)] &= (h, a)(a(p_1 + p_2), p) = (h(p_1 + p_2), p) \\ &= (hp_1, p) + (hp_2, p) = (h, a)(ap_1, p) + (h, a)(ap_2, p) \\ &= (h, a)(a, b) + (h, a)(a, d).\end{aligned}$$

The left-hand distributive law is proved in the same fashion.

Finally, the product of any element by the zero element $(0, b) = 0$ is clearly the zero element; and conversely, if $(a, b)(c, d) = 0$ either $c = 0$ or

$$0 = (a, b)(c, d) = (af_1, df_2)$$

by (33); hence $af_1 \neq 0$ and, since $f_1 = 0$, we have $a = 0$, that is $(a, b) = 0$.

The set of classes of the form $(a, 1)$ forms a subset which is simply isomorphic with E, and hence by the usual process of identification we have a division algebra over E as required.

The following is another type of domain, not necessarily Euclidean, in which the quotient domain exists. Let H be a domain of integrity and J its scalar domain or centrum. If a is any element of H, it sometimes happens (e. g., Example 6) that there exists in H an integer $\bar{a}$ for which $a\bar{a} = \alpha$ is scalar; $\bar{a}$ is then said to be an adjoint of a; it is easily shown that $\bar{a}a = a\bar{a}$. Such a domain may be called a *Hamiltonian* domain. Since J is scalar, it is readily extended so that α has an inverse and then $\bar{a}\alpha^{-1}$ is an inverse of a.

A somewhat more general problem is the introduction of new units in a domain. In particular, when there is given an element b of the domain, it is desirable to know under what conditions the domain may be so extended that b and its powers are units. We shall not attempt a detailed discussion of this question here, but will merely remark that, in view of the discussion given above it is sufficient to suppose that for any element a of the domain there correspond elements a_b, b_a such that $ba_b = ab_a$. If every element can be made a unit by a suitable extension of the domain, then as a rule a quotient domain exists. This quotient domain is a trivial Euclidean domain, a remark which suggests the interesting problem of finding in any particular case the minimum set of units which must be added to make the domain Euclidean. For example, $K(\sqrt{-5})$ is not Euclidean but becomes so on making 3 a unit.

10. Linear equations; the normal form of a matrix. Consider a laevolateral system of linear equations in a Euclidean domain E,

$$y = \sum_{j=1}^{m} a_{ij} x_j, \qquad i = 1, 2, \ldots, n, \tag{34}$$

that is, $y = Ax$ where A is the matrix $\| a_{ij} \|$. Any system $z = Bw$ is said to be equivalent to (34), if we have simultaneously

$$z = Hy, \quad w = Kx; \quad y = Mz, \quad x = Nw,$$

where the coordinates of each of the matrices H, K, M, N are integral, that is, H and K have inverses which are integral in E. We shall show below that H and K can be obtained by a sucession of elementary transformations and are therefore elementary matrices.

A left-hand elementary transformation of type I performed on the y's, say, replacing y_p by $y_p + \theta y_q (p \neq q)$ and leaving the other y's unchanged, leads to a new set of equations in which the vector x is the same as before but with a new matrix which is derived from A by adding to the p^{th} row the q^{th} row multiplied on the left by an integer θ. The same transformation on the x's leads to an equivalent system in which

y is unchanged but in which the matrix is obtained from A by adding to the q^{th} column the p^{th} multiplied by θ on the right. These operations are therefore naturally called elementary transformations of type I on the matrix. The interpretation of transformations of types II, III is immediate. We shall now leave the system (34) and consider only transformations of the matrix A.

The process of finding a normal form for A in a non-commutative domain is considerably more complicated than in ordinary algebra, and it is therefore convenient to break the complete statement of the results into three separate theorems.

Theorem 10. 1. *There exist elementary matrices P, Q with coefficients in E such that PAQ has the form*

$$PAQ = \begin{Vmatrix} \alpha_1 & & & & & & \\ & \alpha_2 & & & & & \\ & & \ddots & & & & \\ & & & \alpha_r & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{Vmatrix}, \tag{35}$$

where (I) *α_i is both a right and a left factor of α_j for $j > i$,* (II) *$\sigma(\alpha_i) \leqq \sigma(\alpha_j) (j > i)$, and* (III) *$\sigma(\alpha_1)$ is not greater than the stathm of any non-zero coordinate of A.*

A diagonal matrix satisfying the conditions of this theorem will be called a *normal* form of A.

The theorem is true for matrices of order 1 so that we can make the proof by induction; we assume, therefore, that it is true for matrices of order $n - 1$ with the exception of the condition $\sigma(\alpha_i) \leqq \sigma(\alpha_j)$, which need not be assumed for the moment. If a coordinate a_{ij} is a left factor of another in the same row, say $a_{ip} = a_{ij}\,\theta$, subtracting the j^{th} column multiplied on the right by θ from the p^{th} column replaces a_{ip} by 0. If a_{ij} is not a left factor of a_{ip}, we can find an integer θ such that $a_{ip} = a_{ij}\,\theta + a'_{ip}$, $\sigma(a'_{ip}) < \sigma(a_{ij})$, and the operation just described replaces a_{ip} by a'_{ip}; and similar operations can be performed on the rows, the only difference being that θ occurs on the left instead of on the right in multiplying. Since the minimum stathm of the coordinates is never increased by this process, we can, permuting rows and columns if necessary, arrive by a finite number of steps at a matrix of the form

$$\begin{matrix} b_{11} & 0 & 0 & \cdots & 0 \\ 0 & b_{22} & b_{23} & \cdots & b_{2m} \\ 0 & b_{32} & b_{33} & \cdots & b_{3m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & b_{m2} & b_{m3} & \cdots & b_{mm} \end{matrix} \tag{36}$$

in which $\sigma(b_{11})$ is not greater than the stathm of any other non-zero b_{ij} and is not greater than the minimum stathm for the non-zero coordinates of A. Suppose that, when this is done, b_{11} is not a R. F. of some other non zero coordinate, say $b_{ij} = \theta\, b_{11} + b'_{ij}$, $\sigma(b'_{ij}) < \sigma(b_{11})$; then after adding the i^{th} column to the first, we can as before deduce a matrix containing the coordinate b'_{ij} (in the position $(i1)$), and we have in this way reduced the stathm of the coordinate of minimum stathm. If b_{11} is not a L. F. of some b_{ij}, a similar operation, interchanging the roles of rows and columns and using left division instead of right, will also produce a coordinate of lower stathm than before. It follows that by a finite sequence of such steps we can arrive at a matrix of the form (36) in which b_{11} is not only a coordinate of minimum stathm but is also both a right and a left factor of

every other coordinate. We can now by the hypothesis of the induction reduce the array formed by omitting the first row and column in (36) to the form (35), and the elementary transformations used in doing this do not disturb the first row or column when applied to (36). If, when this is done, α_1 is not both a right and a left factor of some element in the main diagonal, we can proceed as before to lower the minimum stathm and, since this minimum cannot be less than 1, we finally arrive at the form required by the theorem except for the condition regarding the stathms of the α's. This condition is trivial in the case of proper domains and it is easily shown that it can be satisfied in any Euclidean domain. For if at any stage in the reduction of (36) the stathm $\sigma(b_{11})$ ceases to be minimal, this only means that we can start over again with a lower minimal stathm than before; and, since the stathm cannot decrease indefinitely, we shall reach the form of our theorem after a finite number of steps.

The number r is called the *rank* of A.

Theorem 10. 2. *The rank of a matrix A is independent of the manner in which it is reduced to the normal form of Theorem* 10. 1; *and A has an inverse in the domain if, and only if, $r = m$ and $\alpha_1, \alpha_2, \ldots, \alpha_m$ are all units in which case A is the product of a finite number of elementary transformations.*

Suppose that $A_1 = P_1 A Q_1$ and $A_2 = P_2 A Q_2$ are two reductions of A to the normal form given above and let the diagonal elements which are not zero be $\alpha_1, \alpha_2, \ldots, \alpha_r$ in A_1 and $\beta_1, \beta_2, \ldots, \beta_s$ in A_2 and suppose if possible that $r < s$. Then $A_1 Q_1^{-1} Q_2 = P_1 P_2^{-1} A_2$ or, say,

$$A_1 Q = P A_2, \quad P = \| p_{ij} \|, \quad Q = \| q_{ij} \|,$$

which gives $\alpha_i q_{ij} = p_{ij} \beta_j$. For $i = r+1, r+2, \ldots, n$, $j = 1, 2, \ldots, s$ we have $\alpha_i = 0$, $\beta_j \neq 0$ and hence also $p_{ij} = 0$. If we now reduce the array formed by the first r rows and first s columns of P to the normal form of Theorem 10. 1, the transformations used in doing so will leave unaltered the block of zeros which make up the first s columns of the last $n-r$ rows. But $s > r$ so that, when these transformations are carried out, the new $(r+1)^{\text{th}}$ column must consist of zeros; and this is impossible since P has an inverse and therefore any matrix derived from it by elementary transformations will also have an inverse. Hence r is not less than s. A similar argument shows that $r \not> s$ and therefore $r = s$.

If A has an inverse in E, A_1 is the inverse of $Q_1^{-1} A^{-1} P_1^{-1}$, from which it follows immediately that no α is 0, that is, $r = n$, and that each α is a unit which may be taken to be 1.

Theorem 10. 3. *In a proper Euclidean domain the normal form* (35) *can be so chosen that every left (right) factor of α_i is a right (left) factor of α_j for $i < j$.*

Before proving this theorem we require the following definition and lemma. If A is the diagonal matrix of rank r whose main diagonal is $\alpha_1, \alpha_2, \ldots, \alpha_r, 0, \ldots, 0$, we shall call the vector

$$\sigma(A) \equiv (\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_r), 0, \ldots, 0)$$

the stathm of A. Further, let B be a second diagonal matrix of rank s for which $\sigma(B) = (\sigma(\beta_1), \ldots, \sigma(\beta_s), 0, \ldots, 0)$; then, if the first of the differences[1]) $\sigma(\alpha_i) - \sigma(\beta_i)$ which is not zero is negative, we shall write $\sigma(A) \to \sigma(B)$ and say that $\sigma(A)$ precedes $\sigma(B)$ or that the stathm of A is lower than that of B.

[1]) If $i > r$, then $\sigma(\alpha_i)$ is to be replaced here by 0, and similarly $\sigma(\beta_i)$ when $i > s$.

Lemma. *If the diagonal matrix A is normal and if α_i, α_j $(i < j)$ are replaced by γ_i, γ_j, where $\sigma(\gamma_i) < \sigma(\alpha_i)$, so giving a new matrix C, then C is equivalent to a normal matrix B such that $\sigma(B) \to \sigma(A)$.*

The proof of this lemma is immediate and the details are left to the reader. If C is normal, then $\sigma(C) \to \sigma(A)$ and $B = C$, whereas, if C is not normal, the process used in the proof of Theorem 10. 1 clearly replaces it by a normal matrix B and either $\sigma(B) = \sigma(C) \to \sigma(A)$ or $\sigma(B) \to \sigma(C) \to \sigma(A)$.

Suppose now that A_1 is the normal matrix (35) and that α_i, α_j $(j > i)$ are such that there is a L. F. β of α_i which is not a R. F. of α_j; further let θ be a H. C. R. F. of β and α_j and set

$$\beta = \lambda\,\theta, \quad \alpha_j = \mu\,\theta;$$

we can then find p, q, h, k, such that

$$p\,\lambda + q\,\mu = 1, \quad h\,\lambda + k\,\mu = 0$$

and so that $P = \begin{Vmatrix} p & q \\ h & k \end{Vmatrix}$ is an elementary matrix. If $\alpha_i = \beta\gamma$, this gives

$$p\alpha_i + q\alpha_j\gamma = \theta\gamma, \quad h\alpha_i + k\alpha_j\gamma = 0\,.$$

Since elementary transformations on (35) which involve only the columns and rows in which α_i, α_j occur do not affect any other α_k, we may replace (35) for the moment by $\begin{Vmatrix} \alpha_i & 0 \\ 0 & \alpha_j \end{Vmatrix}$ which is equivalent to

$$\begin{Vmatrix} \alpha_i & 0 \\ \alpha_j\gamma & \alpha_j \end{Vmatrix}.$$

Operating on the left by P we get the equivalent matrix

$$\begin{Vmatrix} p\alpha_i + q\alpha_j\gamma & q\alpha_j \\ h\alpha_i + k\alpha_j\gamma & k\alpha_j \end{Vmatrix} = \begin{Vmatrix} \theta\gamma & q\alpha_j \\ 0 & k\alpha_j \end{Vmatrix}$$

which is equivalent to a normal matrix $\begin{Vmatrix} \gamma_i & 0 \\ 0 & \gamma_j \end{Vmatrix}$ in which $\sigma(\gamma_i) \leqq \sigma(\theta\,\gamma)$. If the domain of the coefficients is proper, then $\sigma(\theta\,\gamma) < \sigma(\alpha_i)$ and by the lemma proved above we are led to a normal matrix B equivalent to A_1 and such that $\sigma(B) \to \sigma(A_1)$. Since it follows from postulate $E1$ that only a finite number of vector stathms can precede a given one, a finite number of applications of the process used above must give a matrix satisfying the conditions of the theorem.

Eingegangen 20. August 1931.