PART I

DEFINITIONS, ILLUSTRATIONS AND ELEMENTARY THEOREMS

1. Arithmetical definition of ordinary complex numbers. The following purely arithmetical theory of couples (a, b) of real numbers differs only in unessential points from the initial theory of W. R. Hamilton*. Two couples (a, b) and (c, d) are called equal if and only if $a = c$, $b = d$. Addition, subtraction and multiplication of two couples are defined by the formulas†

$$\left.\begin{aligned} (a, b) + (c, d) &= (a + c, b + d) \\ (a, b) - (c, d) &= (a - c, b - d) \\ (a, b)\,(c, d) &= (ac - bd, ad + bc) \end{aligned}\right\} \qquad (1).$$

Addition is seen to be commutative and associative:

$$x + x' = x' + x, \quad (x + x') + x'' = x + (x' + x'') \qquad (2),$$

where x, x', x'' are any couples. Multiplication is commutative, associative and distributive:

$$xx' = x'x, \quad (xx')\,x'' = x\,(x'x'') \qquad (3),$$

$$x\,(x' + x'') = xx' + xx'', \quad (x' + x'')\,x = x'x + x''x \qquad (4).$$

* *Trans. Irish Acad.*, vol. 17 (1837), p. 293; *Lectures on Quaternions*, 1853, Preface.

† Each couple (a, b) uniquely determines a vector from the origin O to the point A with the rectangular coordinates a, b. The sum of two vectors from O to A and the point $C = (c, d)$ is defined to be the vector from O to the fourth vertex S of the parallelogram having the lines OA and OC as two sides. The coordinates of S are $a + c$, $b + d$. Subtraction of vectors is the operation inverse to addition; thus $OS - OA = OC$. To define the product of the vectors from O to A and C, we employ initially the polar coordinates r, θ and r', θ' of A and C. Then $OA \,.\, OC$ is defined to be the vector from O to the point P with the polar coordinates rr', $\theta + \theta'$. Since A has the rectangular coordinates $a = r\cos\theta$, $b = r\sin\theta$, and similarly for C and P, the expansions of $\cos(\theta + \theta')$ and $\sin(\theta + \theta')$ lead to the third relation (1) between the rectangular coordinates of A, C, P.

Division is defined as the operation inverse to multiplication. Division except by (0, 0) is possible and unique:

$$\frac{(c, d)}{(a, b)} = \left(\frac{ac + bd}{a^2 + b^2}, \frac{ad - bc}{a^2 + b^2}\right) \tag{5}.$$

In particular, we have

$$(a, 0) \pm (c, 0) = (a \pm c, 0), \quad (a, 0)(c, 0) = (ac, 0),$$
$$\frac{(c, 0)}{(a, 0)} = \left(\frac{c}{a}, 0\right) \quad \text{if } a \neq 0.$$

Hence the couples $(a, 0)$ combine under the above defined addition, multiplication, etc., exactly as the real numbers a combine under ordinary addition, multiplication, etc. Without introducing any contradiction, we may and shall impose upon our system of couples (a, b), subject to the above definitions of addition, etc., the further assumption* that the couple $(a, 0)$ shall be the real number a. For brevity write i for $(0, 1)$. Then

$$i^2 = (0, 1)(0, 1) = (-1, 0) = -1,$$
$$(a, b) = (a, 0) + (0, b) = a + (b, 0)(0, 1) = a + bi.$$

The resulting symbol $a + bi$ is called a complex number. Relations (1) and (5) now take the familiar forms

$$\left.\begin{aligned} (a + bi) \pm (c + di) &= (a \pm c) + (b \pm d)\, i \\ (a + bi)(c + di) &= (ac - bd) + (ad + bc)\, i \\ \frac{c + di}{a + bi} &= \frac{ac + bd}{a^2 + b^2} + \frac{ad - bc}{a^2 + b^2}\, i \end{aligned}\right\} \tag{6},$$

where, for the last, $a + bi \neq 0$, i.e. a and b are not both zero.

2. Number fields. A set of complex numbers is called a number field (domain of rationality or Körper) if the rational operations can always be performed unambiguously within the set. In other words, the sum, difference, product and quotient (the divisor not being zero) of any two equal or distinct numbers of the set must be numbers belonging to the set.

In view of (6), all complex numbers $a + bi$ form a field. Again, all real numbers form a field. The set of all rational numbers is a field, but the set of all integers is not.

* Just as the natural numbers are included among the signed integers, the integers among the rational numbers, and the latter among the real numbers defined by means of them. In the same train of ideas, 1 is often used to denote the principal unit (§ 7, § 11), and the number e for the scalar matrix S_e (§ 4, second foot-note).

3. Matrices. The concept matrix* affords an excellent introduction to the subject of this tract and, moreover, is of special importance in the general theory. We shall consider only square matrices of n rows each containing n elements. For example, if $n = 2$,

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \mu = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{7}$$

are matrices, the elements of the first matrix m being a, b, c, d. Each element may be any number of a given number field F. We shall say that m and μ are equal if and only if their corresponding elements are equal, $a = \alpha$, etc. Addition and multiplication are defined by

$$m + \mu = \begin{pmatrix} a+\alpha & b+\beta \\ c+\gamma & d+\delta \end{pmatrix}, \quad m\mu = \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix} \tag{8}.$$

The element in the ith row and jth column of the product is the sum of the products of each element of the ith row of the first matrix by the corresponding element of the jth column of the second matrix, i.e. first by first, second by second, etc. This rule holds also for matrices of n^2 elements. Of the four possible rules for expressing the product of two determinants of order n as a determinant of order n, the above is the only rule which holds also for matrices.

With the exception of (3_1), the laws (2)—(4) for addition and multiplication hold for matrices. Since the product (8_2) is in general altered when the Roman and Greek letters are interchanged, matric multiplication is usually not commutative. Accordingly we shall see that we must distinguish between two distinct kinds of division of matrices. To this end, note that

$$\begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} m = m \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} = \begin{pmatrix} ea & eb \\ ec & ed \end{pmatrix} \tag{9}.$$

In particular, the *unit* matrix

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{10}$$

has the property that $Im = mI = m$, for every matrix m. By the *inverse* of a matrix m whose determinant $\Delta = |m|$ is not zero is meant

* Cayley, *Phil. Trans. London*, vol. 148 (1858), pp. 17—37 (=*Coll. Math. Papers*, II, pp. 475, 604).

$$m^{-1} = \begin{pmatrix} \frac{d}{\Delta} & \frac{-b}{\Delta} \\ \frac{-c}{\Delta} & \frac{a}{\Delta} \end{pmatrix} \qquad (11),$$

if $n = 2$, while if $n \geqq 2$, we employ as the element in the ith row and jth column the quotient of the co-factor of the element in the jth row and ith column of Δ by Δ. Then

$$mm^{-1} = m^{-1}m = I \qquad (12).$$

Given two matrices m and p such that $|m| \neq 0$, we can find one and only one matrix $\mu = m^{-1}p$ such that $m\mu = p$, also one and only one matrix $\nu = pm^{-1}$ such that $\nu m = p$. These respective kinds of division by p by m shall be called *right-hand and left-hand division*.

On the contrary, if $|m| = 0$, there is no matrix μ for which $m\mu = I$, since this would imply $0\,|\mu| = |I| = 1$. Likewise, there is no matrix ν for which $\nu m = I$.

Thus right- and left-hand division by m are each always possible and unique if and only if the determinant of m is not zero.

Addition, subtraction, multiplication and division of matrices with elements in a field F lead to matrices with elements in F. Accordingly we shall speak of the matric algebra over the field F. When F is the field of all complex numbers, the field of all real numbers, or that of all rational numbers, we have the complex, real or rational matric algebra of square matrices of n^2 elements.

4. A matric algebra viewed as a linear algebra*. Taking $n = 2$, we shall make use of the particular matrices

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \qquad (13).$$

Their sixteen products by twos are

$$e_{ij}e_{jk} = e_{ik}, \quad e_{ij}e_{tk} = 0 \quad (t \neq j) \qquad (14).$$

If m is a matrix and e is a number, we shall define the product† em

* For references, see § 13.

† In the product (9) we may therefore replace the "scalar matrix" $\begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} = S_e$ by the number e. This becomes intuitive if we note that $S_e = eI$. Since $S_e + S_f = S_{e+f}$, $S_eS_f = S_{ef}$, etc., the algebra of all scalar matrices over a field F is abstractly identical with F. This replacement of S_e by e is similar to that of $(a, 0)$ by a in § 1.

or me to be the matrix each of whose elements is the product of e by the corresponding element of m:

$$e\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} e = \begin{pmatrix} ea & eb \\ ec & ed \end{pmatrix} \qquad (15).$$

In view of (13), matrices (7) and (8) may be expressed in the form

$$\left.\begin{aligned} m &= ae_{11} + be_{12} + ce_{21} + de_{22} \\ \mu &= \alpha e_{11} + \beta e_{12} + \gamma e_{21} + \delta e_{22} \end{aligned}\right\} \qquad (16),$$

$$\left.\begin{aligned} m + \mu &= (a+\alpha)\, e_{11} + (b+\beta)\, e_{12} + (c+\gamma)\, e_{21} + (d+\delta)\, e_{22} \\ m\mu &= (a\alpha + b\gamma)\, e_{11} + (a\beta + b\delta)\, e_{12} + (c\alpha + d\gamma)\, e_{21} + (c\beta + d\delta)\, e_{22} \end{aligned}\right\} \qquad (17).$$

The last may also be found from (16) by use of relations (14).

The set of hyper-complex numbers $ae_{11} + \ldots + de_{22}$, in which $a, \ldots, d$ range independently over a field F, and for which addition and multiplication are defined by (17), is called a linear associative algebra over F with the four units $e_{11}, \ldots, e_{22}$ subject to the multiplication table (14).

For any n, let e_{ij} be the square matrix of n^2 elements all zero except that in the ith row and jth column which is unity. Then relations (14) hold. We obtain a linear associative algebra with n^2 units e_{ij}.

5. General definition of hyper-complex numbers and linear algebras*. We shall generalize the notion of couples in § 1 and, with a change of notation, the notion of quadruples (7). Consider the set of all *n-tuples* $(x_1, \ldots, x_n)$, whose *coordinates* $x_1, \ldots, x_n$ range independently over a given number field F.

Two n-tuples are called equal if and only if their corresponding coordinates are equal.

Addition and subtraction of n-tuples are defined by

$$(x_1, \ldots, x_n) \pm (x_1', \ldots, x_n') = (x_1 \pm x_1', \ldots, x_n \pm x_n') \qquad (18).$$

The product of any number ρ of the field F and any n-tuple

$$x = (x_1, \ldots, x_n)$$

is defined to be

$$\rho x = x\rho = (\rho x_1, \ldots, \rho x_n) \qquad (19).$$

* Hamilton's *Lectures on Quaternions*, 1853, Introduction. For definitions by independent postulates, see Dickson, *Trans. Amer. Math. Soc.*, vol. 4 (1903), p. 21; vol. 6 (1905), p. 344.

The n *units* are defined to be

$$e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, 0, \ldots, 0),\ \ldots,\ e_n = (0, \ldots, 0, 1).$$

Hence any n-tuple x can be expressed in the form

$$x = x_1 e_1 + x_2 e_2 + \ldots + x_n e_n.$$

We shall call x a *hyper-complex* number, or briefly a number. In view of the definition of equality of n-tuples, x and

$$x' = x_1' e_1 + \ldots + x_n' e_n$$

are equal if and only if $x_1 = x_1', \ldots, x_n = x_n'$. In particular, $x = 0$ implies that each $x_i = 0$. Hence the units $e_1, \ldots, e_n$ are linearly independent with respect to the field F.

It is assumed that any two such numbers x and x' can be combined by an operation called multiplication subject to the distributive laws (4):

$$xx' = \sum_{i,j=1}^{n} x_i x_j' e_i e_j,$$

and such that the product xx' is a number $\Sigma z_i e_i$ with coordinates in F. Necessary conditions for the latter property are

$$e_i e_j = \sum_{k=1}^{n} \gamma_{ijk} e_k \qquad (i, j = 1, \ldots, n\ ;\ \gamma\text{'s in } F) \qquad (20).$$

These are sufficient conditions, since they imply

$$xx' = y \equiv \Sigma y_k e_k, \quad y_k = \sum_{i,j=1}^{n} x_i x_j' \gamma_{ijk} \qquad (k = 1, \ldots, n) \qquad (21).$$

Properties (18) and (19) of n-tuples give

$$x \pm x' = \sum_{i=1}^{n} (x_i \pm x_i') e_i, \quad \rho x = x\rho = \sum_{i=1}^{n} (\rho x_i) e_i \qquad (22),$$

if ρ is in F. The set of all numbers $\Sigma x_i e_i$, with coordinates in F, combined under multiplication as in (21), under addition and subtraction as in (22_1), and under multiplication by a number ρ of F as in (22_2), shall be said to form a *linear algebra* (or system of hyper-complex numbers) over the field F, with the units $e_1, \ldots, e_n$ (linearly independent with respect to F) and the multiplication table (20). The n^3 numbers γ_{ijk} are called the constants of multiplication. Neither the commutative nor the associative law of multiplication is assumed.

For example, the set of all ordinary complex numbers $a+bi$ form a binary linear algebra over the field F of all real numbers, with the units 1 and i subject to the multiplication table

$$1^2=1, \quad 1.i=i.1=i, \quad i^2=-1.$$

In this algebra (§ 1), multiplication is commutative and associative. The algebra is a field $F(i)$ and may be viewed as a unary algebra over this complex field with the single unit 1.

In § 4 we considered a linear associative algebra with four units.

6. Division. Given two numbers x and y of a linear algebra, we can determine uniquely a number x' of the algebra such that $xx'=y$ provided the n linear equations at the end of (21) are solvable uniquely for $x_1', \ldots, x_n'$ in the field F. This will be the case if and only if the determinant

$$\Delta(x)=\left|\sum_{i=1}^{n} x_i\gamma_{ijk}\right| \qquad (j,k=1,\ldots,n) \qquad (23)$$

is not zero. In that case, right-hand division by x is always possible and unique.

Similarly, there is a unique solution x' in the algebra of the equation $x'x=y$ if and only if

$$\Delta'(x)=\left|\sum_{i=1}^{n} x_i\gamma_{jik}\right| \qquad (j,k=1,\ldots,n) \qquad (24)$$

is not zero. In that case, left-hand division by x is always possible and unique.

We shall call $\Delta(x)$ the *right-hand determinant* of x, and $\Delta'(x)$ the *left-hand determinant* of x.

7. Principal unit (modulus). An algebra may contain a number

$$\epsilon=\epsilon_1 e_1+\ldots+\epsilon_n e_n,$$

called a principal unit or modulus, such that

$$x\epsilon=\epsilon x=x \qquad \text{(for every number } x \text{ of the algebra)} \qquad (25).$$

For example, $\epsilon=1$ in the binary algebra of all complex numbers $a+bi$. Again, $\epsilon=e_{11}+e_{22}$ in the matric algebra of § 4.

There cannot be a second principal unit ϵ'. More generally, there is no new number ϵ' for which $x\epsilon'=x$ for every x. For, if so, $\epsilon\epsilon'=\epsilon$, while by (25_2) for $x=\epsilon'$, $\epsilon\epsilon'=\epsilon'$, whence $\epsilon'=\epsilon$.

Conditions (25) hold if and only if

$$e_j\epsilon=\epsilon e_j=e_j \qquad (j=1,\ldots,n) \qquad (25').$$

With Kronecker, set $\delta_{jj}=1$, $\delta_{jk}=0$ if $j\neq k$. By use of (20) and the linear independence of $e_1, \ldots, e_n$, we see that (25′) are equivalent to

$$\sum_{i=1}^{n}\epsilon_i\gamma_{jik}=\delta_{jk}, \quad \sum_{i=1}^{n}\epsilon_i\gamma_{ijk}=\delta_{jk} \qquad (j, k=1, \ldots, n) \qquad (26).$$

Hence
$$\Delta'(\epsilon)=\Delta(\epsilon)=|\delta_{jk}|=1 \qquad (27).$$

Hence if there exists a principal unit, neither $\Delta(x)$ nor $\Delta'(x)$ is identically zero in $x_1, \ldots, x_n$.

For the case of a linear associative algebra it is easily proved that, conversely*, when neither $\Delta(x)$ nor $\Delta'(x)$ is identically zero, the algebra has a principal unit. Indeed, there is then a number u for which neither $\Delta(u)$ nor $\Delta'(u)$ is zero. By § 6, there is a unique number ϵ of the algebra such that $u\epsilon=u$, and a uniquely determined z for which $zu=x$, where x is an arbitrary number of the algebra. Then, by the associative law,

$$x\epsilon=(zu)\,\epsilon=z\,(u\epsilon)=zu=x,$$
$$u\,(\epsilon x)=(u\epsilon)\,x=ux, \quad \epsilon x=x.$$

Hence ϵ is a principal unit. In such an algebra any number x for which $\Delta(x)\neq 0$ has a unique inverse. For, if x^{-1} is the unique number determined by $xx^{-1}=\epsilon$, then $x^{-1}x=\epsilon$, since

$$x\,(x^{-1}x-\epsilon)=\epsilon x-x\epsilon=0.$$

Hence $x'x=\epsilon$ implies $x'=x^{-1}$, as shown by multiplying by x^{-1} on the right, so that $\Delta'(x)\neq 0$ (§ 6).

Thus $\Delta(x)\neq 0$ implies $\Delta'(x)\neq 0$ and conversely.

8. Transformation of units. Consider n numbers

$$E_i=\sum_{j=1}^{n}c_{ij}e_j \qquad (i=1, \ldots, n) \qquad (28)$$

in which the c's are numbers of a field F such that

$$|c_{ij}|\neq 0 \qquad (i, j=1, \ldots, n).$$

We may solve the n equations and obtain

$$e_i=\sum_{j=1}^{n}t_{ij}E_j, \quad |t_{ij}|\neq 0 \qquad (i=1, \ldots, n) \quad (29),$$

where the t's are numbers of F. By means of (28) and (20) we can

* G. Scheffers, *Leipzig Berichte*, vol. 41 (1889), p. 293. Stated for commutative algebras by Weierstrass, *Göttingen Nach.*, 1884, p. 412.

express E_iE_j as a linear function of the e's, and hence by (29) as a linear function of the E's:

$$E_iE_j = \sum_{k=1}^{n} \Gamma_{ijk}E_k \quad (i, j = 1, \ldots, n) \quad (30).$$

For any number x of the algebra,

$$x \equiv \sum_{i=1}^{n} x_ie_i = \sum_{j=1}^{n} X_jE_j, \quad X_j = \sum_{i=1}^{n} t_{ij}x_i \quad (31).$$

Hence x can be expressed in one way and, in view of the linear independence of $E_1, \ldots, E_n$ with respect to F, but one way as ΣX_jE_j, where the X's are numbers of F. Taking $E_1, \ldots, E_n$ as new units, we obtain a linear algebra over F with the constants of multiplication Γ_{ijk}, which is called the *transform* of the initial algebra by the transformation of units (28) or (29). The two algebras are called *equivalent* under linear transformation of units in F.

9. Any number of a linear algebra is a root of an equation. Any $n+1$ numbers of a linear algebra with n units over a field F are linearly dependent with respect to F. For, if the first n of the $n+1$ numbers are linearly independent with respect to F, the $(n+1)$th number can be expressed as a linear function of them with coefficients in F (§ 8).

Assuming here that multiplication is associative, we may denote the product of i factors A by A^i, where A is any number of the algebra. Since $A, A^2, \ldots, A^{n+1}$ are linearly dependent, A is a root of an equation of degree $\leqq n+1$ with coefficients in F.

If also the algebra has a modulus ϵ, then $\epsilon, A, \ldots, A^n$ are linearly dependent and A is a root of an equation of degree $\leqq n$ with coefficients in F.

For example, in the case of the linear associative algebra of four units in § 4, $\epsilon = e_{11} + e_{22}$ is a principal unit, and the general number m, given by (16_1), is a root of

$$m^2 - (a+d)\, m + (ad - bc)\, \epsilon = 0.$$

10. Polynomials in a single number. An algebraic identity

$$f(x)\, g(x) \equiv p(x),$$

where the functions $f(x)$, etc., are polynomials in an ordinary complex variable with ordinary complex coefficients, without terms free of x, implies that the same relation holds when x is any number of a linear associative algebra. Indeed, the term involving x^k in $f(x)\, g(x)$ is

obtained by multiplying the term in x^i of $f(x)$ by the term in x^{k-i} of $g(x)$ and summing the products for $i = 1, \ldots, k-1$. But the associative law gives $x^i x^{k-i} = x^k$.

The argument holds also for functions with terms free of the variable x provided the algebra has a principal unit ϵ and this is multiplied into those terms of the corresponding relation in the hyper-complex number x.

Since the associative law implies $x^r x^s = x^s x^r$, two polynomials in a hyper-complex number x are commutative.

11. Algebra of real quaternions; its unique place among algebras. We shall determine all linear associative algebras over the field of real numbers such that a product is zero only when one factor is zero. This determination is of decided intrinsic interest and yields an important result on real simple algebras (end of § 56).

If x is a given number $\neq 0$, $xx' = 0$ implies $x' = 0$; similarly, $x'x = 0$ implies $x' = 0$. Hence (§ 6) neither $\Delta(x)$ nor $\Delta'(x)$ is zero when $x \neq 0$. Thus (end of § 7) the algebra contains a principal unit, which we shall denote by 1. If every number is a real multiple of 1, the algebra is the field of all real numbers. Excluding this case, we may take the units to be $1, e_1, \ldots, e_{n-1}$, where $n > 1$. Then (§ 9) any number A of the algebra is a root of an equation $p(x) = 0$ of degree $\leqq n$ with real coefficients. By the fundamental theorem of algebra, $p(x)$ equals a product $f_1(x) f_2(x) \ldots$ of linear or quadratic factors with real coefficients. Then (§ 10), $f_1(A) f_2(A) \ldots = 0$. Thus one factor is zero. Hence any number of the algebra is a root of a quadratic equation with real coefficients.

If $e^2 + 2re + s = 0$, then $(e+r)^2 = r^2 - s$. Hence after adding a real constant to each e_i, we may assume that the square of each new unit e_i is a real number. If e_1^2 is a real number $\geqq 0$,

$$0 = e_1^2 - r^2 = (e_1 - r)(e_1 + r), \quad e_1 = \pm r,$$

whereas e_1 and 1 are linearly independent. Thus $e_1^2 = -t^2$, where t is a real number $\neq 0$. Set $E_1 = e_1/t$. Then $E_1^2 = -1$. If $n = 2$, the new units are $1, E_1 = i$, and the algebra is the system of ordinary complex numbers. Next, let $n > 2$. Then we may take the units to be $1, I, J, \ldots$, where*

$$I^2 = -1, \quad J^2 = -1, \ldots \qquad (32).$$

* Although $I^2 = J^2$, it does not follow that $(I-J)(I+J) = 0$, $I = \pm J$.