ALGEBRAS AND THEIR ARITHMETICS*

BY L. E. DICKSON

1. *Introduction.* Beginning with Hamilton's discovery of quaternions eighty years ago, there has been a widespread interest in linear associative algebras, a subject known also under the name of hypercomplex numbers. The list of investigators in this field includes the following well known names: Hamilton, Cayley, Clifford, and Sylvester in England; Poincaré and Cartan in France; Weierstrass, Frobenius, Lipschitz, Molien, Scheffers, and Study in Germany; A. Hurwitz and Du Pasquier in Switzerland; Benjamin Peirce, C. S. Peirce, Taber, Wedderburn, Hazlett, and others in America.

Needed guides to the extensive literature on this subject are furnished by the recent book by Scorza and the two books by the writer. Many of the papers, especially the older ones, contain serious errors and obscurities. Again, a large proportion of the papers are now obsolete, since they either treat only special algebras or fail in an attempt to give a general theory, and especially since they deal only with algebras over the field of all complex numbers. But the results obtained for this very special case have since been extended to algebras over any field, and it is the latter general subject which is the really important one both for algebra and for the theory of numbers.

* A Report presented to the Society, by invitation of the program committee, at Cincinnati, December 28, 1923. This Report, the work of the author reported in it, and two other papers presented by him to the Society at the Cincinnati meetings (see this BULLETIN, page 280 of this issue) formed the basis for the award to the author of the seventy-fifth anniversary prize of the American Association for the Advancement of Science for the most notable contribution to the advancement of science presented at the meetings of that Association and its affiliated societies at Cincinnati on December 27, 1923 to January 2, 1924. (See this BULLETIN, vol. 30, Nos. 1–2, p. 90.) THE EDITORS.

We shall not attempt to give a complete survey of the entire subject of algebras, but shall restrict attention to a few results on the algebraic side which will be required in our account of the chief results in the recent remarkable theory of the arithmetics of algebras.

Instead of presenting the formal definition of a general algebra by postulates, we shall employ typical illustrations.

2. *Algebra of Complex Numbers.* A complex number $a\cdot 1+bi$ is said to have the real *coordinates* a and b and the *basal units* 1 and i. All complex numbers form an algebra of *order* 2 over the field of all real numbers. We obtain another algebra by restricting the coordinates a and b to rational values; it is an algebra of order 2 over the field composed of all rational numbers. In general, a set of real or complex numbers is called a *field* if the sum, difference, product, and quotient (except by zero) of any two numbers of the set are also numbers of the set.

3. *Algebra of Matrices.* We shall now define a more typical algebra which plays an important rôle in our further discussion. Consider 2-rowed square matrices

$$m=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \mu=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

whose elements a, b, c, d, etc., are numbers of any chosen field F. We define the sum and the product of these matrices to be

$$m+\mu=\begin{pmatrix} a+\alpha & b+\beta \\ c+\gamma & d+\delta \end{pmatrix}, \quad m\mu=\begin{pmatrix} a\alpha+b\gamma & a\beta+b\delta \\ c\alpha+d\gamma & c\beta+d\delta \end{pmatrix}.$$

If k is any number of the field F, we call

$$km=\begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}$$

the *scalar product* of the number k and the matrix m. Consider the four special matrices

$$e_{11}=\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_{12}=\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad e_{21}=\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad e_{22}=\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then the foregoing matrix m can be expressed in the form

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & 0 \\ 0 & d \end{pmatrix} = ae_{11} + be_{12} + ce_{21} + de_{22}.$$

Hence the algebra formed of all 2-rowed matrices with elements in the field F has the four basal units e_{11}, e_{12}, e_{21}, e_{22} and is of order 4.

Similarly, all n-rowed square matrices with elements in a field F form an algebra of order n^2, called a *simple matric algebra.*

In the definition of any algebra over any field F, we employ three operations called addition, multiplication, and scalar multiplication, which are assumed to have properties entirely analogous to those holding for the foregoing three operations on matrices.

4. *Quaternions.* The four special matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; i = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \; j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$k = ij = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$$

satisfy the relations

$$i^2 = j^2 = k^2 = -I, \; ij = k = -ji, \; ki = j = -ik, \; jk = i = -kj,$$

and are the basal units of quaternions

$$xI + yi + zj + wk.$$

Since matrix I plays the rôle of unity, it is usually denoted by 1. Quaternions may therefore be obtained very simply from matrices. Only when the field F contains $\sqrt{-1}$ is the present algebra of quaternions over the field F the same as the foregoing simple matric algebra of order 4.

5. *Definitious.* Let F be a field all of whose numbers are real. Consider any quaternion $q = x + yi + zj + wk$ whose four coordinates belong to F and are not all zero. It is readily verified that the product of q by its conjugate

$q' = x - yi - zj - wk$ is $N = x^2 + y^2 + z^2 + w^2$. Since $x, \ldots, w$ are not all zero, we have $N \neq 0$. Evidently q has the inverse $q^{-1} = (1/N)q'$, which is a quaternion with coordinates in F. Then the equation $xq = r$ has the solution $x = rq^{-1}$, while $qy = r$ has the solution $y = q^{-1}r$. Hence our algebra of all quaternions over the real field F is an example of a *division* algebra, in which each of the two kinds of division (except by zero) can always be performed uniquely.

The special quaternions $x + yi$ form an algebra of order 2 called a *sub-algebra* of the algebra of all quaternions.

A sub-algebra I of an algebra A is called *invariant* in A if the product of every element of I by every element of A is an element of I, and if likewise the product of every element of A by every element of I is in I.

In case A has no invariant sub-algebra other than itself, A is called a *simple* algebra. It is a fundamental theorem that every simple algebra A is a direct product of a simple matric algebra and a division algebra D; this may be understood to mean that all elements of A can be expressed as matrices whose elements belong to D.

An element is called *nilpotent* if some power of it is zero. For example, the square of the foregoing matrix

$$e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

is the matrix zero all four of whose elements are zero, whence e_{12} is nilpotent.

An algebra is called nilpotent if all of its elements are nilpotent. A *semi-simple* algebra is one which has no nilpotent invariant sub-algebra.

An algebra A is said to be the *sum* of two sub-algebras B and C if every element of A can be expressed as a sum of an element of B and an element of C. If also the product of every element of B and every element of C is zero, and vice versa, and if B and C have in common only the element zero, then A is called the *direct sum* of B and C.

Every semi-simple algebra is either simple or is a direct sum of simple algebras, and conversely.

The principal theorem on algebras states that every algebra which is neither nilpotent nor semi-simple is the sum of its unique maximal nilpotent invariant sub-algebra and a semi-simple sub-algebra.

6. *Evolution of the Arithmetic of Algebras.* We have now defined those terms and stated those theorems concerning algebras which are needed in our account of the arithmetic of algebras. That subject has been surprisingly slow in its evolution. Quite naturally the arithmetic of quaternions received attention next to the arithmetic of complex integers.

Lipschitz, in his book of 1886, called a quaternion integral if and only if its four coordinates are all ordinary integers. But his theory was extremely complicated; it was not a success since such integral quaternions do not obey the essential laws of divisibility of ordinary integers. For example, there does not exist a greatest common left divisor of 2 and $q = 1 + i + j + k$. For, the only factors of 2 are the products of 2, 1, $1 + i$, $1 + j$ or $1 + k$ by the various *units* ± 1, $\pm i$, $\pm j$, $\pm k$ (i. e., divisors of unity); while the only factors of q are the products of q, 1, $1 + i$, $1 + j$ or $1 + k$ by the units. But no one of the four common factors listed is divisible by all of the others since $1 + i$, $1 + j$ and $1 + k$ are indecomposable.

But A. Hurwitz in his memoir of 1896 and book of 1919 obtained a wholly satisfactory arithmetic of quaternions. He called a quaternion *integral* if its coordinates are either all integers or all halves of odd integers, and proved that the essential laws of divisibility of ordinary integers hold also for integral quaternions. In particular, there exists a greatest common left (or right) divisor; that of 2 and q is 2 since q is the product of 2 by the integral quaternion $\frac{1}{2}q$.

7. *Postulational Formulation.* Although Hurwitz stated his definition only for the case of quaternions, it may be formulated for any associative algebra A over the field of rational numbers. The integral elements of A are defined to be the elements which belong to a set of elements having the following four properties:

C (closure): *The sum, difference, and product of any two elements of the set are also elements of the set.*

B (basis): *The set has a finite basis* (i. e., *contains elements $b_1, \dots, b_k$ such that every element of the set is a linear combination of the b's with ordinary integral coefficients*).

U': *The set contains the basal units of A.*

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

Note that Lipschitz's integral quaternions with integral coordinates have the properties C, B, U', while Hurwitz's integral quaternions have also property M. That a maximal set is superior to other sets is in accord with the history of the evolution of our number system and our experience in various branches of mathematics.

Du Pasquier, a pupil of Hurwitz, published during the past 15 years many papers in which he modified Hurwitz's definition by replacing U' by the milder assumption U that the set contains the modulus 1 which plays the rôle of unity in multiplication.

8. *Former Definitions Unsatisfactory.* But the definitions by Hurwitz and Du Pasquier are both unsatisfactory in general. This fact will be illustrated for the special algebra having two basal units 1 and e, where $e^2 = 0$.

Under Du Pasquier's definition, any set of elements with properties B and U has a basis of the form $1, q = r + se$, where r and s are rational numbers and $s \neq 0$. Since q^2 belongs to the set by property C, we must have $q^2 = a + bq$, where a and b are ordinary integers. Thus

$$r^2 + 2rse = a + b(r + se), \quad r^2 = a + br, \quad 2rs = bs,$$

whence $2r = b$, $r^2 = a + 2r \cdot r$, $r^2 = -a$. Thus r is an integer. We may therefore replace the initial basis $1, q$ by $1, q-r=se$. Our set, designated by $(1, se)$, is evidently contained in the larger set $(1, \frac{1}{2}se)$, which in turn is contained in the still larger set $(1, \frac{1}{4}se)$, etc., where each such set has properties C, B, U. In other words, there does not exist a maximal set, so that the algebra does not possess integral elements, and the definition of integral elements is unsatisfactory. In such a case, Du Pasquier suggested that we omit the desirable requirement M and define the integral elements to be those of an arbitrarily chosen one of the infinitude of sets $(1, se)$. But it has been definitely proved by the writer* that factorization into indecomposable integral elements is then not unique and cannot be made unique by the introduction of ideals however defined.

These insurmountable difficulties arise also under the definition by Hurwitz, which imposes on the foregoing sets $(1, se)$ the condition that s be the reciprocal of an integer, so that the basal unit e shall belong to the set.

9. *Final Theory. Rank-Equation Postulate.* The writer has recently published a satisfactory theory of the integral elements of any rational algebra in his book *Algebras and Their Arithmetics* (University of Chicago Press). He employs postulates C, U, M and (in place of B) the following assumption.

R (rank equation): *For every element of the set, the coefficients of the rank equation are all ordinary integers.*

If $\xi_1, \ldots, \xi_n$ are independent variables in the field of rational numbers, the element $x=\xi_1 u_1+\cdots+\xi_n u_n$ of a rational algebra A having the basal units $u_1, \ldots, u_n$ is a root of a uniquely determined *rank equation*

$$\omega^r+c_1\omega^{r-1}+\cdots+c_r=0$$

in which $c_1, \ldots, c_r$ are polynomials in $\xi_1, \ldots, \xi_n$ with rational coefficients, while x is not a root of an equation

* Bulletin, vol. 28 (1922), pp. 438-442; Journal de Mathématiques, (9), vol. 2 (1923), pp. 281-326.

of degree less than r all of whose coefficients are such polynomials. For example, the quaternion $\alpha+\beta i+\gamma j+\delta k$ and its conjugate $\alpha-\beta i-\gamma j-\delta k$ are roots of

$$\omega^2-2\alpha\omega+(\alpha^2+\beta^2+\gamma^2+\delta^2)=0,$$

which is the rank equation if α, β, γ, δ are independent variables in the field of rational numbers.

As a first justification of our new definition of the integral elements of any algebra A, note that for the case in which A is any algebraic field, there is a unique set of its elements which have properties C, U, R and M, and this set coincides with the totality of integral algebraic numbers of the field. In other words, the new theory is a direct generalization of the classic theory of algebraic numbers.

Next, the serious difficulties observed in the foregoing algebra with the basal units 1 and e entirely disappear under the new definition. For $x=a+be$, we evidently have $(x-a)^2=0$, which is the rank equation if a and b are independent variables in the field of rational numbers. Its coefficients are integers if and only if a is an integer. Evidently the unique maximal set of elements having properties C, U, R is composed of all the $x=a+be$ in which a is an integer and b is rational. These elements x are therefore the integral elements of the algebra. For any rational number k, the product of the integral elements $u=1+ke$ and $1-ke$ is 1, whence each is called a *unit*. Let $a \neq 0$ and choose $k=-b/a$. Then $xu=a$. The product of x by any unit u is said to be *associated* with x. Hence the integral elements are here associated with the ordinary integers a, so that the arithmetic of our algebra is associated with (and reduces to) the arithmetic of ordinary integers.

Note that our set of integral elements is the aggregate of the infinitude of non-maximal sets $(1, se)$ of Du Pasquier. Our satisfactory set may therefore by derived by a suitable enlargement of any one of Du Pasquier's unsatisfactory sets. Similarly, Hurwitz obtained his satisfactory set of integral quaternions by a suitable enlargement of Lipschitz's unsatisfactory set. There are many instances in the history of mathematics where success has been achieved by the principle of enlargement; examples are the growth of our number system and the introduction of ideals in the theory of algebraic numbers.

Note also that our integral elements $a+be$ do not have a finite basis, since b ranges over all rational numbers, and hence do not form a set of integral elements according to the definition either of Hurwitz or Du Pasquier. Thus the writer's conception of integral elements is entirely different from the conceptions of Hurwitz and Du Pasquier. It was only after long experimentation and tests of various kinds that the writer became fully convinced that his conception of the proper subject matter of arithmetics of algebras is from every standpoint wholly satisfactory and in particular far more desirable than all earlier conceptions. Moreover, the new conception greatly facilitated the development of a rich array of fundamental theorems, wholly lacking under former conceptions. The resulting remarkable science of the arithmetics of algebras furnishes the final justification of the new conception of the proper subject matter. It is obviously more difficult to justify a new determination of the proper subject matter of an embryo science than to compare different foundations of an established science.

10. *Theorems on Arithmetics.* According to the principal theorem on algebras stated above, any rational algebra A is a sum of its maximal nilpotent invariant sub-algebra N and a semi-simple sub-algebra S. The fundamental theorem on arithmetics states that the arithmetic of A is associated with that of S in the sense that every integral element (whose determinant is not zero) of A is the product of an integral element of S by a unit. For, all integral elements x of A are obtained by assigning values to the coordinates of those basal units which belong to S, such that the

S-component of x is an integral element of S, and assigning arbitrary rational values to the coordinates of the basal units which belong to N. Furthermore we can choose an element ν of N such that the product of x by the unit $1+\nu$ reduces to the component of x which belongs to S. In other words, the effect of multiplying x by a suitably chosen unit is to suppress the nilpotent component belonging to N (viz., be in our above example).

Next, the problem of the arithmetic of a semi-simple algebra S reduces to that of the arithmetics of simple algebras. For, we saw that S is a direct sum of simple algebras $S_1, S_2, \ldots,$ so that each element σ of S is a sum of components $\sigma_1, \sigma_2, \ldots$ belonging to $S_1, S_2, \ldots$ respectively. It is an important theorem that when σ is an integral element of S, each σ_i is an integral element of S_i, and conversely. Moreover, the divisibility properties for S follow at once from those of the component algebras S_i.

We saw that the elements of any simple algebra Σ can be expressed as matrices whose elements range over the same division algebra D. It can be proved that the integral elements of Σ are those matrices whose elements range over the integral numbers of D, and conversely.

Let D be such that its integral numbers possess a division process yielding always a remainder whose norm is numerically less than the norm of the divisor. We may then establish a theory of reduction and equivalence of matrices whose elements are integral numbers of D. The resulting theory is a direct generalization of the classic theory of matrices whose elements are ordinary integers. In that case factorization into prime matrices is unique apart from unit factors. In our more general case, each matrix is the product of units and a diagonal matrix having exclusively zeros outside the diagonal, so that the arithmetic is associated with the simpler arithmetic of diagonal matrices.

We have therefore reduced the study of arithmetics of all rational algebras to the study of arithmetics of simple algebras, i. e., of matric algebras over a division algebra D, and we have completed the latter study when D is of a certain type.

11. *Conclusion.* Under the new definition, any set of integral elements of the same order as the order of the rational algebra A has a basis if and only if A is semi-simple. Hence the new definition is in complete accord with the older definitions by Hurwitz and Du Pasquier only in the important case of semi-simple algebras. For the remaining algebras, the older definitions led to insurmountable difficulties, whereas under the new definition the arithmetic of such an algebra is associated with that of its semi-simple sub-algebra S, since we may suppress the components belonging to its maximal nilpotent invariant sub-algebra N. It is fortunate that we can get rid of these bizarre nilpotent components since they would interfere seriously in applications. Their elimination also greatly simplifies the theory.

The theory of algebraic numbers finds applications only to problems involving forms which contain only two variables homogeneously and hence can be factored into linear forms. This serious limitation may often be removed by employing hypercomplex numbers. For example, $x^2+y^2+z^2+w^2$ has as factors the quaternion $x+yi+zj+wk$ and its conjugate. Since the new theory of arithmetics of algebras finds applications to problems involving forms in any number of variables it furnishes us with an effective new tool for problems in algebra and the theory of numbers.

THE UNIVERSITY OF CHICAGO