JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

L.-E. DICKSON

A New Simple Theory of Hypercomplex Integers

Journal de mathématiques pures et appliquées 9^e série, tome 2 (1923), p. 281-326.
<http://www.numdam.org/item?id=JMPA_1923_9_2__281_0>

A New Simple Theory of Hypercomplex Integers;

By L.-E. DICKSON.

1. *Introduction.* — Since this Memoir presents ideas of more general interest than its title would indicate, it has been so written that it may be read by those having no previous acquaintance with hypercomplex numbers. It opens up a broad subject which is destined to furnish a wide generalization of the theory of algebraic numbers.

A clear idea of the nature of our conclusions is furnished by §§ 4-6. These and the earlier sections are strictly elementary and self-contained, and make use only of facts proved here.

The immediate purpose of the Memoir is to present a new conception of hypercomplex integers which is entirely free from the fatal objections valid against the earlier conceptions of Hurwitz and Du Pasquier (§ 4). If their definitions are taken literally, there do not exist hypercomplex integers in the majority of algebras of hypercomplex numbers. If we discard a certain one of their assumptions, we obtain integers but are faced with the insurmountable difficulty that factorization into primes is not only not unique, but cannot be made unique by the introduction of ideals of any kind, a fact proved in this Memoir. These essential difficulties all disappear under the new definition proposed here.

In his various papers cited below, Du Pasquier merely determined the integers in each algebra in the classic lists, without investigating the properties of the integers. This investigation is made here for the algebras in 2 and 3 units, to obtain material for an adequate comparison of the old and new definitions, and such a comparison is always

decidedly in favor of the new. Incidentally, the new definition tells us automatically just what enlargement we need to make of a Du Pasquier system of integers in order to obtain a system having unique factorization into primes.

The new definition has been tested by all the classic algebras in 2, 3 and 4 units, and found in every case to give wholly satisfactory results, as well as to explain serious difficulties arising under the earlier definitions. Moreover, the new theory is far simpler to apply than the old, and more readily lends itself to the proof of general theorems, which are wholly lacking in the writings based on the old definitions.

2. *Hypercomplex numbers.* — The oldest example is that of ordinary complex numbers $a+bi$, where a and b are real and i denotes $\sqrt{-1}$. Next we have algebraic numbers, like

$$x=a+b\sqrt{-3}, \qquad y=a+b\sqrt[3]{2}+c\sqrt[3]{4},$$

where now a, b, c are rational numbers (integers or fractions). These are examples of hypercomplex numbers

$$x=a+be\,(e=\sqrt{-3}), \qquad y=a+be_1+ce_2\,(e_1=\sqrt[3]{2},\ e_2=\sqrt[3]{4}),$$

the first having two *basals units*, $e_0=1$, e, and the second three basal units $e_0=1$, e_1, e_2. The numbers a, b or a, b, c, which are multiplied into the units, are called *coordinates*. The units satisfy the relations

$$e^2=-3; \qquad e_1^3=e_2, \qquad e_1e_2=e_2e_1=2, \qquad e_2^2=2e_1.$$

We may and shall ignore the values of the units as radicals, and employ these relations to express any product (or square) of the units as a linear function of the units. The same is therefore true as to the product of any two numbers x or any two numbers y. We call such a set of relations the *multiplication table* of the units.

We give another important example needed later. Let

$$(1) \quad e_0=\begin{pmatrix}1&0\\0&0\end{pmatrix}, \qquad e_1=\begin{pmatrix}0&0\\1&0\end{pmatrix}, \qquad e_2=\begin{pmatrix}0&1\\0&0\end{pmatrix}, \qquad e_3=\begin{pmatrix}0&0\\0&1\end{pmatrix}.$$

Then any two-rowed square matrix x may be expressed in terms of these four as follows

$$(2) \qquad x = \begin{pmatrix} x_0 & x_2 \\ x_1 & x_3 \end{pmatrix} = x_0 e_0 + x_1 e_1 + x_2 e_2 + x_3 e_3,$$

since the product of matrix e_0 by x_0 is a similar matrix having the element x_0 in place of 1. The general matrix x is thus expressed as a hypercomplex number with the four basal units e_0, e_1, e_2, e_3, whose multiplication table is (1)

$$(3) \qquad e_0^2 = e_0, \quad e_3^2 = e_3, \quad e_0 e_2 = e_2 e_3 = e_2, \quad e_3 e_1 = e_1 e_0 = e_1,$$
$$e_2 e_1 = e_0, \quad e_1 e_2 = e_3,$$

together with the relations which state that all further squares and products are zero.

Instead of adding or multiplying these hypercomplex numbers, we may (more quickly) add or multiply the corresponding matrices x. To find the element in the rth row and cth column of the product of x by a similar matrix x', we multiply the elements of the rth row of x by the corresponding elements of the cth column of x' and add the two products. For example,

$$x' = \begin{pmatrix} x_3 & -x_2 \\ -x_1 & x_0 \end{pmatrix}, \qquad x x' = \begin{pmatrix} x_0 x_3 - x_1 x_2 & 0 \\ 0 & x_0 x_3 - x_1 x_2 \end{pmatrix}.$$

Hence x and x' are roots of

$$(4) \qquad x^2 - (x_0 + x_3) x + (x_0 x_3 - x_1 x_2) \varepsilon = 0, \qquad \varepsilon = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Here $\varepsilon = e_0 + e_3$ plays the rôle of unity in multiplication. Thus every two-rowed square matrix x is a root of a quadratic equation. Matrices are known to obey the associative law of multiplication $xy.z = x.yz$.

In the same manner, we can express all n-rowed square matrices as hypercomplex numbers in n^2 basal units. Such a matrix x is the

(1) If we write e_{11} for e_0, e_{21} for e_1, e_{12} for e_2, and e_{22} for e_3, we may express the multiplication table (of 16 products) in the compact form

$$e_{ij} e_{jk} = e_{ik}, \qquad e_{ij} e_{lk} = 0 \qquad (l \neq j).$$

root (1) of an equation of degree n whose constant term is the determinant of x and is called the *norm* of x. Hence the norm of a product is the products of the norms of the factors.

In general, we shall consider only hypercomplex numbers (2)

$$x = x_0 e_0 + x_1 e_1 + \ldots + x_n e_n \tag{5}$$

with rational coordinates $x_0, \ldots, x_n$ and a multiplication table

$$e_i e_j = \sum_{k=0}^{n} \gamma_{ijk} e_k \qquad (i, j = 0, 1, \ldots, n), \tag{6}$$

where the constants γ_{ijk} are rational numbers. The product of x by

$$y = y_0 e_0 + \ldots + y_n e_n$$

is defined to be the number obtained from $\Sigma x_i y_j e_i e_j$ by replacing $e_i e_j$ by its expression (6). We agree that x and y are equal if and only if $x_0 = y_0, \ldots, x_n = y_n$. We assume the associative law and the existence of a (unique) *principal unit* ε such that $\varepsilon x = x\varepsilon = x$ for every hypercomplex number x; we shall often write 1 for ε. If r is a rational number, rx denotes $\Sigma(rx_i)e_i$. We define $x + y$ to be

$$(x_0 + y_0)e_0 + \ldots + (x_n + y_n)e_n.$$

Hence the set of all numbers (5) with rational coordinates is closed under addition, subtraction, and multiplication. It is called a rational

---

(1) For a very simple proof, see the second foot-note in § 15.

(2) We may identify e_j with the matrix having the element γ_{ijk} in the $(i+1)$ th row and $(k+1)$ th column; then relations (6) hold in matrices. For example, if

$$e_0^2 = e_0, \qquad e_1 e_0 = e_0 e_1 = e_1, \qquad e_1^2 = -e_0,$$

then

$$e_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad e_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Hence ordinary complex numbers $x_0 + x_1 i$ may be expressed as matrices

$$\begin{pmatrix} x_0 & x_1 \\ -x_1 & x_0 \end{pmatrix}.$$

linear associative algebra with a principal unit (briefly a rational *algebra*), or a rational hypercomplex number system.

Since $\varepsilon, x, x^2, \ldots, x^{n+1}$ are linear homogeneous functions of $e_0, \ldots, e_n$ with rational coefficients, some linear combination of them with rational coefficients is zero. Hence x satisfies an unique equation of lowest degree with rational coefficients and leading coefficient unity. This is called the *rank equation* when the coordinates of x are arbitrary rational numbers. Its constant term is called the *norm* of x and designated $\mathrm{N}(x)$.

5. *Preliminary survey of hypercomplex integers.* — Gauss called $a + bi$ a complex integer if a and b are rational integers; every complex integer decomposes into complex primes uniquely apart from unit factors, $\pm 1, \pm i$.

For $\theta = \sqrt{-3}$, we might call $a + b\theta$ a quadratic integer if and only if a and b are rational integers. But 4 would then have two essentially different factorizations

$$4 = 2 \times 2, \qquad 4 = (1 + \theta)(1 - \theta)$$

into indecomposable integers $2, 1 + \theta, 1 - \theta$, no one of which is the product of another by a unit, necessarily ± 1. By a *unit* is meant a (quadratic) integer $u = a + b\theta$ which divides 1, so that there exists another integer v such that $uv = 1$. Then $\mathrm{N}(u)\mathrm{N}(v) = 1$, where $\mathrm{N}(u) = a^2 + 3b^2$ is a rational integer. Hence $\mathrm{N}(u) = 1$, $a = \pm 1$, $b = 0$, and $u = \pm 1$.

We may avoid all such double factorizations by including among our (algebraic) integers not only the numbers $a + b\theta$ in which a and b are rational integers, but also those in which a and b are both halves of odd integers. Then

$$u = \frac{1}{2} + \frac{1}{2}\theta, \qquad u' = \frac{1}{2} - \frac{1}{2}\theta$$

are units since they are algebraic integers whose product is 1. The only units are here $\pm 1, \pm u, \pm u'$. Thus the second of the above factorizations of 4 may now be written in the form $4 = (2u)(2u')$, which

is not regarded as essentially different from $4 = 2 \times 2$, just as the latter is not distinguished from $4 = (-2)(-2)$.

A still simpler example will show the wisdom of enlarging certain proposed systems of integers. Let the system S be composed of unity and all positive *even* integers, This system is evidently closed under multiplication. Then 60 has two (and only two) decompositions into indecomposables of S :

$$60 = 2 \times 30, \qquad 60 = 6 \times 10,$$

where no one of 2, 6, 10, 30 is a product of two numbers, each not the unique unit 1, of S, so that all four are indecomposable. We evidently restore unique factorization into indecomposables by annexing to S all positive odd integers.

An algebraic number is called integral if and only if it is a root of an equation having rational integral coefficients and having unity as the coefficient of the highest power of the unknown. For example, $x = a + b\sqrt{m}$ is a root of

$$x^2 - 2ax + (a^2 - mb^2) = 0,$$

which, for $m = -1$, has rational integral coefficients only when a and b are both rational integers, so that we have Gauss's complex integers $a + bi$. For $m = -3$, the coefficients are rational integers only when a and b are either both rational integers or both halves of odd integers (see above). For $m = -3k^2$, where k is a rational integer, a and kb have the values just mentioned, so that the coordinate b of the algebraic integer x may have the denominator $2k$.

There is no point in studying factorization in the set A of all integral algebraic numbers. For, if a is any rational integer,

$$a = a_1^2 = a_2^4 = a_3^8 = \ldots,$$

where a_1, a_2, a_3, ..., are roots of $x^2 = a$, $x^4 = a$, $x^8 = a$, ..., and hence belong to A, so that the factorization of a within A would never terminate. Hence in the theory of algebraic numbers we confine our attention to the rational functions with rational coefficients of a particular algebraic number. Then uniqueness of factorization into primes

either holds true or can always be secured by the introduction of Dedekind's ideals. The above definition of algebraic integers led to this wholly satisfactory conclusion and is therefore a thoroughly satisfactory definition.

However, this definition fails in general for hypercomplex numbers. For example, let us call a two-rowed square matrix (2) integral if and only if its four elements are rational and the coefficients of the quadratic equation (4) satisfied by it are rational integers. Then, if k is an arbitrary rational integer $\neq 0$,

$$M_k = \begin{pmatrix} 0 & k^{-1} \\ k & 0 \end{pmatrix}$$

is an integral matrix, since it is a root of $x^2 - 1 = 0$ by $M^2 = \varepsilon$. But

$$P = M_2 M_1 = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{pmatrix}, \qquad S = M_1 + M_2 = \begin{pmatrix} 0 & \frac{3}{2} \\ 3 & 0 \end{pmatrix}$$

are neither integral matrices, since the middle coefficient of (4) is $\frac{5}{2}$ for P, and the constant term is $-\frac{9}{2}$ for S. Hence this set of integral matrices is closed neither under multiplication nor under addition.

Historically the first definition of hypercomplex integers was that made for the case of quaternions

$$q = a + bi + cj + dk$$

by R. Lipschitz (1). The multiplication table of the basal units (2) is

(7) $\quad i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$

---

(1) *Journal de Math.*, série 4, t. II, 1886, p. 393-439.

(2) They may be defined in terms of the matrix units (1) as follows :

$$1 = e_0 + e_3, \qquad i = \sqrt{-1}\,(e_3 - e_0), \qquad j = e_2 - e_1,$$
$$k = -\sqrt{-1}\,(e_2 + e_1),$$

Or we may define $1, i, j, k$ as 4-rowed square matrices with rational integral elements by means of the last note in § 2.

He called q an integral quaternion if and only if a, b, c, d are rational integers. But we then have three essentially different factorizations of 2 into prime quaternions $1+i$, $1+j$, $1+k$:

$$(8) \qquad 2=-i(1+i)^2, \qquad 2=-j(1+j)^2, \qquad 2=-k(1+k)^2,$$

while $1+i$ is not the product of $1+j$ or $1+k$ by a unit, here ± 1, $\pm i$, $\pm j$, or $\pm k$.

A. Hurwitz (1) avoided all such difficulties by including among the integral quaternions not only those of Lipschitz, but also all quaternions whose coordinates are all halves of odd numbers. Now the three factorizations (8) are no longer essentially different; for example,

$$1+j=(1+i)u, \qquad u=\frac{1}{2}(1-i)(1+j)=\frac{1}{2}(1-i+j-k),$$

and the integral quaternion u is a unit since $uu'=1$, where

$$u'=\frac{1}{2}(1+i-j+k)$$

is an integral quaternion. Hurwitz's system of integral quaternions is closed under addition, subtraction, and multiplication, and they have unique factorization into prime quaternions when the arrangement of the norms of those primes is prescribed.

We do not obtain satisfactory results by following the definition of integral algebraic numbers and calling a quaternion q integral if and only if its coordinates are rational and the coefficients of the quadratic equation satisfied by q and its conjugate

$$q'=a-bi-cj-dk$$

are rational integers. For,

$$Q=\frac{3}{5}i+\frac{4}{5}j$$

would be integral since $Q^2=-1$, and $Q-i$ not integral being a

(1) *Göttinger Nachrichten*, 1896, p. 311-340; amplified in his *Vorlesungen über die Zahlentheorie der Quaternionen* (Berlin, 1919).

root of $x^2 + \frac{4}{5} = 0$. Thus the difference of the integral quaternions Q and i is not integral.

4. *Hypercomplex integers as defined by Hurwitz and Du Pasquier.* — Our aim is to select the integers from the set of all hypercomplex numbers (5) with rational coordinates, having a multiplication table (6) in which the γ_{ijk} are given rational numbers. In brief we seek the arithmetic of a given rational algebra.

Although the definition by Hurwitz was stated only for quaternions, it may be expressed in general form as follows.

Within a rational hypercomplex number system [*cf.* (5), (6)] a system of *integral* hypercomplex numbers shall have the following properties :

B (basis) : The system has a finite basis (i. e., it contains numbers $q_1, \ldots, q_k$ such that every number of the system is expressible in the form $\Sigma c_i q_i$, where each c_i is a rational integer);

C (closure) : The system is closed under addition, subtraction, and multiplication;

U (units) : The system contains the basal units $e_0, \ldots, e_n$;

M (maximal) : The system is a maximal (i. e., it is not contained in a larger system having properties B, C, U).

The only modification made by Du Pasquier (1) was to replace U by the weaker assumption U_1 :

U_1 (unit 1) : The systems contains the principal unit 1.

We proceed to show that each of these definitions fails completely for the algebra with two basal units 1 and e, where $e^2 = 0$. Any system has a basis 1, $q = r + se$, where r and s are fixed rational numbers, $s \neq 0$. Since q^2 is in the system by C, we must have $q^2 = a + bq$, where a and b are rational integers. Hence

$$r^2 = a + br, \qquad 2rs = bs; \qquad 2r = b, \qquad r^2 = -a.$$

Thus r is a rational integer, so that any system has the basis 1, se,

(1) *Vierteljahrsschrift Naturf. Gesell. Zürich*, t. 54, 1909, p. 116-148; *L'enseignement math.*, t. 17, 1915, p. 340-343; t. 18, 1916, p. 201-260.

where s is rational. This system is contained in that having the basis, $1, te$ if and only if $\frac{s}{t}$ is a rational integer. Since therefore the system $(1, se)$ is contained in the larger system $\left(1, \frac{1}{2}se\right)$, and the latter is contained in the still larger system $\left(1, \frac{1}{7}se\right)$, etc., there exists no maximal system. In other words, there exist no hypercomplex integers in this algebra.

The same conclusion holds true also for Hurwitz's definition, which adds the requirement U that e shall occur in the system $(1, se)$ and hence that s be the reciprocal of a rational integer.

Suppose we omit the requirement M that the system be a maximal. It is to be anticipated (§ **5**) that the laws of divisibility in a chosen system will not be as simple as in a larger (existing) system, nor the laws in the latter as simple as in a still larger (existing) system, and so on to infinity, and hence that the laws in the chosen system will be extremely complicated. This conjecture is confirmed in § **5**.

5. *Insurmountable difficulties in any Hurwitz or Du Pasquier binary arithmetic with* $e^2 = 0$. — We shall examine the laws of divisibility in the system having the basis $1, se$, where s is a chosen rational number $\neq 0$. Without disturbing the relation $e^2 = 0$, we may take se as a new basal unit e. Hence we may take $s = 1$.

Then the integers are $x + ye$, where x and y are rational integers. Since $x + ye$ is a root of $(\omega - x)^2 = 0$, its norm is x^2. Hence $x = \pm 1$ for a unit. Conversely, $\pm 1 + ke$ is a unit when k is any rational integer, since its product by $\pm 1 - ke$ is 1. Write

$$c_0 = 3, \qquad c_1 = 3 + e, \qquad c_2 = 3 + 2e.$$

Then

$$c_1 c_2 = c_0^2 u, \qquad c_0 c_2 = c_1^2, \qquad c_0 c_1 = c_2^2 v, \tag{9}$$

where $u = 1 + e$, and $v = 1 - e$ are units. No one of c_0, c_1, c_2 can be obtained from another one of them by multiplication by units both on the left and right. For if u_k denotes $\pm 1 + ke$,

$$u_k c_j u_l = c_n, \qquad n = j \pm 3(l + k) = j \pmod 3.$$

Finally, since no integer has the norm 3, c_j is not the product of two integers neither of which is a unit, and hence is a prime. Thus, by (9), we have two essentially different decompositions $c_0 c_2$ and c_1^2 of the same integer into primes.

Nor is it possible to restore unique factorization into primes by the introduction of ideals, however defined. It is understood that in introducing ideals, each integer whose norm is not zero, and its associates (i. e., all products of it on both sides by arbitrary units), shall correspond to the same unique ideal, and that the product of two integers corresponds to the ideal which is the product of the two ideals corresponding to the two integers, and finally that the ideal I corresponding to the units plays the rôle of unity in the multiplication of ideals and has no ideal factor other than I. Hence the totality of ideals contains a set of ideals simply isomorphic with the set of classes of associated integers.

Then c_0, c_1, c_2 correspond to distinct ideals C_0, C_1, C_2, no one the unit ideal I, such that, by (9),

$$C_1 C_2 = C_0^2, \qquad C_0 C_2 = C_1^2, \qquad C_0 C_1 = C_2^2. \tag{10}$$

By the last two equations, any prime ideal factor D of C_0 divides both C_1 and C_2. Hence $C_i = DQ_i (i = 1, 2, 3)$, where Q_0, Q_1, Q_2 are distincts ideals. Thus

$$Q_1 Q_2 = Q_0^2, \qquad Q_0 Q_2 = Q_1^2, \qquad Q_0 Q_1 = Q_2^2.$$

No Q_i is I. For, if $Q_2 = I$, the third equation would give $Q_0 = Q_1 = I$. Hence the Q_i have the same properties as the C_i, and it is impossible to express the equal ideals $C_1 C_2$ and C_0^2 as the same product of prime ideals.

THEOREM I. — *For the algebra with the basal units* 1 *and* e, *where* $e^2 = 0$, *the definitions of integers by both Hurwitz and Du Pasquier fail since there is no maximal system. They fail also if we omit their requirement that a maximal system exists, since, if the integers are defined to be numbers of any chosen one of the infinitude of non-maximal systems, factorisation into indecomposable numbers is not unique and cannot be made unique by the introduction of ideals however defined.*

Similar insurmountable difficulties will be shown (§§ **11**, **12**) to arise for the majority of algebras in three units. This is doubtless true also of algebras in four units, for the majority of which there is certainly no maximal system (§ **14**) and hence, properly speaking, no integers under the definition of Hurwitz or Du Pasquier.

6. *New definition of hypercomplex integers.* — We shall employ the assumptions C (closure), U_1 (unit 1), M (maximal) and R :

R (rank equation) : For every number of the system, the coefficients of the rank équation are all rational integers.

We shall often obtain the same system of integers if we replace R by the weaker assumption N:

N (norm) : The norm of every number of the system is a rational integer.

Consider the algebra with the units 1, e, where $e^2 = 0$, for which we saw that the definitions by Hurwitz and Du Pasquier both fail. We make the assumptions C, U_1, M, N. Since $x = a + be$ is a root of $(\omega - a)^2 = 0$, we have $N(x) = a^2$. Hence if x is in a system satisfing our assumptions, a is a rational integer. The unique maximal system (of integers) is evidently composed of all the $x = a + be$, in which a is a rational integer and b is rational. The product of x by the unit $1 + ke$ is $a + (b + ak)e$, which, for $a \neq 0$, becomes a by taking $k = -\frac{b}{a}$. Hence every integer whose norm is not zero is associated with a rational integer a, and hence is factorable into primes uniquely apart from unit factors.

Our unique system of integers is the aggregate of the integers in the infinitude of systems obtained in § **4** by the definition of either Hurwitz or Du Pasquier. The insurmountable difficulties, which arose when they chose as their integers the numbers of any one of their systems, have now been shown to disappear for our properly chosen enlargement of their too restricted system. This enlargement was accomplished by the abandonment of their strong assumption B of a finite basis and the replacement of it by the weaker assumption N about the norm (*cf.* § **8**).

THEOREM II. — *All of the difficulties mentioned in Theorem* I

disappear under the new definition of integers, which now decompose into primes uniquely.

7. *Characteristic equations, property of* $\mathrm{N}(x)$. — To define the characteristic equations, note that, by (6),

$$xe_j = \sum_{k=0}^{n} \gamma_{jk} e_k, \qquad \gamma_{jk} \equiv \sum_{i=0}^{n} x_i \gamma_{ijk}.$$

Writing the first equation in full for $j = 0, 1, \ldots, n$, we get

$$\begin{aligned}
&(\gamma_{00} - x)e_0 + \gamma_{01}e_1 \qquad + \ldots + \gamma_{0n}e_n = 0,\\
&\gamma_{10}e_0 \qquad + (\gamma_{11} - x)e_1 + \ldots + \gamma_{1n}e_n = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\gamma_{n0}e_0 \qquad + \gamma_{n1}e_1 \qquad + \ldots + (\gamma_{nn} - x)e_n = 0.
\end{aligned}$$

When x is replaced by an ordinary variable ω, the determinant of the coefficients of $e_0, \ldots, e_n$ is

$$\delta(\omega) = \left| \sum_{i=0}^{n} \gamma_{ijk} x_i - \delta_{jk}\omega \right|,$$

where $\delta_{jj} = 1$, $\delta_{jk} = 0$ if $j \neq k$. We call $\delta(\omega)$ the *right-hand characteristic determinant* of x. Let $C_0(\omega), \ldots, C_n(\omega)$ denote the adjoint minors of the elements of j th column. Let $\varepsilon = \Sigma \varepsilon_j e_j$ be the principal unit. Multiply the above linear equations by $C_0(x)\varepsilon, \ldots, C_n(x)\varepsilon$ on the left and add. We evidently get $\delta(x)e_j = 0$. Multiply this by ε_j and sum for $j = 0, 1, \ldots, n$; we get $\delta(x)\varepsilon = 0$. Hence x is a root of the right-hand characteristic equation $\delta(\omega) = 0$. It is understood that, besides substituting x^k for ω^k, we multiply the constant term $\delta(0) \equiv \Delta(x)$ by ε.

Similarly, every hypercomplex number x is a root of its left-hand characteristic equation $\delta'(\omega) = 0$, obtained by starting from $e_j x$ instead of the above xe_j. Denote $\delta'(0)$ by $\Delta'(x)$. These characteristic determinants $\delta(\omega)$ and $\delta'(\omega)$ remain unaltered (1) under any linear transformation on the basal units e_j.

If y is a fixed and x a variable hypercomplex number, the rela-

(1) Dickson, *Linear Algebras*, Cambridge University Tract, n° 16, 1914, p. 19.

tion $x' = xy$ defines a linear transformation on $x_0, \ldots, x_n$ with the determinant $\Delta'(y)$. Similarly, to y' corresponds a second transformation $x'' = x'y'$. Then to $y'' = yy'$ corresponds $x'' = xy''$, which is the product of the former transformations. Hence

$$\Delta'(y)\,\Delta'(y') = \Delta'(yy').$$

Similarly, the determinant of the linear transformation defined by $x' = yx$ is $\Delta(y)$, and we get

$$\Delta(y)\,\Delta(y') = \Delta(yy').$$

If the coordinates of x are arbitrary rational integers, its *rank equation* $\mathrm{R}(\omega) = 0$ is the unique equation of lowest degree having the root x and coefficients which are polynomials in the coordinates of x, the leading coefficient being unity. Evidently $\mathrm{R}(\omega)$ divides both $\delta(\omega)$ and $\delta'(\omega)$. Hence $\mathrm{N}(x) \equiv \mathrm{R}(0)$ divides both $\Delta(x)$ and $\Delta'(x)$. By the above definitions, either characteristic equation for $x = \varepsilon$, where ε is the principal unit, is $(1-\omega)^{n+1} = 0$, and $\mathrm{R}(\omega)$ is then a power of $1-\omega$, whence $\mathrm{N}(\varepsilon) = 1$. It now follows (1) that

$$\mathrm{N}(y)\,\mathrm{N}(y') = \mathrm{N}(yy').$$

THEOREM III. — *The norm of a product of any two hypercomplex numbers is equal to the product of their norms.*

8. *General remarks on the definitions of hypercomplex integers.* — In the new definition, we may replace assumption R by the assumption that, for every number of the system, the coefficients of the right-hand characteristic equation are rational integers, or by the similar property for the left-hand characteristic equation. The advantage in demonstrations is that we know the explicit form of the characteristic equations for a general algebra, but not that of the rank equation. Furthermore, we shall prove that the assumptions B and C of Hurwitz and Du Pasquier imply the property R of the rank equation.

THEOREM IV. — *If all the coefficients of the rank equation are*

(1) DICKSON, *Comptes rendus du Congrès international des Mathématiciens*, (Strasbourg, 1920), Toulouse, 1921, § 5.

rational integers, those of either characteristic equation are rational integers, and conversely.

The converse follows from Gauss's lemma; if

$$\delta(\omega) = \omega^m + a_1\omega^{m-1} + \ldots + a_m$$

has rational integral coefficients and is divisible by

$$R(\omega) = \omega^r + A_1\omega^{r-1} + \ldots + A_r,$$

with rational coefficients, these coefficients A_i are all rational integers.

Next let $R(\omega)$ have rational integral coefficients. Then the roots of $R(\omega) = 0$ are integral algebraic numbers. But (1) these roots include all the distinct roots of $\delta(\omega) = 0$. Hence the coefficients of the latter are integral algebraic numbers and also rational (since the coordinates x_i and γ_{ijk} are assumed to be rational), and hence are rational integers.

THEOREM V. — *For every system having the closure pooperty* C *and a finite basis composed* (2) *of as many linearly independent numbers as the algebra has basal units, the characteristic equations of each number of the system have rational integral coefficients.*

Such a system has a basis $E_0 = 1, E_1, \ldots, E_n$. We may take the E_i as new basal units of the algebra. By the closure property C, E_iE_j belongs to the system. By the property B of the basis, E_iE_j is equal to a linear function of $E_0, \ldots, E_n$ with rational integral coefficients. Hence the new constants of multiplication Γ_{ijk} are rational integers. The same is true of the coordinates X_i of every number $X = \Sigma X_iE_i$ of the system (property B). Hence either characteristic equation of X has rational integral coefficients. But the coefficients of that equation are invariant under every linear transformation of the basal units (§ 7).

Hence *any system according to the definition of Du Pasquier is*

---

(1) G. SCHEFFERS, *Math. Annalen*, t. 39, 1891, p. 302. — DICKSON, *Linear Algebras*, p. 22.

(2) Assumed by Du Pasquier (ref. in § 4) in finding his systems of 2-rowed square matrices, the only algebra for which he has given details of the work of finding maximal systems.

a system according to the new definition, but not conversely, so that the new maximal systems are usually not systems of Du Pasquier.

After the introduction of the new basal units E_i, the particular Du Pasquier system becomes the set of linear combinations of the E_i with rational integral coordinates and hence has property U; but this need not be true simultaneously of the remaining Du Pasquier systems of the same algebra (*cf.* § **16**). Hence after making a suitably chosen transformation of the basal units with rational coefficients, we obtain an algebra in which at least one Du Pasquier system is a Hurwitz system.

9. *General theory of integers of reducible algebras.* — A linear associative algebra S of hypercomplex numbers with s basal units whose coordinates range independently over all rational numbers, and having a principal unit ε, is called *rationally reducible* if it contains $\alpha + \beta = s$ numbers $e_1, \ldots, e_\alpha, E_1, \ldots, E_\beta$, not satisfiing a linear homogeneous equation with rational coefficients, such that

$$(11) \qquad e_i E_j = 0, \qquad E_j e_i = 0 \qquad (i = 1, \ldots, \alpha; j = 1, \ldots, \beta).$$

In the contrary case, S is called rationally irreducible.

Let S be rationally reducible. It is readily proved (1) that all squares and products of $e_1, \ldots, e_\alpha$ are linear functions of $e_1, \ldots, e_\alpha$ with rational coefficients, so that $e_1, \ldots, e_\alpha$ are the basal units of an algebra a with rational coordinates. Likewise, $E_1, \ldots, E_\beta$ are the basal units of an algebra A. Also, a and A have principal units e and E respectively, whose sum is ε.

Conversely, from any two linear associative algebras a and A with basal units e_i and E_j, principal units e and E, and rational coordinates, we evidently obtain a linear associative algebra S with the basal units $e_1, \ldots, e_\alpha, E_1, \ldots, E_\beta$, principal unit $e + E$, and rational coordinates, by postulating relations (11) and regarding $e_1, \ldots, E_\beta$ as satisfyng no linear homogeneous equation with rationial coefficients.

We call S the *direct sum* of a and A and write $S = a + A = A + a$, and call a and A the *components* of S.

---

(1) Dickson, *Linear Algebras*, p. 26, 27.

THEOREM VI. — *Consider systems of integers having properties* C, U_1, R (*and* M). *The first* (*or second*) *components of the numbers of any* (*maximal*) *system of integers of a rationally reducible algebra constitute a* (*maximal*) *system of integers of the first* (*or second*) *component algebra. Conversely, given a* (*maximal*) *system* $[x]$ *of integers* x *of an algebra* a *and a* (*maximal*) *system* $[\mathrm{X}]$ *of integers* X *of another algebra* A, *if we add every number* x *to every number* X, *we obtain sums forming a* (*maximal*) *system of integers of the direct sum* $a + \mathrm{A}$.

By Theorem IV, R implies that the coefficients of the right-hand characteristic equation are rational integers, and conversely.

(*i*). Let $[z]$ be any given system of integers z of a reducible algebra $\mathrm{S} = a + \mathrm{A}$. We have $z = x + \mathrm{X}$, where x is a number $\Sigma x_i e_i$ of the first component algebra a, and X is a number $\Sigma \mathrm{X}_k \mathrm{E}_k$ of A. To determine the right-hand characteristic determinant of z for S (§ 7), we employ

$$ze_j = \sum_{i=1}^{\alpha} x_i e_i e_j + 0 \qquad (j = 1, \ldots, \alpha),$$

$$z\mathrm{E}_j = 0 + \sum_{k=1}^{\beta} \mathrm{X}_k \mathrm{E}_k \mathrm{E}_j \qquad (j = 1, \ldots, \beta).$$

Hence the right-hand characteristic determinant of z for S is equal to the product of that of x for a by that of X for A. Hence, by Gauss's lemma (§ 8), the polynominals in ω which are equal to the last two determinants have rational integral coefficients when z is in the system $[z]$. Hence the rank equations of x and X for a and A, respectively, have rational integral coefficients. Next, if also $z' = x' + \mathrm{X}'$ is in $[z]$, then $zz' = xx' + \mathrm{XX}'$ is in $[z]$ by the closure property C. We have now proved the first half of Theorem VI with both words maximal omitted.

(*ii*) Conversely, let $[x]$ by any given system of integers x of an algebra a, and $[\mathrm{X}]$ any given system of integers of another algebra A. As explained above, we may regard a and A as the components of a rationally reducible algebra $\mathrm{S} = a + \mathrm{A}$ for which relations (11) hold. To every number x of $[x]$ add every number X of $[\mathrm{X}]$. By the

facts in (i), these sums form a system $[z]$ of numbers of S having properties C, U_1, and R.

Further, let $[x]$ and $[X]$ be maximal systems of a and A, respectively. Then if $[z]$ is not a maximal system of S, it is contained in a larger system $[z']$ of S. By (i), the first components x' of the $z' = x' + X'$ form a system $[x']$ of numbers of a having properties C, U_1, R, and likewise for the second components X'. Either $[x']$ is larger than $[x]$ and contains it, or else $[X']$ is larger than $[X]$, contrary to hypothesis. This proves the last half of Theorem VI.

(iii) Returning to part (i), let $[z]$ be a maximal system of S. Then if $[x]$ is contained in a larger system $[x']$ of a, part (ii) shows that $[x']$ and $[X]$ determine a system $[z']$ of numbers $z' = x' + X$ of S, which have properties C, U_1, and R, such that $[z']$ contains the smaller system $[z]$, whereas $[z]$ was assumed to be a maximal. This completes the proof of the first half of Theorem VI.

THEOREM VII. — *The second part of Theorem VI holds also for systems of integers defined by properties* C, U_1, N *and* M.

We employ the known result (1) that the rank equation of S is equal to the product of the rank equations of the component algebras a and A. From their constant terms, we get

$$N_S(z) = N_a(x) . N_A(X), \tag{12}$$

where each norm is taken with respect to the algebra indicated by the subscript.

Let there be given systems $[x]$ and $[X]$ of integers of a and A, respectively. To every x of $[x]$ add every X of $[X]$; these sums form a set $[z]$ of numbers $z = x + X$ of the direct sum $S = a + A$. Since $N_a(x)$ and $N_A(X)$ are rational integers by assumption N, $N_S(z)$ is a rational

(1) For, if $r(\omega) = 0$ is the rank equation of a and $R(\omega) = 0$ that of A, x and X are both roots of $r(\omega).R(\omega) = 0$. But $z = x + X$ implies $z^k = x^k + X^k$, whence $f(z) = f(x) + f(X)$ for any polynomial f. Hence, z is a root of $r.R = 0$. That it is not the root of an equation of lower degree follows by use of $z = x + 0$ or $z = 0 + X$, since the coefficients of r are independent of the coordinates of X.

integer by (12). Thus $[z]$ has property N and evidently also properties C and U_1.

Suppose that $[z]$ is not a maximal, but is contained in a larger system $[z']$ of numbers of S having properties C, U_1, N. Since $e+0$ and $0+E$ are in $[z]$, they are in $[z']$. Then if $z'=x'+X'$ is any number of $[z']$, $ez'=x'$ and $x'+E$ are in $[z']$. Thus $N_s(x'+E)$ is a rational integer by hypothesis, and is equal to $N_a(x')$ by (12), since $N_A(E)=1$ by § 7 (end). Hence $N_a(x')$ is a rational integer. Hence the x' form a system $[x']$ of numbers of a having properties C, U_1, N. Likewise for the X'. Either $[x']$ is larger than $[x]$ and contains it, or $[X']$ is larger than $[X]$, contrary to the assumption that $[x]$ and $[X]$ are maximal.

From the third and fourth sentences of the preceding paragraph, we obtain the following analogue of the first part of Theorem VI.

THEOREM VIII. — *In a rationally reducible algebra* $S=a+A$, *consider systems of integers having properties* C *and* N *and containing* (1) *the principal units* e *and* E *of* a *and* A. *The first components of the numbers of any* (*maximal*) *system of integers of* S *constitute a* (*maximal*) *system of integers of* a, *and the second components a system of* A.

Let a number $z=x+X$ of a system $[z]$ of integers be a unit, so that there exists a number $z'=x'+X'$ of $[z]$ such that $zz'=\varepsilon=e+E$. Then $xx'=e$, $XX'=E$, and x is a unit of a, and X of A. Conversely, if x and X are units of a and A, then $x+X$ is a unit of $a+A$.

If all integers of norm $\neq 0$ of the component algebras a and A factor into primes uniquely apart from unit factors, the same is true of the integers of $a+A$.

For example, consider the direct sum $(e_0)+(e_1)+(e_2)$:

$$e_i^2=e_i, \qquad e_ie_j=0\,(j\neq i), \qquad 1=e_0+e_1+e_2.$$

The rank and characteristic equations are $\Pi(x_i-\omega)=0$.

---

(1) Without assuming that the systems contain e and E, I have verified the theorem for the three classic reducible algebras in 3 units (§ **11**), the proof being long only for $a=(e_0)+(e_1)$, $b=(e_2)$.

Hence under the new definition by properties C, U_1, R, M the integers are the numbers having rational integral coordinates. The latter are all $\geqq 0$ in the product of x by a suitably chosen unit $\pm e_0 \pm e_1 \pm e_2$. We restrict attention to integers x of norm $x_0x_1x_2 \neq 0$ and having positive integral coordinates. Denote x by (x_0, x_1, x_2). Then $xy = (x_0y_0, x_1y_1, x_2y_2)$. Since

$$(p, q, rs) = (p, q, r)(1, 1, s), \quad (p, q, r) = (p, q, 1)(1, 1, r),$$

one of the coordinates of a prime is a rational prime and the remaining two are unity, and conversely every such number is a prime. Hence if the p_i, q_j, r_k are all rational primes, we have the following unique factorization into primes :

$$(p_1 \dots p_a, q_1 \dots q_b, r_1 \dots r_c) = \prod_{i=1}^{a} (p_i, 1, 1) \cdot \prod_{j=1}^{b} (1, q_j, 1) \cdot \prod_{k=1}^{c} (1, 1, r_k).$$

Given that a number x of an algebra a is an integer if and only if specified coordinates x_i are rational integers and the remaining coordinates x_j are rational, and similarly for another algebra A, then we know from Theorem VI that in the direct sum $S = a + A$ a number $z = x + X$ is an integer if and only if the coordinates x_i and X_i are rational integers and the remaining coordinates x_j and X_j are rational. From $zz' = xx' + XX'$, where $z' = x' + X'$ is a unit, we conclude that an integer z is associated with those and only those integers whose first components are associated with x in a and whose second components are associated with X in A.

If a is one of the two rationally irreducible algebras in two basal units (§ **10**), or one of the three in three basal units (§ **12**), we shall find that an integer x of a, such that $N(x) \neq 0$, is associated with the abridged integer having the same coordinates x_i (which were rational integers in x), but having zeros in place of the coordinates x_j (which were rational in x). Hence for every rationally reducible algebra in 2, 3 or 4 basal units, each integer $z = x + X$, such that $X(z) \neq 0$, is associated with the abridged integer having each x_j and X_j zero, but with no further coordinates zero. Thus the laws of factorization in $a + A$ are the same as in $a' + A'$, where a' denotes the abridgement

of a to the basal units e_i, and A′ the abridgement of A to the units E_i.

But if a is the algebra of matrices (§ 13), further coordinates are zero in the associates of x.

By the results in this section we may read off at once all the properties of the integers of a rationally reducible algebra from those of the components.

10. *Algebras in two units.* — We assume properties C, U_1, N, M. The unique maximal system of integers of the reducible algebra

$$(e_0)+(e_1)\,:\ e_0^2=e_0,\qquad e_0e_1=e_1e_0=0,\qquad e_1^2=e_1,\qquad 1=e_0+e_1,$$

is composed of all the numbers $x_0e_0+x_1e_1$ in which x_0 and x_1 are rational integers. Those of norm $x_0x_1\neq 0$ decompose into primes uniquely apart from unit factors $\pm e_0\pm e_1$ (§ 9). This algebra is another form of that with the basal units 1, e, where $e^2=1$. That with $e^2=0$ was treated in §§ 4, 5. That with $e^2=-1$ has as integers Gauss's complex integers $x+yi$, where x and y are rational integers. For $e^2=\pm 1$, the same results are obtained by Du Pasquier's definition.

11. *Reducible algebras in three units* – Such an algebra is the direct sum of an algebra in two units e_0 and e_1 (§ 10) and the algebra (e_2) in a single unit such that $e_2^2=e_2$. Hence they are $(e_0)+(e_1)+(e_2)$;

$A+(e_2)$,	$A=(e_0, e_1)$,	$e_0^2=e_0$,	$e_0e_1=e_1e_0=e_1$,	$e_1^2=-e_0$;
$B+(e_2)$,	$B=(e_0, e_1)$,	$e_0^2=e_0$,	$e_0e_1=e_1e_0=e_1$,	$e_1^2=0$.

Under the new definition (1) of integers, Theorem VI shows that the integers of the first two algebras are the numbers all of whose coordinates are rational integers, while those of $B+(e_2)$ are Σx_ie_i, where x_1 is rational and x_0 and x_2 are rational integers. For all three algebras, every integer of norm $\neq 0$ decomposes into primes uniquely apart from unit factors.

Only for the first two of these algebras are the integers the same by

(1) Also with R replaced by N, the proof being longer.

Du Pasquier's (1) definition. In $B+(e_2)$ replace e_0 by $1-e_2$; we get his system 3. He found that the most general system of numbers under his definition has the basis 1, αe_1, $\beta e_1+g'e_2$, where α and β are rational, $\frac{\beta}{\alpha}=\frac{g_1}{g}$, while g_1 and g are rational integers, whence no systems is maximal and integers do no exist. Note that the aggregate of the numbers in all of his systems is the above system of integers under the new definition.

Let us ignore the assumption of a maximal, and take as integers the numbers of an arbitrarily chosen one of his systems. Without altering the multiplication table of the units, we may take αe_1 as a new unit e_1, which amounts to taking $\alpha=1$. Then the integers have the basis

$$1=e_0+e_2, \qquad e_1, \qquad g^{-1}g_1e_1+ge_2.$$

Thus g^2e_2 is integral. Write h for g^2+3, and

$$c_j=(3, j, h)=3+je_1+g^2e_2,$$

where (x_0, x_1, x_2) denotes $\Sigma\, x_ie_i$. Since

$$(x_0, x_1, x_2)(y_0, y_1, y_2)=(x_0y_0, x_0y_1+x_1y_0, x_2y_2),$$

we have

$$c_jc_k=c_l^2 \ (\text{if } j+k=2l), \quad c_ju_l=c_{j+3l},$$
$$u_l=(1, l, 1), \qquad u_lu_{-l}=1,$$

whence u_l is a unit. Thus

$$c_1^2=c_0c_2, \qquad c_2^2=c_1c_3=c_1c_0u_1, \qquad c_0^2=c_2c_{-2}=c_2c_1u_{-1},$$

which may be written as

$$c_1c_2=c_0^2u_1, \qquad c_0c_2=c_1^2, \qquad c_0c_1=c_2^2u_{-1},$$

which are exactly of the type (9). The only possible units are $(1, l, \pm 1)$ and their negatives; but $(1, l, -1)$ is not one of our integers, and hence is not a unit, if $|g|>2$. We find that no two of c_0, c_1, c_2 are associated numbers and that each is a prime. Hence (§ 5)

(1) *Bull. Soc. Math. de France*, t. XLVIII, 1920, p. 109-132.

factorization into primes is not unique and cannot be made unique by the introduction of ideals of any kind. This conclusion applies to each of the triply infinite number of systems of integers, one system for each set of values of α, β, g. We saw above how these difficulties disappear under the new definition.

12. *Irreducible Algebras in Three Units.* — We employ assumptions C, U_1, N, M, and find that the resulting integers have also properties U and R. For the algebra

$$T_1: \quad e_0 = 1, \qquad e_1^2 = e_2, \qquad e_1 e_2 = e_2 e_1 = e_2^2 = 0,$$

the rank and characteristic equations are all $(x_0 - \omega)^3 = 0$. The maximal system of integers is composed of all numbers x for which x_0 is a rational integer and x_1, x_2 are rational. If

$$x_0 \neq 0, \qquad x u = x_0, \qquad \text{for} \qquad u = 1 - \frac{x_1}{x_0} e_1 + \frac{x_1^2 - x_0 x_2}{x_0^2} e_2.$$

Hence x is a unit if $x_0 = 1$. Thus u is a unit, and any integer x of norm $x_0^3 \neq 0$ is associated with x_0, and hence decomposes into primes uniquely.

If we replace u by $1 - \frac{x_1}{x_0} e_1 - \frac{x_2}{x_0} e_2$, we see that all the preceding statements hold also for the algebra

$$T_2: \quad e_0 = 1, \qquad e_1^2 = e_1 e_2 = e_2 e_1 = e_2^2 = 0.$$

Finally, consider the algebra

$$T_3: \quad e_0^2 = e_0, \qquad e_1^2 = e_1, \qquad e_1 e_2 = e_2 e_0 = e_2,$$
$$e_0 e_1 = e_1 e_0 = e_0 e_2 = e_2 e_1 = e_2^2 = 0,$$
$$e_0 + e_1 = 1, \qquad R(\omega) = (x_0 - \omega)(x_1 - \omega), \qquad \delta(\omega) = (x_0 - \omega)(x_1 - \omega)^2.$$

Thus

$$N(x) = x_0 x_1, \qquad N(x + 1) = (x_0 + 1)(x_1 + 1).$$

Hence if x is an integer, $x_0 x_1$ and $x_0 + x_1$ are rational integers. Thus the maximal system is composed of all numbers x for which x_0 and x_1 are rational integers, while x_2 is rational.

Denote x by (x_0, x_1, x_2). Then

$$(13) \qquad (x_0, x_1, x_2)(y_0, y_1, y_2) = (x_0 y_0, x_1 y_1, x_1 y_2 + x_2 y_0).$$

For $u_z \equiv (1, 1, z)$, $u_z u_{-z} = 1$, so that u_z is a unit. Now

$$(14) \qquad u_w x u_z = (x_0, x_1, r), \qquad r = x_2 + x_0 w + x_1 z.$$

Hence, unless $x_0 = x_1 = 0$, we can find rational numbers w, z such that $r = 0$. Thus any integer of norm $x_0 x_1 \neq 0$ is associated with $x_0 e_0 + x_1 e_1$. By § **10**, the latter integers decompose into primes uniquely.

These satisfactory results regarding the integers of any of these three algebras T_i are in marked contrast to the results obtained by the definitions of either Hurwitz or Du Pasquier. Then there is no maximal system of integers, while if we select any system we meet essential difficulties.

First, for T_1, which is Du Pasquier's system 4, the most general system of integers was stated by him to have the basis 1, $g^{-1}\alpha^2 e_2$, $\alpha e_1 + \beta e_2$, where α and β are rational and g is a rational integer, so that no system is maximal. Taking

$$E_1 = \alpha e_1 + \beta e_2, \qquad E_2 = E_1^2 = \alpha^2 e_2,$$

we obtain T_1 written in capital letters E_i. Hence the new basis is 1, E_1, tE_2, where $t = \frac{1}{g}$. Write e_j for $3 + jtE_2$. We obtain (9), where now

$$u = 1 + tE_2, \qquad v = 1 - tE_2$$

are units. No two of the primes e_0, e_1, e_2 are associates. Hence (§ 5), decomposition into primes is not unique, and cannot be made unique by the introduction of ideals of any kind.

For T_2, which is Du Pasquier's system 6, the most general system of integers was stated by him to have the basis, 1, αe_1, $\beta e_1 + \gamma e_2$, where α, β, γ are rational, so that no system is maximal. The last two numbers of the basis may be taken as new units E_1, E_2 without disturbing T_2. The further discussion for T_1 applies also here, where $t = 1$.

Du Pasquier's system 5 is

$$e_0 = 1, \qquad e_1^2 = 1, \qquad e_1 e_2 = e_2, \qquad e_2 e_1 = -e_2, \qquad e_2^2 = 0,$$

and his most general system of integers has the basis 1, αe_2, $g\mathrm{E} + \beta e_2$, where α and β are rational, g is a rational integer, and $\mathrm{E} = \frac{1}{2}(1 + e_1)$. Taking the latter as a new unit in place of e_1, and then $\varepsilon = \mathrm{E} + g^{-1}\beta e_2$ in place of E, we get

$$\varepsilon^2 = \varepsilon, \qquad \varepsilon e_2 = e_2, \qquad e_2 \varepsilon = 0, \qquad e_2^2 = 0,$$

and the basis 1, αe_2, $g\varepsilon$. The effect of taking αe_2 as a new e_2 is to take $\alpha = 1$. Finally, we write e_1 for ε, and e_0 for $1 - \varepsilon$, and get algebra T_3 and the basis 1, ge_1, e_2. Hence (p, q, r) is an integer if and only if p, q, r are rational integers such that $p \equiv q \pmod{g}$. By (13),

$$(p, q, r) = (p, 1, z)(1, q, w), \qquad \text{if} \qquad z + w = r.$$

All three numbers are integers if

$$p \equiv q \equiv 1 \pmod{g}.$$

As special cases, or by (14),

$$(p, 1, 0)u_z = (p, 1, z), \qquad u_w(1, q, 0) = (1, q, w).$$

Hence (p, q, r) is the product of units and $(p, 1, 0)$, $(1, q, 0)$. Also, $(p, q, 0)$ is the product of the last two. By (14) for $x = (p, p, 0)$, x is associated with (p, p, r) if and only if $r = p(w + z)$. Hence if $p \equiv 1 \pmod{g}$ and if r is not divisible by p, (p, p, r) and $(p, p, 0)$ are not associated, but have the same factorization apart from units. This property of (p, p, r) holds also for the product of (r, s, l) by (a, b, n), where

$$l = rw + sz, \qquad n = aw_1 + bz_1,$$

if $sn + al$ is not divisible by the greatest common divisor of ra and sb; for example, if r and b have a common factor not a divisor of $as(z + w_1)$.

THÉORÈME IX. — *For the six classic algebras in three units, the integers of the unique system obtained by the new definition have unique factorization into primes and the system is either identical (in the case of two reducible algebras) with the system of integers obtained by Du Pasquier's definition or else is the aggregate of the numbers in his infinitely many systems, no one of which is a maximal nor has satisfactory laws of factorization into primes.*

Thus the new definition succeeds when that of Du Pasquier fails, by causing the proper enlargement of every one of his systems which present serious difficulties to a system having no difficulties.

13. *The Associated Arithmetic.* — In § **12**, we proved that the integers of norm $\neq 0$ of the algebra T_3 in three basal units are associated (by multiplication by units) with the integers $x_0e_0 + x_1e_1$ of the algebra $S = (e_0) + (e_1)$. We shall say that the latter integers form the arithmetic associated with the arithmetic of the integers of T_3. And similarly in general.

14. *Algebras in Four Units.* — We make use of Study's (1) list of the algebras into which any algebra in four units can be transformed by a real linear transformation on the units. Ten of them are rationally reducible, and the properties of their integers are obtained by inspection from the results in § **9**. Thirteen of them are rationally irreducible (although III_6 is algebraically reducible). We shall discuss in §§ **16**, **17** the algebra of real quaternions and the algebra XII_6 obtained from it by an imaginary transformation of the units.

There remain eleven algebras. For each of them, there is no maximal system under the definition of Du Pasquier (2), so that integers do not exist. Under the new definition by properties C, U_1, R, M, the integers are found by a mere inspection of the left-hand characteristic equation $\delta'(\omega) = 0$, while their essential properties are readily

(1) *Monatshefte Math. Physik*, t. 1, 1890, p. 305-309.

(2) *Comptes rendus du Congrès international des Mathématiciens* (Strasbourg, 1920); Toulouse, 1921, p. 164-175.

found. The notation V (13) means that the algebra is numbered V in Study's list and is system 13 in Du Pasquier's list. The notation $[x_0, x_1]$ means that $\Sigma x_i e_i$ is an integer (under the new definition) if and only if x_0 and x_1 are rational integers and the remaining coordinates x_2 and x_3 are rational.

For algebras V (13), IX (17), X (18), XI (19), XIV (22), and XVI (29), we have

$$\delta'(\omega) = (x_0 - \omega)^2 \qquad \text{and} \qquad [x_0].$$

The associated arithmetic is that of rational integers x_0.

For III_b (11) and XIII (20),

$$\delta'(\omega) = [(x_0 - \omega)^2 + x_1^2]^2 \qquad \text{and} \qquad [x_0, x_1].$$

The associated arithmetic is that of ordinary complex integers $x_0 + x_1 i$.

For VII (15), we employ new units

$$\mathrm{E}_0 = \frac{1}{2}(1 - e_1), \qquad \mathrm{E}_1 = \frac{1}{2}(1 + e_1), \; e_2, \; e_3,$$

and get

$$\mathrm{E}_0^2 = \mathrm{E}_0, \quad \mathrm{E}_1^2 = \mathrm{E}_1, \quad \mathrm{E}_1 e_2 = e_2, \quad \mathrm{E}_1 e_3 = e_3, \quad e_2 \mathrm{E}_0 = e_2, \quad e_3 \mathrm{E}_1 = e_3,$$

all further products being zero. Then

$$\delta'(\omega) = (x_0 - \omega)^2 (x_1 - \omega)^2, \qquad [x_0, x_1].$$

For XIII_b (21), we employ as units the preceding E_0, E_1, and

$$\mathrm{E}_2 = \frac{1}{2}(e_2 - e_3), \qquad \mathrm{E}_3 = \frac{1}{2}(e_2 + e_3),$$

and get

$$\mathrm{E}_0^2 = \mathrm{E}_0, \quad \mathrm{E}_1^2 = \mathrm{E}_1, \quad \mathrm{E}_0 \mathrm{E}_2 = \mathrm{E}_2, \quad \mathrm{E}_1 \mathrm{E}_3 = \mathrm{E}_3, \quad \mathrm{E}_2 \mathrm{E}_1 = \mathrm{E}_2, \quad \mathrm{E}_3 \mathrm{E}_0 = \mathrm{E}_3,$$

all further products being zero. Then

$$\delta'(\omega) = (x_0 - \omega)^2 (x_1 - \omega)^2, \qquad [x_0, x_1].$$

For XV (23), we employ new units E_0, E_1, e_2, e_3, and get

$$E_0^2 = E_0, \quad E_1^2 = E_1, \quad E_1 e_2 = e_2, \quad E_1 e_3 = e_3, \quad e_2 E_0 = e_2, \quad e_3 E_0 = e_3,$$

all further products being zero. Then

$$\delta'(\omega) = (x_0 - \omega)^3 (x_1 - \omega), \qquad [x_0, x_1].$$

For the last three algebras the associated arithmetic is that of $(E_0) + (E_1)$, and hence is that of pairs of rational integers.

13. *Algebra and Arithmetic of Square Matrices.* — It was shown in § **2**, that all n-rowed square matrices with rational elements form a linear associative algebra in n^2 basal units. We shall now investigate maximal systems of such matrices having properties C, U_1, R.

The system S composed of all matrices whose elements are all rational integers has the properties C, U_1, R by § **2**. We shall now prove that it is a maximal. Suppose that S is contained in a larger system L having those properties. Thus L contains a matrix m whose elements are fractions having a least common denominator d, where $d > 1$. By a theorem due to H. J. S. Smith (1), we can find square matrices p and q having rational integral elements of determinant unity such that $pmq = \delta$, where δ is a diagonal matrix all of whose elements outside the main diagonal are zero, while those in the diagonal are $\frac{d_1}{d}, \cdots, \frac{d_r}{d}, 0, \ldots, 0$ where r is the rank of m, the d_i are rational integers which are positive with the exception (when $r = n$) of d_n, whose sign is that of $|m|$, and d_i is a divisor of d_{i+1}. Any common divisor of d_1 and d would divide every d_i and hence divide the numerator of every element of m, contrary to the definition of d. Hence d_1 and d are relatively prime.

Since matrices p and q belong to S and hence to L, the product $pmq = \delta$ belongs to L by property C. We shall prove that δ does not

(1) *Phil. Trans. London*, t. **151**, 1861, p. 293; *Coll. Math. Papers*, t. I, p. 367; *Cf.* BACHMANN, *Arith. Quadr. Formen*, t. IV, 1898, p. 294; BÔCHER, *Introduction to Higher Algebra*, 1907, p. 264-267. *We first remove the rational factor* $\frac{1}{d}$ *from m and place it in front of p.*

have property R. If $R(\omega)=0$ denotes the rank equation of the general n-rowed square matrix x, we obtain $R(\omega)$ by subtracting ω from each diagonal term of x. This classic theorem (1) was verified in § 2 for $n=2$.

For δ the rank equation becomes

$$\Pi\left(\frac{d_i}{d}-\omega\right)=0.$$

Its coefficients are rational integers by the assumption R. Hence its roots are rational integers, whereas $\frac{d_1}{d}$ is not integral. In view of this contradiction, our system S is a maximal.

But this systems S is not the only maximal system. If Σ is any system of matrices with rational elements having properties C, U_1, R, M, and if t is any matrix such that both t and t^{-1} transform every matrix with rational elements into one with rational elements, we readily prove that t transforms Σ into a system of matrices having the same four properties. The conditions on t are evidently satisfied if (2) the elements of t are all products of rational numbers by the same number. This common factor may be omitted since it cancels from $t^{-1}mt$. Hence if we transform our maximal system S by any matrix having rational elements of determinant not zero, we obtain a maximal system of matrices with rational elements having properties C, U_1, R. We obtain in this way an infinitude of distinct maximal systems. For, if we employ as t the diagonal matrix whose diagonal

---

(1) Let e_{ij} denote the matrix whose elements are all zero except that in the ith row and jth column, which is unity. Let x_{ij} be the element in the ith row and jth column of x. Then

$$x\,e_{ij}=x_{1i}e_{1j}+x_{2i}e_{2j}+\ldots+x_{ni}e_{nj}.$$

Transposing and keeping j fixed, but taking $i=1,\ldots,n$, we have n equations the matrix of whose coefficients is derived from (x_{ij}) by subtracting $\omega=x$ from each diagonal term. The determinant D of this matrix is known to be an irreducible polynomial, when the x_{ij} are arbitrary. Thus the rank equation is $D=0$.

(2) And only then for 2-rowed square matrices.

elements are $k_1, \ldots, k_n$, we see that t transforms (c_{ij}) into a matrix having $c_{ij}\frac{k_j}{k_i}$ as the element in the ith row and jth column. Since the $k's$ are arbitrary rational numbers $\neq 0$, we may take $k_1 = 1$ without loss of generality. For example, if $n = 2$,

$$t = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}, \qquad t^{-1}\begin{pmatrix} x_0 & x_2 \\ x_1 & x_3 \end{pmatrix} t = \begin{pmatrix} x_0 & kx_2 \\ k^{-1}x_1 & x_3 \end{pmatrix}.$$

If in the final matrix we let x_0, x_1, x_2, x_3 range independently over all rational integers, we obtain a system S_k which is identical with S_l if and only if $k = \pm l$.

THEOREM X. — *There exist infinitely many maximal systems of n-rowed square matrices with rational elements having properties* C, U_1, R. *One such maximal system is composed of all the matrices with rational integral elements.*

Whether or not there exist maximal systems, not derivable from S by transformation, is not decided here and a decision is immaterial for our theory. In any case we would make an arbitrary selection of one maximal system and call its matrices integral. Fortunately the selection of S itself is wholly satisfactory, since the matrices of S have unique factorization into primes, as we proceed to prove.

Nothing is simpler (1) than the arithmetic of all matrices m with rational integral elements. Any such matrix u is a unit if and only if its determinant is ± 1; for, its adjoint matrix u' has rational integral elements, and $uu' = u'u = 1$. By the above discussion (with now $d = 1$), there exist units p and q such that $pmq \equiv \delta$, where δ is a diagonal matrix whose diagonal terms d_i are all positive integers or zero. Thus matrix m is associated with such a diagonal matrix δ. Hence unique factorization of matrices of non-vanishing determinants into prime matrices will follow if proved for diagonal matrices all of whose diagonal elements are positive rational integers. But this was proved for diagonal matrices near the end of § 9 (for the typical case $n = 3$),

(1) In spite of the very long discussion by ideals, etc., by DU PASQUIER in his Zürich thesis (*Vierteljahrsschrift Naturf. Gesell. Zürich*, t. 51, 1906, p. 55-129; t. 52, 1907, p, 243-248).

since the product of two diagonal matrices $(d_1, \ldots, d_n)$ and $(\delta_1, \ldots, \delta_n)$ is $(d_1\delta_1, \ldots, d_n\delta_n)$.

Or, if we prefer, we may write $\delta = d_1 e_1 + d_2 e_2 + d_3 e_3$, where

$$e_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad e_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad e_3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$e_i^2 = e_i, \qquad e_i e_j = 0 \quad (j \neq i), \qquad e_1 + e_2 + e_3 = 1,$$

which are the basal units of the algebra employed in § 9. But there are now infinitely many units, while there were only eight.

THEOREM XI. — *The arithmetic of all n-rowed square matrices with rational integral elements is associated with the arithmetic of the direct sum* $(e_1) + (e_2) + \ldots + (e_n)$, *and has unique factorization into primes.*

16. *The Property* U. — An equivalent statement of the first theorem in § 15 is that the system S of n-rowed square matrices with rational integral elements is the unique maximal system of all matrices with rational elements having properties C, R, and U, where U states that all the basal units e_{ij} occur in the system.

The initial result in § 15 shows also that S is the unique maximal system of matrices with rational elements having properties B, C, U, so that the matrices (of S) having rational integral elements are the integral matrices according to Hurwitz's definition (§ 4). For, if S is not a maximal system, we proved that it contains the diagonal matrix δ, and hence by property C also every power of δ. There is no finite basis (i. e., property B fails), since δ^n is not a linear function of the lower powers of δ with rational integral coefficients c_i. For, $\left(\frac{d_1}{d}\right)^n$ would then be equal to $\Sigma c_i \left(\frac{d_1}{d}\right)^i$ which is the quotient of a rational integer by d^{n-1}, whereas $\frac{d_1^n}{d}$ is not a rational integer.

Under Du Pasquier's (1) definition by properties B, C, U_1, M, a

(1) *Vierteljahrsschrift Naturf. Gesell. Zürich*, t. 51, 1906, p. 116-148; quoted in *l'Enseignement math.*, t. 18, 1916, p. 201-260.

long computation led him to all of the ∞^6 maximal systems of 2-rowed square matrices with rational elements, since the four basal matrices involve six arbitrary rational integers.

Hence, if we assume C and either B or R, we find a unique maximal system of matrices or an infinitude of maximal systems, according as we assume also U or U_1. However, we have an excellent reason for deciding not to assume U, in spite of its having led us to a simpler conclusion than does U_1. In fact, property U is not always invariant under a linear tsansformation of the basal units with rational (1) coefficients, while the properties U_1, B, R, N, C, M are always all invariant. Expressed otherwise, a maximal system of integers containing all the basal units may transform into a system not containing all the new basal units.

Light is thrown on this question by the algebra derived from the algebra (7) of real quaternions by taking

$$E_3 = i\sqrt{-1}, \qquad E_2 = j\sqrt{-1}, \qquad E_1 = -k.$$

Thus

$$(15) \qquad \begin{gathered} E_1^2 = -1, \qquad E_2^2 = E_3^2 = +1, \qquad E_1E_2 = -E_2E_1 = E_3, \\ E_1E_3 = -E_3E_1 = -E_2, \qquad E_2E_3 = -E_3E_2 = -E_1. \end{gathered}$$

Call x and x' conjugates if

$$x = x_0 + \Sigma x_i E_i, \qquad x' = x_0 - \Sigma x_i E_i.$$

Then

$$(16) \qquad N(x) = xx' = x'x = x_0^2 + x_1^2 - x_2^2 - x_3^2.$$

Consider maximal systems of integers x with rational coordinates having properties C, U, N. Let x be an integer, so that $N(x)$ and $N(x+1)$ are rational integers. By their difference, the double of the

(1) If the coefficients are rational integers of determinant ± 1 (the case of arithmetical equivalence), property U is invariant. When that property is postulated, we should not confine our investigation of all possible arithmetics to a study of a complete list of algebras no two of which are equivalent under transformations of the units with rational coefficients, but study the much larger list of algebras no two of which are equivalent under transformations with rational integral coefficients.

« absolute term » x_0 of x is a rational integer. By property C, $E_1 x$, $E_2 x$, $E_3 x$ are integers; their absolute terms are $-x_1, x_2, x_3$. Hence each $2x_i$ is a rational integer. Evidently $x_i = X_i + a_i$, where X_i is a rational integer and $a_i = 0$ or $\frac{1}{2}$. Then $x = X + a$, where X is an integer by property U. By C, $a = x - X$ is an integer. Write

$$a = \tfrac{1}{2}(A_0 + \Sigma A_i E_i), \qquad A_j = 0 \text{ or } 1.$$

By $N(a)$, $A_0^2 + A_1^2$ and $A_2^2 + A_3^2$ differ by a multiple of 4, while each sum is 0, 1, or 2; hence they are equal. Thus the only sets of values are

$$(17) \qquad \begin{aligned} (A_0, A_1, A_2, A_3) = {} & (0,0,0,0), \quad (0,1,1,0), \\ & (0,1,0,1), \quad (1,0,1,0), \\ & (1,0,0,1), \quad (1,1,1,1). \end{aligned}$$

An evident system I of integers satisfying our assumptions is composed of all the numbers X whose four coordinates are all rational integers. We shall examine the systems obtained by annexing to I one or more of the five numbers $a \neq 0$ corresponding to the sets (17) other than the first set.

First, annex the a corresponding to either the second or fifth set (17), viz.,

$$(18) \qquad e_1 = \tfrac{1}{2}(E_1 + E_2), \qquad e_3 = \tfrac{1}{2}(1 + E_3).$$

Since $e_1 E_2 = e_3$, $e_3 E_2 = e_1$, the enlarged system contains both e_1 and e_3 by property C. If we annex also the a corresponding to either the third or fourth set (17), viz.,

$$(19) \qquad e_1' = \tfrac{1}{2}(E_1 + E_3), \qquad e_3' = \tfrac{1}{2}(1 + E_2),$$

we annex both, since $E_3 e_1' = e_3'$, $E_3 e_3' = e_1'$.

But

$$e_3' + e_1 - E_2 = \tfrac{1}{2}(1 + E_1)$$

has the norm $\frac{1}{2}$, and we do not obtain a system satisfying our assumptions. Hence the only possible maximal systems are I, the system S_1 obtained by annexing the pair (18) to I, and the system S_2 obtained by annexing the pair (19) to I. For, the a corresponding to the sixth set (17) is equal to $e_1 + e_3$ and to $e'_1 + e'_3$ and hence is in both S_1 and S_2.

The system S_1 contains (18) and all the E_i, and hence also

$$(20) \qquad e_0 = \frac{1}{2}(1 - E_3) = e_3 - E_3, \qquad e_2 = \frac{1}{2}(E_2 - E_1) = e_1 - E_1.$$

Conversely, from (18) and (20) we obtain by additions and subtractions the three E_i and 1. The multiplication table of the e_i is given by (3). Hence the system S_1 is composed of the linear combinations of the e_i with rational integral coefficients, and has properties C, U, M. While we may deduce the new norm from (16) by expressing the old coordinates x_i in terms of the new, we obtain it directly from the next remark. The relations (3) are all satisfied by the matrices (1) (1). Then $x = \Sigma x_i e_i$ becomes the matrix (2), whose determinant $x_0 x_3 - x_1 x_2$ is $N(x)$ by (4), and is a rational integer when x is in S_1. Thus S_1 has the properties C, U, N, M.

Also S_2 has the same properties since it is derived from S_1 by interchanging e_2 and e_3 and changing the sign of e_1, and this transformation of units leaves unaltered the multiplication table (3).

THEOREM XII. — *Algebra* (15) *contains exactly two maximal sets* S_1 *and* S_2 *of integers having properties* C, U, N, *and each is equivalent* (*under rational transformation of the units*) *to the arithmetic of* 2*-rowed square matrices with rational integral elements.*

We proved above that the algebra of matrices with rational elements has a single maximal set S of integers having properties C, U, R (and hence N). When we transform the algebra (15) into the

(1) But by no other 2-rowed square matrices apart from the interchange of those corresponding to e_0 and e_3 as well as those corresponding to e_1 and e_2, such interchanges leaving unaltered the set of equations (3).

matric algebra by the rational transformation (18) and (20), we thereby trausform S_1 into S, and S_2 into the system of matrices

$$(21) \qquad \begin{pmatrix} x_0 + x_1 + \frac{1}{2}x_2 + 2x_3, & x_1 + \frac{1}{2}x_2 \\ \frac{1}{2}x_2, & x + \frac{1}{2}x_2 \end{pmatrix},$$

in which x_0, x_1, x_2, x_3 range independently over all rational integers. This system of matrices (21) does not contain e_0. It has properties C, N, M, U_1, but not U.

In view of Theorem X and our transformation of units, algebra (15) has an infinitude of maximal systems having properties C, U_1, R, and hence composed of integers according to the definition adopted in this memoir. By the formula above Theorem X, such systems include that formed of the linear combinations of 1, $k^{-1}e_1$, kE_2, e_3 with rational integral coefficients, where k is any fixed rational number $\neq 0$.

The value of the provisional assumption U lies in its help in detecting at least one maximal system according to our definition (with U_1 and not U), and moreover one having the pleasing property U, as well as uniqueness of factorization into primes, which recommend its selection in preference to all other maximal systems as the system of integers of the algebra in its initial units.

17. *Integral Quaternions.* — If x is in a maximal system of quaternions with rational coordinates having properties C, U, N, we find at once that only the first and last cases (17) exist, so that the four coordinates of x are either all rational integers or all halves of odd integers. Hence x is a linear combination of

$$(22) \qquad \rho = \frac{1}{2}(1 + i + j + k), \qquad i, j, k,$$

with rational integral coefficients. The squares and products of the numbers (22) are equal to such linear combinations of (22).

THEOREM XIII. — *The unique maximal system of quaternions with rational coordinates having properties* C, U, N *is composed of all quaternions whose four coordinates are either all rational integers or all halves of odd integers.*

A like conclusion was reached by Hurwitz for quaternions having properties C, D, B, as required by his definition of integers. His proof is much longer and more difficult then the above proof.

According to the definition of integer in this memoir, there is at least one maximal system of integral quaternions, viz., the system of Hurwitz, and its numbers would naturally be chosen as our integral quaternions in view of their admirable properties as to factorization into prime quaternions.

18. *General Theory.* — We shall now give a complete theory of integers in any linear associative algebra, the coordinates of whose numbers range over all complex numbers. There are two categories of such algebras. For any algebra of the first category we may introduce new units $\varepsilon_1, \ldots, \varepsilon_h, \eta_1, \ldots, \eta_k$, such that (1)

$$\varepsilon_i^2 = \varepsilon_i, \qquad \varepsilon_i \eta_\rho = \eta_\rho, \qquad \eta_\rho \varepsilon_j = \eta_\rho, \qquad \eta_\rho \eta_\sigma = \Sigma \gamma_{\rho\sigma\tau} \eta_\tau,$$

while all further products are zero. Here η_ρ, η_σ and η_τ are of characters (i, j), (j, l) and (i, l); while in the summation, $\tau > \rho$, $\tau > \sigma$. For the general number

$$z = x_1 \varepsilon_1 + \ldots + x_h \varepsilon_h + y_1 \eta_1 + \ldots + y_k \eta_k,$$

we have $\delta(\omega) = \Pi(x_i - \omega)^{m_i}$. Since $R(\omega)$ is a divisor of the latter, the maximal system of integers is composed of all the numbers z in which the x_i are rational integers and the y_j are rational. We readily prove that $u = 1 + \Sigma a_j \eta_j$ is a unit if the a_j are any rational numbers. For,

$$u(1 - a_1 \eta_1) = 1 - a_1^2 \eta_1^2 + l_2 = 1 + a_{12} \eta_2 + l_3,$$

where l_i is a linear function of $\eta_i, \eta_{i+1}, \ldots$, with rational coefficients. Similarly,

$$(1 + a_{12} \eta_2 + l_3)(1 - a_{12} \eta_2) = 1 - a_{12}^2 \eta_2^2 + l_3' = 1 + a_{13} \eta_3 + l_4,$$
$$(1 + a_{13} \eta_3 + l_4)(1 - a_{13} \eta_3) = 1 + a_{14} \eta_4 + l_5.$$

---

(1) E. CARTAN, *Annales de la Fac. Sc. de Toulouse*, t. 12, 1898, B. 33; DICKSON, *Linear Algebras*, p. 44.

We finally reach a product equal to 1. Hence

$$uv=1, \qquad v=(1-a_1\eta_1)(1-a_{12}\eta_2)(1-a_{13}\eta_3)\ldots=1+\Sigma b_j\eta_j,$$

where each b_j is rational. Thus v is an integer, and u and v are units.

If $x_1, \ldots, x_h$ are given rational integers each $\neq 0$ and $y_1, \ldots, y_k$ are any rational numbers, $z=\Sigma x_i\varepsilon_i+\Sigma y_\rho\eta_\rho$ is associated with $\Sigma x_i\varepsilon_i$, *i. e.*, there exists a unit v such that $zv=\Sigma x_i\varepsilon_i$. For, if u is the unit

$$u=1+\Sigma x_i^{-1}y_\rho\eta_\rho,$$

$\Sigma x_i\varepsilon_i u=z$. As shown above, there exists a unit v such that $uv=1$. Hence *the arithmetic of any algebra of the first category is associated* (§ **13**) *with the arithmetic of the algebra which is the direct sum* $(\varepsilon_1)+\ldots+(\varepsilon_h)$.

The units of an algebra of the second category (1) fall into sets, each corresponding to a unit of an algebra of the first category, and having the multiplication table

$$e^i_{\alpha\beta}e^i_{\beta\gamma}=e^i_{\alpha\gamma}, \qquad e^i_{\alpha\beta}\eta^\rho_{\beta\gamma}=\eta^\rho_{\alpha\gamma}, \qquad \eta^\rho_{\beta\gamma}e^i_{\gamma\delta}=\eta^\rho_{\beta\delta}, \qquad \eta^\rho_{\alpha\beta}\eta^\sigma_{\beta\gamma}=\sum_\tau \gamma_{\rho\sigma\tau}\eta^\tau_{\alpha\gamma}$$
$$(\tau>\rho,\ \tau>\sigma),$$

where the superscripts do not denote powers, the γ's are constants, and all further products of the e and η are zero.

Consider any number z of the algebra. Then

$$z=x+y, \qquad x=\sum_{k,\lambda,\mu} x^k_{\lambda\mu}e^k_{\lambda\mu}, \qquad y=\sum_{\rho,\lambda,\beta} y^\rho_{\lambda\beta}\eta^\rho_{\lambda\beta}.$$

The right-hand characteristic determinant $\delta(\omega)$ of z is known to be a product of powers of the determinants

$$D_i(\omega)=\begin{vmatrix} x^i_{11}-\omega & x^i_{12} & \ldots & x^i_{1p_i} \\ \ldots\ldots & \ldots & \ldots & \ldots\ldots \\ x^i_{p_i1} & x^i_{p_i2} & \ldots & x^i_{p_ip_i}-\omega \end{vmatrix},$$

which involve no coordinate of y. Hence z is an integer if and only

(1) CARTAN, *loc. cit.*, B. 51; DICKSON, *loc. cit.*, p. 54.

if x is an integer, the coordinates of y being arbitrary rational numbers. Consider

$$u = 1 + \sum_{\rho, \alpha, \beta} a^{\rho}_{\alpha\beta} \eta^{\rho}_{\alpha\beta}.$$

Then

$$xu = x + \sum_{\lambda, \rho, \alpha, \beta} x^{\lambda}_{\lambda\alpha} a^{\rho}_{\alpha\beta} \eta^{\rho}_{\lambda\beta}$$

will reduce to $x + y$ if and only if

$$\sum_{\alpha} x^{\lambda}_{\lambda\alpha} a^{\rho}_{\alpha\beta} = y^{\rho}_{\lambda\beta} \qquad \text{(for all } \rho, \lambda, \beta).$$

Here α and λ each take the same values $1, \ldots, p_i$. The determinant of the coefficients of $a^{\rho}_{1\beta}, \ldots, a^{\rho}_{p_i\beta}$ is $D_i(0)$, which is not zero if $N(x) \neq 0$. Then the equations uniquely determine the a.

The proof that u is a unit is similar to that above:

$$u\left(1 - \sum_{\alpha, \beta} a^{1}_{\alpha\beta} \eta^{1}_{\alpha\beta}\right) = 1 + \sum_{\alpha, \beta}^{\rho \geq 2} b^{\rho}_{\alpha\beta} \eta^{\rho}_{\alpha\beta},$$

whose product by

$$1 - \sum b^{2}_{\alpha\beta} \eta^{2}_{\alpha\beta}$$

is

$$1 + \sum_{\alpha, \beta}^{\rho \geq 3} c^{\rho}_{\alpha\beta} \eta^{\rho}_{\alpha\beta},$$

$$\ldots\ldots \quad \ldots\ldots$$

We finally reach a product equal to 1. Hence $uv = 1$ for

$$v = \left(1 - \sum_{\alpha, \beta} a^{1}_{\alpha\beta} \eta^{1}_{\alpha\beta}\right)\left(1 - \sum_{\alpha, \beta} b^{2}_{\alpha\beta} \eta^{2}_{\alpha\beta}\right)\left(1 - \sum_{\alpha, \beta} c^{3}_{\alpha\beta} \rho^{3}_{\alpha\beta}\right)\ldots = 1 + \sum_{\rho, \alpha, \beta} g^{\rho}_{\alpha\beta} \eta^{\rho}_{\alpha\beta},$$

where the g are rational. Thus v is an integer, and u and v are units. Then $xu = z$ gives $zv = x$. Thus every number z whose norm is not zero is associated with its x component.

These x components are known to be the numbers of the algebra which is the direct sum of several general matric algebras (§ 15).

Applying Theorems VI and XI, and noting that our conclusion applies also to algebras of the first category, we obtain

THEOREM XIV. — *The arithmetic of any linear associative algebra the coordinates of whose numbers range over all complex numbers is associated with the arithmetic of a direct sum of algebras each with a single unit. Any number whose norm is not zero decomposes into primes uniquely.*

We therefore obtain only trivial arithmetics from algebras the coordinates of whose numbers range over the field of all complex numbers. If we restrict the coordinates and the coefficients of the transformations of the units to the field of real numbers, we obtain algebras in addition to those just investigated (for example, real quaternions) and now obtain arithmetics which are not trivial. If we employ the field of rational numbers, we obtain still further algebras and a rich variety of arithmetics, which will form the subject of the book cited in § **20**.

19. *The Integers of Cayley's Algebra.* — We employ the four quaternion units $1, i, j, k$ as well as the new units

$$e = e_4, \qquad ie = e_5, \qquad je = e_6, \qquad ke = e_7.$$

Any linear combination of these 8 basal units may be designated by $x = q + Qe$, where

$$(23) \qquad q = x_0 + x_1 i + x_2 j + x_3 k, \qquad Q = x_4 + x_5 i + x_6 j + x_7 k$$

are quaternions. Instead of employing Cayley's multiplication table for these 8 units, it is far simpler to use the condensed law of multiplication

$$(24) \qquad (q + Qe)(r + Re) = t + Te, \qquad t \equiv qr - R'Q, \qquad T \equiv Rq + Qr',$$

found by the writer (1), who also discovered that both right-hand and left-hand division, except by zero, is always uniquely possible.

(1) DICKSON, *Linear Algebras*, p. 15.

Here r' denotes the quaternion conjugate to r (§ 5). Unlike all the earlier algebras in this memoir, the present algebras is not associative.

As a special case of (24), the product of x by $q'-Qe$ in either order is

$$qq'+QQ'=x_0^2+\ldots+x_7^2,$$

which is the norm $N(x)$ of x, since it is the constant term of the quadratic equation satisfied by x. We have

$$N(xy)=N(x)N(y).$$

We shall determine all maximal sets of integers x with rational coordinates having properties C, U, N.

With x, also $x+1, x+i, \ldots, x+e_7$, are integers. From their norms we subtract $N(x)$ and conclude that $2x_0+1, \ldots, 2x_7+1$, are all rational integers. Hence

$$x_t=\tfrac{1}{2}X_t \qquad (t=0,\ldots,7),$$

where each X_t is a rational integer. Since $N(x)$ is a rational integer, ΣX_t^2 is divisible by 4. According as X_t is even or odd, X_t^2 has the remainder 0 or 1 when divided by 4. Hence the number of odd X_t is 0, 4 or 8. In the first and third cases, q and Q are Hurwitz's integral quaternions. By annexing e to all such quaternions, we obtain a system H containing our x, and forming a part of the larger system (30) obtained below.

Hence let exactly four of the eight coordinates of $x=q+Qe$ be halves of odd integers, the four not being those of q, nor those of Q (otherwise x is in H). If three of those four are in one of q, Q, and hence the fourth in the other, then, by employing xe instead of x if necessary, we may assume that three are in Q and one in q. After multiplying x on the left by $1, i, j$, or k, we may assume that x_0 is half an odd integer, while x_1, x_2, x_3 are rational integers. Subtracting from x a quaternion with rational integral coordinates, we get $\frac{1}{2}+Q_1e$. Its product by $1+i$ is $\frac{1}{2}(1+i)+Q_1e$, which falls under the next case.

Next, let exactly two of the coordinates of q and two of those of Q be halves of odd integers. After multiplying x on the left by $1, i, j,$ or k, we may take x_0 as half an odd integer. Since the multiplication table (7) of quaternions is unaltered by a cyclic permutation of i, j, k, we may treat only one of three analogous cases (and at the end of our discussion draw similar conclusions for the two omitted cases), and hence assume here that x_1 is half an odd integer, while x_2 and x_3 are rational integers. Then by subtracting a quaternion with rational integral coordinates, we get $q = \frac{1}{2}(1 + i)$. Since

$$iq + 1 = iq + 1 + (Qi)e, \qquad iq + 1 = q,$$

we may replace Q by Qi without disturbing q. Hence if either x_1 or x_5 of Q is half an odd integer, we may take x_1 to be that one. After subtracting Re, where R is a quaternion with rational integral coordinates, we have the cases

$$(25) \qquad Q = \tfrac{1}{2}(1+i), \quad \tfrac{1}{2}(1+j), \quad \tfrac{1}{2}(1+k), \quad \tfrac{1}{2}(j+k).$$

We shall reduce these cases to the second, for which x is

$$(26) \qquad Z = \tfrac{1}{2}(1+i) + \tfrac{1}{2}(1+j)e,$$

whence

$$(1+j)Z = \tfrac{1}{2}(1+i+j-k) + je,$$

so that the set contains

$$(27) \qquad \rho = \tfrac{1}{2}(1+i+j+k),$$

and hence all of Hurwitz's integral quaternions. We shall assume that the latter occur in our set in all cases.

For the first case (25), x is

$$L = \tfrac{1}{2}(1+i) + \tfrac{1}{2}(1+i)e.$$

Then

$$(\rho e)\mathrm{L} = \tfrac{1}{2}(-1-j)+\tfrac{1}{2}(1+k)e.$$

Apply the cyclic permutation (ikj) and to the result add $1+i$; we get Z. In the third case (25), replace j by $-k$, and k by j (so that the multiplication table of quaternion units is unaltered); we get the second case (25). In the fourth case (25), we add

$$\tfrac{1}{2}(1+i-j-k)e,$$

which belongs to our set by hypothesis, and get the first case (25). Hence all cases have now been reduced to (26).

Since the set contains Z, it contains

$$e\mathrm{Z} = w \equiv \tfrac{1}{2}(-1+j)+\tfrac{1}{2}(1-i)e, \qquad (\rho e)\mathrm{Z} = v \equiv \tfrac{1}{2}(-1-k)+\tfrac{1}{2}(1+k)e.$$

Adding $1+ie$ to w, and $1+k$ to v, we get

$$(28) \qquad \mathrm{W} = \tfrac{1}{2}(1+j)+\tfrac{1}{2}(1+i)e, \qquad \mathrm{V} = \tfrac{1}{2}(1+k)+\tfrac{1}{2}(1+k)e.$$

The followings 8 numbers

$$(29) \qquad i,\ j,\ k,\ \rho,\ e,\ \mathrm{W},\ \mathrm{Z},\ \mathrm{V}$$

are evidently linearly independent. In view of $2\mathrm{W}$, $2\mathrm{Z}$, $2\mathrm{V}$, 2ρ, we may express ie, je, ke, 1 as linear functions of the numbers (29) with rational integral coefficients. Note also that

$$\rho e = \mathrm{Z}-\mathrm{W}+\mathrm{V}+ie-1-i-k.$$

Hence all of the numbers previously mentioned as belonging to our system of integers are linear functions of the eight in (29) with rational integral coefficients. It can be verified that this is true also of the product of any two of the numbers (29). Hence the system of numbers

$$(30) \qquad \left\{ \begin{array}{l} x = x_0\rho + x_1 i + x_2 j + x_3 k + x_4 e + x_5 \mathrm{W} + x_6 \mathrm{Z} + x_7 \mathrm{V} \\ (x_0, \ldots, x_7 \text{ rational integers}) \end{array} \right.$$

has the properties U and C. It has the property N, since

$$(31)\quad x=\tfrac{1}{2}(x_0+x_5+x_6+x_7)+\left(x_1+\tfrac{1}{2}x_0+\tfrac{1}{2}x_6\right)i+\left(x_2+\tfrac{1}{2}x_0+\tfrac{1}{2}x_5\right)j$$
$$+\left(x_3+\tfrac{1}{2}x_0+\tfrac{1}{2}x_7\right)k+\left[x_4+\tfrac{1}{2}(x_5+x_6+x_7)\right]e$$
$$+\tfrac{1}{2}x_5ie+\tfrac{1}{2}x_6je+\tfrac{1}{2}x_7ke,$$

the sum of the squares of whose eight components is the rational integer

$$\mathrm{N}(x)=x_0^2+\ldots+x_7^2+x_0(x_1+x_2+x_3+x_5+x_6+x_7)$$
$$+x_4(x_5+x_6+x_7)+x_1x_6+x_2x_5+x_3x_7+x_5x_6+x_5x_7+x_6x_7.$$

If we make any enlargement of this system (30), we obtain a system not having properties U, C, N. For, let us annex $u=q+\mathrm{Q}e$, four of whose coordinates are rational integers, while four are the halves of odd integers. First, let two of the latter be coordinates of q and two of Q. This will be true also of u, iu, ju, ku, in one of which x_4 is half an odd integer. After subtracting $\mathrm{R}e$, where R has rational coordinates, we may take

$$\mathrm{Q}=\tfrac{1}{2}(1+i),\qquad \tfrac{1}{2}(1+j),\qquad \text{or}\qquad \tfrac{1}{2}(1+k).$$

In the respective cases, we subtract W, Z, or V from u and get a number lacking e and hence a quaternion r. If r is in Hurwitz's arithmetic, r is in our system (30), and we have caused no enlargement by annexing u. Hence r is not in Hurwitz's arithmetic and therefore enlarges it to a system of quaternions not having properties U, C, N (§ **17**).

Finally, let exactly three of the coordinates of Q and one of q be halves of odd integers (the reverse case reducing to this after multiplication by e). As above we may assume that $q=\frac{1}{2}$, while three of the coordinates of Q are $\frac{1}{2}$ and the fourth is zero. Subtracting ρe, we get $\frac{1}{2}-\frac{1}{2}le$, where $l=1, i, j$, or k. But the norm is now $\frac{1}{2}$ and not a rational integer. Hence our system is a maximal.

THEOREM XV. — *The only maximal systems of integers of Cayley's algebra having properties* C, U, N *are* (30) *and the two systems obtained from it by cyclic permutations of* i, j, k.

For the system (30) there are exactly 240 units :

$$\pm 1, \quad \pm i, \quad \pm j, \quad \pm k, \quad \pm e, \quad \pm ie, \quad \pm je, \quad \pm ke,$$

$$u = \tfrac{1}{2}(\pm 1 \pm i \pm j \pm k), \quad ue,$$

$$\tfrac{1}{2}(\pm 1 \pm j) + \tfrac{1}{2}(\pm 1 \pm i)e, \qquad \tfrac{1}{2}(\pm 1 \pm j) + \tfrac{1}{2}(\pm j \pm k)e,$$

$$\tfrac{1}{2}(\pm 1 \pm i) + \tfrac{1}{2}(\pm 1 \pm j)e, \qquad \tfrac{1}{2}(\pm 1 \pm i) + \tfrac{1}{2}(\pm i \pm k)e,$$

$$\tfrac{1}{2}(\pm 1 \pm k) + \tfrac{1}{2}(\pm 1 \pm k)e, \qquad \tfrac{1}{2}(\pm 1 \pm k) + \tfrac{1}{2}(\pm i \pm j)e,$$

$$\tfrac{1}{2}(\pm i \pm k) + \tfrac{1}{2}(\pm 1 \pm i)e, \qquad \tfrac{1}{2}(\pm i \pm k) + \tfrac{1}{2}(\pm j \pm k)e,$$

$$\tfrac{1}{2}(\pm j \pm k) + \tfrac{1}{2}(\pm 1 \pm j)e, \qquad \tfrac{1}{2}(\pm j \pm k) + \tfrac{1}{2}(\pm i \pm k)e,$$

$$\tfrac{1}{2}(\pm i \pm j) + \tfrac{1}{2}(\pm 1 \pm k)e, \qquad \tfrac{1}{2}(\pm i \pm j) + \tfrac{1}{2}(\pm i \pm j)e.$$

There are many ways to express 2 as the product of an integer f by its conjugate : $f = 1 + i$, or a number with any two coordinates ± 1 and the others zero; $f = \rho + e$, for ρ in (27), or a number with any four coordinates $\pm \frac{1}{2}$, one ± 1, and three zero; $f = q + Qe$, where q and Q are both of the form

$$\tfrac{1}{2}(\pm 1 \pm i \pm j \pm k).$$

Note that

$$(1+i)\sigma = \rho + \rho e, \qquad \sigma = \tfrac{1}{2}(1+j) + \tfrac{1}{2}(1+k)e,$$

$$\tau(1+i) = \rho + \rho e, \qquad \tau = \tfrac{1}{2}(1+k) + \tfrac{1}{2}(i+j)e,$$

where τ is a unit, but σ is not an integer (30). Thus $\rho + \rho e$ is the product of $1 + i$ on the left by a unit, but not on the right. Again

$$(1+i)\lambda = \rho + e, \qquad \lambda = \tfrac{1}{2}(1+j) + \tfrac{1}{2}(1-i)e = \text{unit}.$$

But it would be very laborious to prove that two integers of the same norm are not associates if we permit unit factors both on the right and left simultaneously.

If g is a given integer (3o), we can find an integer q of the same form (3o) such that

$$\mathrm{N}(g - mq) \leqq \frac{5}{4} m^2,$$

where m is any given positive rational integer. When a and b are any given integers, we can find integers q and c such that

$$a = qb + c, \qquad \mathrm{N}(c) \leqq \frac{5}{4} \mathrm{N}(b).$$

Take (1) $g = a\bar{b}$, $m = b\bar{b}$, and write c for $a - qb$. We readily verify by (24) that $(qb)\bar{b} = qm$, although the associative law usually fails here. Thus

$$g - qm = (a - qb)\bar{b} = c\bar{b}, \qquad \mathrm{N}(c)\,\mathrm{N}(\bar{b}) \leqq \frac{5}{4} m^2.$$

For integral quaternions, Hurwitz proved similarly that

$$\mathrm{N}(g - mq) < m^2, \qquad a = bq + c, \qquad \mathrm{N}(c) < \mathrm{N}(b),$$

and hence established the existence of a right-hand greatest common divisor of a and b. Since we are unable to prove its existence for our integers (3o), we have no valid reason to prefer the system (3o), or one of its two equivalents, to other maximal systems (if such exist) having properties C, U_1, N, M.

20. *Outlook.* — We investigated above the integers of the classic canonical algebras to which any algebra in 2, 3, or 4 basal units can be reduced by a linear transformation with real coefficients. If we restrict attention to transformations with rational coefficients, we obtain a much larger list of canonical algebras. The arithmetic of the

(1) If $b = r + \mathrm{Re}$, we write $\bar{b}$ for $r' - \mathrm{Re}$, where r' is the conjugate of the quaternion r.

new algebras not in the former list will have new types of properties. In particular, we may now secure unique factorization into primes, only after the introduction of ideals. This becomes evident if we recall that an algebraic number field of degree n is a special type of linear algebra in n basal units. This more general theory of hypercomplex integers will be presented in the author's book, *Algebras and Their Arithmetics*, in course of publication by the University of Chicago Press.