ON THE RELATION BETWEEN LINEAR ALGEBRAS AND CONTINUOUS GROUPS.

BY PROFESSOR L. E. DICKSON.

1. THE aim of this note is to give a very elementary account of the mutual relation between any linear associative algebra (system of hypercomplex numbers) and a type of continuous groups, without presupposing on the part of the reader a knowledge of either subject. The relation in question, first observed by Poincaré, enables us to translate the concepts and theorems of the one subject into the language of the other subject. It not only doubles our total knowledge, but gives us a better insight into either subject by exhibiting it from a new point of view. Incidentally, we shall obtain several other results of general interest.

2. To begin with the simplest illustration, we set up a correspondence between each real number c, not zero, and the transformation $z' = cz$, denoted by T_c, on the real variable z. The result of applying in succession T_c and the new transformation $T_{c'}$ (which we may express in the form $z'' = c'z'$) is the same as applying the single transformation $z'' = (c'c)z$. Hence we say that the *product* $T_cT_{c'}$ of the two given transformations is the transformation $T_{c''}$, where $c'' = c'c$. The set of transformations which correspond to the system (or algebra) of all real numbers, other than zero, is said to form a *group* G since the product of any two of these transformations is a transformation of the same set. In particular, G is a one-parameter continuous group. The relation $c'' = c'c$ between the parameters in $T_cT_{c'} = T_{c''}$ defines a transformation of c into c'' with the parameter c'. Since c' ranges over all real numbers other than zero, the resulting transformations $c'' = c'c$ on the parameters form a group which is the same as G, apart from the notation of the variables. Hence G is said to be its own parameter group.

Next, let z denote a complex variable $x + yi$ and let c range over all complex numbers $a + bi$ other than zero. Then T_c is equivalent to the binary transformation

$$T_{a,\,b}: \qquad x' = ax - by, \quad y' = bx + ay.$$

The set of transformations $T_{a,b}$ in which a and b range independently over all real numbers (with the exclusion of $a = b = 0$) forms a two-parameter real continuous group which is its own parameter group. While these facts can be readily verified by use of the binary transformations $T_{a,b}$ (and that method is recommended to the beginner as a desirable exercise), they follow at once from the earlier work, in which z is now interpreted to be a complex variable and c a complex parameter.

To the linear algebra of ordinary complex numbers $a + bi$, with real *coordinates* a, b and two *units* 1, i, therefore corresponds a two-parameter group of binary linear transformations $T_{a,b}$ in which the parameters a and b enter linearly and homogeneously, and such that the group is its own parameter group. Given, conversely, a group of this character, we can exhibit a corresponding linear associative algebra, the product of any two hypercomplex numbers c and z of which is the number z' such that the expanded form of the relation $z' = cz$ is that transformation of the group whose parameters are the coordinates of c. Additional simple illustrations of this statement are given in the following sections.

3. We shall obtain an important algebra by considering the linear transformations which leave unaltered the quadric surface S defined by

$$\begin{vmatrix} x_1 & x_2 \\ x_3 & x_4 \end{vmatrix} = 0.$$

The four variables and the coefficients of the transformations may be taken to be real numbers or to be ordinary complex numbers; either interpretation may be made by the reader, but the one chosen is to be retained throughout the discussion.

The surface S contains two sets of straight lines

$$L_k: \qquad x_1 = kx_3, \quad x_2 = kx_4,$$

$$\lambda_k: \qquad x_1 = kx_2, \quad x_3 = kx_4.$$

A linear transformation which replaces every plane through L_k by a plane through L_k is such that

$$x_1' - kx_3' = y_1(x_1 - kx_3) + y_3(x_2 - kx_4),$$

$$x_2' - kx_4' = y_2(x_1 - kx_3) + y_4(x_2 - kx_4),$$

in which $y_1, \cdots, y_4$ are linear functions of k. Let the trans-

formation leave unaltered three lines L_k. Then the preceding equations, quadratic in k, hold for three values of k and hence are identities in k. Since the left members are linear in k, we see that $y_1, \cdots, y_4$ are independent of k. Hence a linear transformation which leaves unaltered three lines L_k leaves unaltered every line L_k and is of the form

$$T_y: \quad \begin{aligned} x_1' &= y_1x_1 + y_3x_2, \quad x_3' = y_1x_3 + y_3x_4, \\ x_2' &= y_2x_1 + y_4x_2, \quad x_4' = y_2x_3 + y_4x_4, \end{aligned}$$

in which the parameters $y_1, \cdots, y_4$ are such that

$$y_1y_4 - y_2y_3 \neq 0.$$

If two transformations leave every L_k unaltered, their product leaves every L_k unaltered. Hence the set of all transformations T_y forms a group G. The direct verification of this fact will lead also to another needed property. The product $T_yT_{y'}$ is found to be $T_{y''}$, where

$$\begin{aligned} y_1'' &= y_1'y_1 + y_3'y_2, \quad y_3'' = y_1'y_3 + y_3'y_4, \\ y_2'' &= y_2'y_1 + y_4'y_2, \quad y_4'' = y_2'y_3 + y_4'y_4. \end{aligned}$$

These equations define a transformation with the parameters $y_1', \cdots, y_4'$ from the variables $y_1, \cdots, y_4$ to the variables $y_1'', \cdots, y_4''$; under this interpretation, the transformation is the same as $T_{y'}$, apart from the notation of the variables. Hence G is its own parameter group. According to the general statement at the end of § 2, the group G should correspond to a linear associative algebra. As the general element (or hypercomplex number*) of the algebra, we may take the matrix

$$x = \begin{Vmatrix} x_1 & x_2 \\ x_3 & x_4 \end{Vmatrix}.$$

The product xy is defined to be the matrix x' in which $x_1', \cdots, x_4'$ are given by the equations marked T_y. Hence the group G defines the algebra whose elements are the matrices x; the general transformation T_y of G is merely the expanded form of the relation $x' = xy$ between matrices.

* For the exhibition of x as a linear combination of four units and the resulting linear aspect of the algebra, see the writer's Linear Algebras, Cambridge Tracts, 1914, pp. 3–5, p. 59.

Consider the product $\xi = yx$ of the same factors taken in reverse order. We obtain the transformation

$$T'_y: \quad \begin{aligned} \xi_1 &= y_1x_1 + y_2x_3, \quad \xi_2 = y_1x_2 + y_2x_4, \\ \xi_3 &= y_3x_1 + y_4x_3, \quad \xi_4 = y_3x_2 + y_4x_4. \end{aligned}$$

All such transformations form a group G'. This fact can be verified as above by forming the product $T'_yT'_{y'}$, or by showing that the T'_y leave unaltered every line λ_k and give all the linear transformations leaving unaltered every λ_k, or by the following third method. The product of T'_y, given by $\xi = yx$, and $T'_{y'}$, given by $\xi' = y'\xi$, is found by the elimination of ξ. Since $y'(yx) = (y'y)x$, the product is $T'_{y''}$, given by $\xi' = y''x$, where $y'' = y'y$.

Each transformation of G is commutative with each transformation of G' since $T_yT'_{y_1}$ is $\xi = y_1(xy)$, while $T'_{y_1}T_y$ is $\xi' = (y_1x)y$. The transformations of G and G' therefore generate the group Γ of the linear transformations $x' = y_1xy$. Suppose that this transformation is identical with $x' = Y_1xY$. Then $xA = Bx$ for every x, where $A = yY^{-1}$, $B = y_1^{-1}Y_1$. As is easily verified, the identity in x gives

$$A = B = \begin{Vmatrix} c & 0 \\ 0 & c \end{Vmatrix} \equiv S_c.$$

Then $Y = S_{c^{-1}}y$, $Y_1 = y_1S_c$. Hence Γ is a seven-parameter group.

To complete the discussion, we shall prove that the only linear transformations leaving the quadric surface S unaltered (i. e., automorphs of S) are the transformations of Γ (which permute the lines L_k among themselves and the lines λ_k among themselves) and their products by any one transformation, as (x_2x_3), which interchanges the two sets of lines. Let T be any linear automorph of S. If T replaces only a finite number of lines L_k by lines L_κ, it replaces an infinitude of lines L_k by lines λ_κ, so that the product of T by (x_2x_3) replaces an infinitude of lines L_k by lines L_κ. Hence either T itself or its product by (x_2x_3) is an automorph t which replaces an infinitude of lines L_k by lines L_κ. But we can find a transformation T'_y which replaces any three distinct lines L_k by any three distinct lines L_κ. This will evidently follow if we prove that there exists a transformation T'_y which replaces L_0, L_∞, L_1 by L_a, L_b, L_c, respectively, where a, b, c are any three distinct numbers; the conditions are

$$\frac{y_2}{y_4} = a, \quad \frac{y_1}{y_3} = b, \quad \frac{y_1 + y_2}{y_3 + y_4} = c,$$

and are satisfied when

$$y_4 = 1, \quad y_2 = a, \quad y_3 = \frac{c - a}{b - c}, \quad y_1 = by_3.$$

The product of t by the inverse of the first T'_y leaves unaltered three lines L_k and hence is a transformation T_y, as proved above. Thus t is in the group Γ and hence either T is in Γ or T is the product of a transformation of Γ by (x_2x_3).

The group of all linear automorphs of S is therefore of the kind called a mixed group. It is however determined in a very simple manner from the continuous seven-parameter subgroup Γ composed of the transformations $x' = y_1xy$. As in this instance, the introduction of hypercomplex numbers enables us to give a very compact and convenient notation for the transformations of important groups.

4. From the preceding algebra whose elements are matrices we can derive in a very natural manner the algebra of quaternions and deduce as corollaries several important results. To this end we take the interpretation which assigns ordinary complex values to the variables and coefficients of the transformations in § 3. To transform the equation of the quadric surface into

$$X_1^2 + X_2^2 + X_3^2 + X_4^2 = 0,$$

we have merely to write

$$x_1 = X_1 + iX_4, \quad x_4 = X_1 - iX_4, \quad x_2 = -X_2 + iX_3,$$
$$x_3 = X_2 + iX_3.$$

The new form of transformation T_y involves the parameters only in the combinations $y_4 \pm y_1$, $y_2 \pm y_3$. Hence we write

$$y_4 + y_1 = 2Y_4, \quad y_4 - y_1 = 2iY_1, \quad y_2 - y_3 = 2Y_3,$$
$$y_2 + y_3 = 2iY_2.$$

In terms of the new variables and parameters, T_y becomes

$$t_Y: \quad \begin{aligned} X_1' &= X_4Y_1 - X_3Y_2 + X_2Y_3 + X_1Y_4, \\ X_2' &= X_3Y_1 + X_4Y_2 - X_1Y_3 + X_2Y_4, \\ X_3' &= -X_2Y_1 + X_1Y_2 + X_4Y_3 + X_3Y_4, \\ X_4' &= -X_1Y_1 - X_2Y_2 - X_3Y_3 + X_4Y_4. \end{aligned}$$

The identical transformation $X_1' = X_1$, etc., is obtained by taking $Y_1 = Y_2 = Y_3 = 0$, $Y_4 = 1$. To our group therefore corresponds a linear associative algebra whose general number is

$$X = X_1 i + X_2 j + X_3 k + X_4,$$

where the products of the units $i, j, k, 1$ are such that

$$XY = X' \equiv X_1' i + X_2' j + X_3' k + X_4',$$

in which the values of $X_1', \cdots, X_4'$ are given by t_Y. Taking $X_1 = Y_1 = 1$, $X_s = Y_s = 0$ $(s = 2, 3, 4)$, we find that $ii = -1$. In this way, we get

$$Q: \quad \begin{aligned} i^2 = j^2 = k^2 = -1, \quad ij = k, \quad ji = -k, \\ jk = i, \quad kj = -i, \quad ki = j, \quad ik = -j. \end{aligned}$$

We thus obtain the algebra of quaternions with ordinary complex coordinates. In view of its origin it is equivalent under a linear transformation on the units to the algebra of matrices with complex coordinates (§ 3). It has as a sub-algebra the system of real quaternions.

The transformation t_Y leaves the quadric surface unaltered. By finding the coefficient of X_1^2, we see that

$$\sum_{s=1}^{4} X_s'^2 = \sum_{s=1}^{4} Y_s^2 \cdot \sum_{s=1}^{4} X_s^2.$$

The left member is called the *norm* of the quaternion X'. Since the transformation is $X' = XY$, we conclude that the norm of the product of two quaternions equals the product of their norms.

By interchanging X_s and Y_s $(s = 1, 2, 3, 4)$ in t_Y, we obtain the transformation t_Y' which has the more compact notation $X' = YX$. The product of the commutative transformations t_Y and t_{Y_1}' is $X' = Y_1 X Y$. The latter form a seven-parameter continuous group Γ. The determinant of each of its real transformations is positive, since the determinant of T_y in § 3 is the square of

$$y_1 y_4 - y_2 y_3 = Y_1^2 + Y_2^2 + Y_3^2 + Y_4^2.$$

To $(x_2 x_3)$ corresponds the transformation τ which changes the sign of X_2 without altering X_1, X_3, X_4. The only linear automorphs of the surface are the transformations of Γ and

their products by τ (§ 3), these products having negative determinants. In four-dimensional space these products are reflexions, so that the group generated by the rotations around the origin and the stretchings from it is formed of the transformations $q' = q_1 q q_2$, where q and q' are variable real quaternions, while q_1 and q_2 are real quaternion parameters. Concerning this group, the corresponding one in three dimensons, and references on related subjects, see Linear Algebras, page 61.

5. Our final illustration will be more typical of the general theory since it treats a group not initially its own parameter group. Consider any two-parameter binary linear group in which the parameters Y_1, Y_2 enter linearly and homogeneously. Its transformations are therefore of the form

$$x_1' = (AY_1 + BY_2)x_1 + (CY_1 + DY_2)x_2,$$
$$x_2' = (EY_1 + FY_2)x_1 + (GY_1 + HY_2)x_2.$$

Let $Y_1 = a$, $Y_2 = b \neq 0$ be the values of the parameters giving the identical transformation. Introduce the new parameters

$$y_1 = bY_1 - aY_2, \quad y_2 = Y_2/b.$$

Then the values $y_1 = 0$, $y_2 = 1$ give the identical transformation. The new equations of our transformations will be of the above form, in which now $B = H = 1$, $D = F = 0$. Further, we set $AY_1 + Y_2 = y_2$, $Y_1 = y_1$. Hence the transformation becomes

$$T_y: \quad x_1' = y_2 x_1 + c y_1 x_2, \quad x_2' = a y_1 x_1 + (d y_1 + y_2) x_2.$$

The product $T_y T_{y'}$ is seen to be $T_{y''}$, where

$$P: \quad y_1'' = (y_2' + d y_1') y_1 + y_1' y_2, \quad y_2'' = ac y_1' y_1 + y_2' y_2.$$

Hence the totality of transformations T_y forms a group G. Regarding y_1' and y_2' as the parameters, we have the general transformation of the parameter group of G. Thus G is its own parameter group only when $d = 0$, $c = 1$.

Without loss of generality we may take $c = 1$. If $c \neq 0$, this may be done by taking cy_1 as a new y_1. If $c = 0$, $a \neq 0$, we interchange x_1 and x_2 and take $dy_1 + y_2$ as a new y_2, obtaining T_y with $c \neq 0$. If $c = a = 0$, the case $d = 0$ is excluded since the group has two parameters, so that $dy_1 + y_2$ may be taken as the new y_1. Then

$$g: \quad x_1' = y_2 x_1, \quad x_2' = y_1 x_2.$$

Using the new variables $X_1 = x_1 + x_2$, $X_2 = x_1 - x_2$ and new parameters $Y_1 = (y_2 - y_1)/2$, $Y_2 = (y_2 + y_1)/2$, we get

$$g': \qquad X_1' = Y_2X_1 + Y_1X_2, \quad X_2' = Y_1X_1 + Y_2X_2,$$

which is of type T_Y with $c = a = 1$, $d = 0$.

There is a general method of selecting new variables X_1 and X_2* such that the group on the new variables will become its own parameter group. In the equations for T_y we have only to erase the accents in the left members, replace y_1, y_2 by X_1, X_2 and give to x_1, x_2 such special values that the resulting equations are independent. We may take $x_1 = 0$, $x_2 = 1$, and get

$$x_1 = X_1, \quad x_2 = dX_1 + X_2.$$

Expressed in the new variables, the transformation T_y (with $c = 1$) becomes

$$t_y: \quad X_1' = (y_2 + dy_1)X_1 + y_1X_2, \quad X_2' = ay_1X_1 + y_2X_2.$$

In view of P, the group of these transformations is its own parameter group. For $y_1 = 0$, $y_2 = 1$, the transformation is identity. Hence we obtain an algebra with units e, ϵ, where ϵ is the principal unit, such that, if $y = y_1e + y_2\epsilon$ is its general number, $Xy = X'$, where the coordinates of X' are defined by t_y. The multiplication table is therefore

$$\epsilon^2 = \epsilon, \quad \epsilon e = e\epsilon = e, \quad e^2 = de + a\epsilon.$$

Taking $e - \frac{1}{2}d\epsilon$ as a new e, we have $d = 0$. Then multiplying e by r, we see that a is replaced by r^2a, which may be made equal to 0 or 1 by choice of r. Hence there are just two types of binary algebras with complex coordinates and having a principal unit.

The corresponding groups are composed of the transformations t_y, with $d = 0$, $a = 0$ or 1. That with $a = 1$ is g' and was seen to be equivalent to g. Hence every binary linear group in which the two parameters enter linearly and homogeneously is equivalent to g or to the group h of transformations t_y with $a = d = 0$.

Scheffers proceeded in the reverse order. Making use of Lie's determination of all types of binary linear groups, he selected the two-parameter groups in which the parameters

* Lie-Scheffers, Continuierliche Gruppen, 1893, p. 634.

enter linearly and homogeneously, found their finite equations, and introduced variables such that each group becomes its own parameter group. The resulting groups (l. c., page 648, bottom, and page 649) are our h and g. From these he derived the above two algebras.

6. Scheffers' determination (pages 654–6) of the algebra of quaternions is based upon the existence of the group of transformations t'_Y of § 4. In a rather arbitrary manner he selected four infinitesimal transformations out of an aggregate of the ∞^6 infinitesimal automorphs of the quadric surface, and verified that the four generate a four-parameter group. The guide to this seemingly fortunate selection may well have been the previous knowledge of the group defined by the algebra of quaternions. The above discussion in § 4 not only gives a natural derivation of quaternions from the theory of groups but leads to the total group of automorphs of a quadric surface and not merely to its continuous subgroup.

THE UNIVERSITY OF CHICAGO.

AN ASPECT OF THE LINEAR CONGRUENCE WITH APPLICATIONS TO THE THEORY OF FERMAT'S QUOTIENT.

BY MR. H. S. VANDIVER.

(Read before the American Mathematical Society, August 4, 1915.)

IN 1903, Professor G. D. Birkhoff communicated to me the following theorem:

If p is a prime integer and a is a positive integer prime to p, then there is at least one and not more than two sets (x, y) such that

$$a \equiv \pm x/y \pmod{p}$$

where x and y are integers prime to each other and $0 < x < \sqrt{p}$, $0 < y < \sqrt{p}$.

Professor Birkhoff has kindly allowed me to use this result, and in the present paper I shall give a proof of the theorem which involves a continued fraction algorithm for a direct determination of each set. Some extensions and applications are also given.