OUTLINE OF THE THEORY TO DATE OF THE ARITHMETICS OF ALGEBRAS

By Professor L. E. Dickson,
University of Chicago, Chicago, Illinois, U.S.A.

Scope of the Lecture. Our purpose is to sketch in a broad way the leading features of the origin and development of a new branch of number theory which furnishes a fundamental generalization of the theory of algebraic numbers. Algebraic fields (Körper) are all very special cases of linear associative algebras, briefly called algebras. The integral quantities of any algebra will be so defined that they reduce to the classic integral algebraic numbers in the special case in which the algebra becomes an algebraic field.

For the sake of clearness, we shall not presuppose any acquaintance with the concept of algebras, but explain that concept and such of the results concerning the theory of algebras as are indispensable in the later discussion of the arithmetics of algebras.

Examples of Algebras. All complex numbers $x.1+yi$ form an algebra of order 2 with the basal units 1 and i. The quantities of which an algebra is composed may be numbers as in this example, or matrices as in the next example, or abstract elements.

A more typical algebra is that whose quantities are two-rowed square matrices

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

etc., whose elements $a, b, \ldots$ are numbers of a specified kind, complex, or real, or rational. We define the sum and product of these two matrices to be

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

Since the last matrix is altered in form by the interchange of the Roman and Greek letters, $m\mu$ is usually distinct from μm, so that multiplication of matrices is not always commutative. If k is any number, we call the matrix

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

the scalar product of the number k and the matrix m and denote it by km or mk. Consider the four special matrices

$$e=\begin{pmatrix}10\\00\end{pmatrix},\ f=\begin{pmatrix}01\\00\end{pmatrix},\ g=\begin{pmatrix}00\\10\end{pmatrix},\ h=\begin{pmatrix}00\\01\end{pmatrix}.$$

Then

$$m=\begin{pmatrix}a0\\00\end{pmatrix}+\ldots+\begin{pmatrix}00\\0d\end{pmatrix}=ae+bf+cg+dh.$$

Hence e, f, g, h are basal units of our *total matric algebra* of order 4 of two-rowed square matrices.

In the definition of any algebra 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. This close relation between general algebras and matric algebras is explained by the theorem which states that any algebra of order n can be expressed concretely as an algebra of matrices with n or $n+1$ rows, although the latter is usually not the total matric algebra.

QUATERNIONS. The four special matrices

$$u=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ i=\begin{pmatrix}\sqrt{-1}&0\\0&-\sqrt{-1}\end{pmatrix},\ j=\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ k=ij=\begin{pmatrix}0&\sqrt{-1}\\\sqrt{-1}&0\end{pmatrix}$$

satisfy the relations

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

and are the basal units of quaternions $xu+yi+zj+wk$. Since matrix u plays the rôle of unity in multiplication, it is usually denoted by 1.

Consider the algebra of all real quaternions

$$q=x+yi+zj+wk$$

with real coordinates x, y, z, w. Its *conjugate* is

$$q'=x-yi-zj-wk.$$

Each of the products $qq', q'q$ has the value

$$N=x^2+y^2+z^2+w^2,$$

which is called the *norm* of q. Let q be not zero, so that x, y, z, w are not all zero and hence $N\neq 0$. Then q evidently has the inverse

$$q^{-1}=\frac{1}{N}q',$$

which is a quaternion with the real coordinates $x/N, \ldots, -w/N$. The equation $\xi q=r$ in real quaternions has the unique solution $\xi=rq^{-1}$, while the equation $q\eta=r$ has the unique solution $\eta=q^{-1}r$. Hence our algebra of all real quaternions is an example of a *division* algebra, in which 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. The $x+zj$ form another sub-algebra.

DEFINITIONS AND THEOREMS ON ALGEBRAS. A sub-algebra I of an algebra A is called *invariant* in A if the product taken in either order of every quantity of I and every quantity of A belongs to I. In case A has no invariant sub-algebra other than itself, A is called a *simple* algebra. It is known that every simple algebra can be expressed in a form such that its quantities are the matrices whose elements belong to a division algebra.

The square of the matrix $\begin{pmatrix}01\\00\end{pmatrix}$ is the matrix zero all four of whose elements are zero. A quantity is called *nilpotent* if some power of it is zero. An algebra is called nilpotent if all of its quantities 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 quantity of A can be expressed as a sum of a quantity of B and a quantity of C. If also the product in either order of every quantity of B and every quantity of C is zero, and if B and C have in common no quantity other than 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 $N+S$ of its unique maximal nilpotent invariant sub-algebra N and a semi-simple sub-algebra S.

THE INTEGRAL QUATERNIONS OF LIPSCHITZ AND THOSE OF HURWITZ. In his book* of 1886, Lipschitz called a quaternion integral if and only if its four coordinates are ordinary integers. By very complicated discussions be obtained some interesting results. But his theory was not a real success, since his integral quaternions do not obey the essential laws of ordinary arithmetic. For example, there does not exist a greatest common left (or right) divisor of 2 and $q=1+i+j+k$, as shown by listing their divisors.

Hurwitz† overcame all such difficulties by developing a new, successful theory of the arithmetic of quaternions. Using postulates quoted below, he was led to define integral quaternions to be those whose four coordinates are either all ordinary integers or all halves of odd integers. He proved that the essential laws of ordinary arithmetic hold also for such integral quaternions. For example, there exists a greatest common left divisor of any two integral quaternions, that of 2 and the above q being 2 since q is the product of 2 by the integral quaternion $\frac{1}{2}q=\frac{1}{2}+\frac{1}{2}i+\frac{1}{2}j+\frac{1}{2}k$. Thus we do not now have the difficulty which we met under the definition by Lipschitz.

HURWITZ'S POSTULATES. Although Hurwitz stated his postulates only for the case of quaternions, it will prove convenient for later comparisons to formulate them for any rational algebra A whose quantities have rational coordinates

**Intersuchungen über die Summen von Quadraten*, Bonn, 1886; French translation in Jour. de Math., p. 4, t. 2, 1886, 393-439.

†Göttinger Nachrichten, 1896, 311-40. Amplified in his book, *Zahlentheorie der Quaternionen*, Berlin, 1919.

and obey the associative law of multiplication. We assume also that A has the modulus 1 which plays the role of unity in multiplication.

The integral quantities of A are defined to be the quantities belonging to a set of quantities satisfying the following four postulates:

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

B (basis): The set has a finite basis (*i.e.*, it contains quantities $b_1, \ldots, b_k$ finite in number, such that every quantity of the set is a linear combination of the b's with ordinary integral coefficients).

U': The set contains 1 and the basal units of A.

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

Note that Lipschitz's integral quaternions with integral coordinates form a set having the properties C, B, U'. For example, they have the basis $1, i, j, k$. This set is, however, not a maximal, being contained in the larger set of Hurwitz's integral quaternions. We saw that the latter maximal set has properties which are simpler and more desirable than those of the former non-maximal set. The superiority of a maximal set is illustrated also by the advantage of the set of all complex numbers over number systems containing only real numbers, or only positive real numbers, or only the primitive numbers 1, 2, 3, ...

Du Pasquier, a pupil of Hurwitz, published during the past fifteen years many papers* in which he replaced Hurwitz's postulate U' by the milder postulate U that the set contains 1. This replacement is an improvement, since all of the resulting postulates are invariant under every transformation of the basal units, while U' is evidently not invariant.

THE DEFINITIONS BY HURWITZ AND DU PASQUIER ARE UNSATISFACTORY. This fact will be illustrated for the special algebra having the two basal units 1 and e, where $e^2=0$. Under Du Pasquier's definition, any set of quantities 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 must belong to the set by property C, and hence is equal to $a+bq$, where a and b are ordinary integers, we find that $r^2=a+br$, $2r=b$, whence $r^2=-a$. Thus r is an integer. We may therefore replace the initial basis $1, q$ by $1, q-r=se$. Our set is evidently contained in the larger set with the basis $1, \frac{1}{2}se$, which in turn is contained in the still larger set with the basis $1, \frac{1}{4}se$, 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 quantities.

The same unfortunate conclusion results also from the definition by Hurwitz, which imposes the further condition that e shall belong to the set and hence that s be the reciprocal of an integer.

*Vierteljahrsschrift Naturf. Gesell. Zürich, 51 (1906), 55-129; 52 (1907), 243-8; 54 (1909), 116-48. L'Enseignement Math., 17 (1915), 340-3; 18 (1916), 201-60. Nouv. Ann. Math. (4), 18 (1918), 448-61. Bull. Soc. Math. France, 48 (1920), 109-32. Comptes Rendus du Congrès International des Mathématiciens, Strasbourg, 1920, 164-75.

Under the definition by either Hurwitz or Du Pasquier there exist no integral quantities in the great majority of algebras, in fact for any algebra which is not semi-simple.

THE NEW CONCEPTION OF INTEGRAL QUANTITIES. The lecturer has recently published* a satisfactory theory of the integral quantities of any rational algebra having a modulus 1. Let its basal units be $u_1, \ldots, u_n$. If $\xi_1, \ldots, \xi_n$ are variables ranging independently over all rational numbers, the quantity $q=\xi_1 u_1+\ldots+\xi_n u_n$ is a root of a uniquely determined *rank equation* whose coefficients are polynominals in $\xi_1, \ldots, \xi_n$ with rational coefficients, the leading coefficient of the equation being unity, while q is not a root of an equation of smaller degree all of whose coefficients are such polynomials. For example, the quaternion $q=x+yi+zj+wk$ and its conjugate are roots of

$$\omega^2-2x\omega+(x^2+y^2+z^2+w^2)=0,$$

which is the rank equation of the algebra of rational quaternions if x, y, z, w are variables ranging independently over all real numbers.

The new definition of integral quantities employs postulates C, U, M and (in place of B).

R: For every quantity of the set, the coefficients of the rank equation are all ordinary integers.

As a first justification of this definition of the integral quantities of any rational algebra A having a modulus 1, note that when A is any algebraic field it is readily proved that its integral quantities coincide with the integral algebraic numbers of the field. In other words, the new theory is a direct generalization of the classic theory of algebraic numbers.

Second, when A is the algebra of rational quaternions, the new definition leads very simply to the desirable integral quaternions of Hurwitz.

Third, every algebra now has† integral quantities, whereas this was rarely true under the earlier definitions.

The final justification of the new conception of integral quantities of an algebra lies in the rich array of fundamental general theorems which have been developed under the new conception and will be summarized later on, whereas under the earlier conceptions no general theorem had been obtained.

OLD AND NEW CONCEPTIONS CONTRASTED IN AN EXAMPLE. We shall apply the new definition to the foregoing rational algebra having the basal units 1 and e, where $e^2=0$. For $x=a+be$, we evidently have $(x-a)^2=0$, which is the rank equation when a and b are variables ranging independently over all rational numbers. Its coefficients are ordinary integers if and only if a is an integer. Evidently the unique maximal set of quantities x having properties C, U, R is composed of all the $x=a+be$ in which a is an integer and b is a rational number.

*_Algebras and their Arithmetics_, University of Chicago Press.

†Proved in the lecturer's paper, _Further development of the Theory of Arithmetics of Algebras_, these Proceedings.

These quantities x are therefore the integral quantities of the algebra. For any rational number k, the product of the integral quantities $u=1+ke$ and $1-ke$ is 1, whence each is called a *unit*. Let $a\neq 0$ and choose $k=-b/a$. Then $xu=a$. Such a product of x by a unit u is said to be *associated* with x. Associated quantities play equivalent roles in questions of divisibility. The integral quantities of our algebra are therefore associated with the ordinary integers a and may be replaced by the latter in questions of divisibility.

Contrast these simple and satisfactory results under the new conception with the unfortunate conclusion, under the conceptions of integral quantities held by Hurwitz and Du Pasquier, that this algebra has no integral quantities. Faced with the dilemma that no maximal set exists under his definition, Du Pasquier suggested that we omit the desirable postulate M, that the set be a maximal and hence define the integral quantities to be those of an arbitrarily chosen one of the infinitude of sets with the basal units 1 and se. But it has been definitely proved by the lecturer* that factorization into indecomposable integral quantities is then not unique and cannot be made unique by the introduction of ideals however defined. These insurmountable difficulties are in marked contrast with the simple conclusion, under the new conception, that the integral quantities are uniquely determined and are associated with ordinary integers.

It is worthy of notice that our set of integral quantities is the aggregate of the infinitude of non-maximal sets of Du Pasquier. Our satisfactory set may therefore be derived by a suitable enlargement of any one of his unsatisfactory sets. There are many instances in the history of mathematics where success has been achieved by the principle of enlargement; examples are the evolution of our number system, the introduction of ideals in the theory of algebraic numbers, and the enlargement of Lipschitz's unsatisfactory set of integral quaternions to Hurwitz's satisfactory set.

GENERAL THEORY OF ARITHMETICS OF ALGEBRAS. Let A be any rational associative algebra with a modulus 1. According to the principal theorem on algebras stated above, $A=S+N$, where N is the maximal nilpotent invariant sub-algebra of A, and S is a semi-simple sub-algebra. The fundamental theorem on arithmetics states that the arithmetic of A is associated with that of S in the sense that every integral quantity (whose determinant is not zero) of A is the product of an integral quantity of S by a unit. This theorem is illustrated by the foregoing example, in which N is composed of the components be and S is composed of the rational components a, so that the integral quantities of S are the ordinary integers. Another statement of this theorem is that in questions of divisibility we may suppress the bizarre nilpotent components belonging to N. This elimination of undesirable elements is fortunate both for the theory and for its applications.

We have therefore reduced the problem of the arithmetics of all algebras to that of semi-simple algebras S. We can further reduce the problem to the case of simple algebras. For, we saw that S is a direct sum of simple algebras

*Bull. Amer. Math. Soc., 28 (1922), 438-42; Jour. de Math. p. 9, t. 2 (1923), 281-326.

$S_1, S_2, \ldots$, so that each quantity 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 if each σ_i is an integral quantity of S_i, then σ is one of S, and conversely. Moreover, the divisibility properties for S follow at once from those of the component algebras S_i.

We saw that the quantities of any simple algebra Σ can be expressed as matrices whose elements range independently over the same division algebra D. It can be proved that there is a unique set of integral quantities of Σ which contains* all matrices whose elements are ordinary integers, and that this set is composed of the matrices whose elements range independently over the integral quantities of D, and conversely.

Although we know the integral quantities of Σ as soon as we know those of D, it remains to deduce the divisibility properties of the former from the latter. This has been accomplished for the case of those division algebras D which have the property that its integral quantities possess a process of division yielding always a remainder whose norm is numerically less than the norm of the divisor. This property holds when D is the algebra of rational numbers, or one of numerous quadratic algebraic fields, or the algebra of rational quaternions, or certain algebras of generalized quaternions. For such a D, we have a theory of reduction and equivalence of matrices whose elements are integral quantities of D. The resulting theory is a direct generalization of the classic theory of matrices whose elements are ordinary integers, and then factorization into prime matrices is unique apart from unit factors. In our more general case, each matrix is a product of units and a matrix having only zeros outside the diagonal.

We have therefore reduced the study of arithmetics of all rational algebras to the case of simple algebras, *i.e.*, of the algebra of all matrices whose elements belong to a division algebra D, and have treated the arithmetic of the latter algebra when the integral quantities of D admit a process of division yielding a remainder of norm numerically less than that of the divisor. Such a process of division implies the existence of a right (or left) greatest common divisor. But the latter may exist even when that process of division is lacking†.

APPLICATIONS TO DIOPHANTINE EQUATIONS. The theory of algebraic numbers is applicable only to problems involving polynomials which contain only one variable or two variables homogeneously, so that the polynomial can be factored into linear functions. This serious limitation can often be removed by employing quantities of an algebra. For example, $N=x^2+y^2+z^2+w^2$ has as factors the quaternion $x+yi+zj+wk$ and its conjugate. By using integral quaternions we readily find all integral solutions of $N=uv$. Taking u as the sum and v as the difference of two unknowns, we deduce all ways of finding five integers the sum of whose squares is a square.

*If we omit this assumption, we find many sets of integral quantities. For example, let D be composed of the rational numbers. Every set of integral quantities of the resulting total rational matric algebra Σ can be transformed into the set of matrices whose elements are ordinary integers by a suitably chosen matrix with rational elements.

†Dickson, Amer. Jour. Math., 1923.

Various other Diophantine equations have been solved completely in integers for the first time by using the integral quantities of certain algebras of generalized quaternions.

Since the new theory of arithmetics of algebras solves completely certain types of Diophantine equations in any number of variables which were not solvable by any earlier method, it furnishes us with an effective new tool for the theory of numbers.

CONCLUSION. We have given a brief outline of the theory to date of arithmetics of algebras. This new branch of the theory of numbers is a far reaching generalization of the classic theory of integral algebraic numbers.

We have also made it clear why it was necessary to discard the earlier conceptions of the integral quantities of a general algebra and introduce a new conception of them.

The gradual enlargement of the conception of number from the primitive numbers used in counting to the system of all complex numbers and finally to its culmination in hypercomplex numbers (or quantities of any algebra) has its parallel in the growth of the concept integer, which was first restricted to the counting numbers, was greatly enriched in the last century by the study of integral algebraic numbers, and now finds its culmination in the integral quantities of any algebra.