

Proof of the Third Fundamental Theorem in Lie's Theory of Continuous Groups. By J. E. CAMPBELL. Read January 10th, 1901. Received January 12th, 1901.

If we have any set of r^3 constants, $c_{i\kappa h} \dots$, satisfying the conditions

$$c_{i\kappa h} + c_{\kappa i h} = 0,$$

$$\sum_{h=1}^{h=r} (c_{i\kappa h} c_{hjt} + c_{\kappa j h} c_{hit} + c_{jih} c_{h\kappa t}) = 0$$

$$(i, \kappa, j, t = 1, \dots, r), \quad (1)$$

they are said to form a set of composition constants of the r -th order; and the third fundamental theorem in Lie's theory of continuous groups is that, given any such set, r independent infinitesimal transformations

$$X_1, \dots, X_r$$

can be found, such that

$$X_i X_\kappa - X_\kappa X_i = c_{i\kappa 1} X_1 + \dots + c_{i\kappa r} X_r;$$

and therefore such that they generate a group of the given composition.

Lie gives a proof of this proposition in the second volume (seventeenth chapter) of *Transformationsgruppen*, but it requires a considerable previous knowledge of his theory of function groups to follow it; and a proof has also been given by Herr Schur, which is sketched in the third volume, § 144. Recently M. Poincaré has discussed the theorem in the *Trans. of the Camb. Phil. Soc.*, Vol. XVIII., p. 234, and given a proof of the soundness of which I do not feel sure. He has shown how to construct r infinitesimal transformations which are independent; to verify their group property is not easy, and would, in effect, be Schur's method; if this property is not verified independently, the reasoning which occurs on p. 234—"Let

$$e^V e^T = e^W, \quad e^W e^U = e^Z, \quad e^T e^U = e^Y,$$

where $U = \sum u_\kappa X_\kappa, \quad Z = \sum z_\kappa X_\kappa, \quad Y = \sum y_\kappa X_\kappa;$

the associative character of the operations shows us that we have

$$e^V e^Y = e^Z,$$

where

$$w_{\kappa} = \phi_{\kappa}(v_i, t_i), \quad y_{\kappa} = \phi_{\kappa}(t_i, u_i),$$

$$Z_{\kappa} = \phi_{\kappa}(w_i, u_i) = \phi_{\kappa}(v_i, y_i)''$$

—seems to presuppose the existence of a group of the required composition.

If it is objected that we can let $X_1 \dots X_r$ be the group adjoint, then, unless these operators are independent, we do not know that the associative law holds.

The proof given here is perhaps simpler than those to which I have referred, with the exception of M. Poincaré's, if the latter is correct; in any case the proposition is so important that it may perhaps justify one in giving another proof.

Since writing this paper my attention has been drawn by one of the referees to a proof of this theorem by Klein, in his *Einleitung in die höhere Geometrie*, Vol. II., pp. 163–167, which at first is on the same lines as the proof of this paper, viz., the replacing of the given composition constants by an equivalent but simpler set when the adjoint group is of order less than r . I believe that this proof is erroneous; perhaps the simplest reason for doubting it is that, if correct, it would (as the referee remarked) prove that a group which contains self-conjugate (*ausgereichnete*) operations must be the direct product of two independent groups. Klein assumes, in fact, that the constants which in § 5 I have denoted by $d_{i\kappa m} \dots$ are all zero. I might perhaps add here that the results in §§ 1–3 of my paper are implicitly contained in chapter xvii. of the first volume of the *Transformationsgruppen*.

$$1. \text{ If } w_i = \sum_{\kappa=1}^{\kappa=r} a_{\kappa i} x'_{\kappa} \quad (i = 1, \dots, r)$$

is any linear transformation whose modulus does not vanish, and

$$x'_i = \sum_{\kappa=1}^{\kappa=r} A_{\kappa i} x_{\kappa}$$

the inverse transformation, then $c_{i\kappa h} \dots$ being any r^3 other set of variables, and $c'_{i\kappa h} \dots$ another set connected with the former by the equations

$$\sum_{h=1}^{h=r} a_{hs} c'_{i\kappa h} = \sum_{p,q} a_{ip} a_{\kappa q} c_{pq s} \quad (2)$$

(the summation on the right being for all values of p, q from 1 up to r inclusive, and i, κ, s having any values from 1 up to r inclusive). it is clear that (2) gives $c'_{i\kappa h} \dots$ in terms of $c_{i\kappa h} \dots$.

From the fact that
$$\sum_{p=1}^{p=r} A_{pi} a_{\kappa p} = e_{i\kappa},$$

where $e_{i\kappa}$ is zero if $i \neq \kappa$, and unity if $i = \kappa$, we easily verify that

$$\sum_{h=1}^{h=r} A_{hs} c_{i\kappa h} = \sum_{pq} A_{ip} A_{\kappa q} c'_{pq s};$$

and therefore $c_{i\kappa h} \dots$ are given in terms of $c'_{i\kappa h} \dots$.

2. It must now be proved that, if one set $c_{i\kappa h} \dots$ satisfy the system of equations (1), so will the other $c'_{i\kappa h} \dots$.

To see this, multiply (2) by $a_{tm} c_{smj}$, and sum for all values of h, s, m, p, q , and we get

$$\sum_{h, s, m} a_{hs} a_{tm} c'_{i\kappa h} c_{smj} = \sum_{m, s, p, q} a_{ip} a_{\kappa q} a_{tm} c_{pq s} c_{smj}.$$

Noticing that by (2) the left-hand member may be written

$$\sum_{m, h} a_{mj} c'_{i, \kappa, h} c'_{h, t, m},$$

we see that
$$\sum_{m=1}^{m=r} a_{mj} \sum_{h=1}^{h=r} (c'_{i\kappa h} c'_{h tm} + c'_{\kappa th} c'_{him} + c'_{i, i, h} c'_{h, \kappa, m})$$

is the sum of a number of terms which vanish by the conditions (1).

We conclude therefore that, since the modulus does not vanish,

$$\sum_{h=1}^{h=r} (c'_{i\kappa h} c'_{h tm} + c'_{\kappa th} c'_{him} + c'_{i, i, h} c'_{h, \kappa, m}) = 0$$

for all values of i, κ, m, t .

To prove that $c'_{i\kappa t} + c'_{\kappa it} = 0$,

interchange i, κ in (2); we get

$$\sum_{h=1}^{h=r} a_{hs} c'_{\kappa ih} = \sum_{pq} a_{iq} a_{\kappa p} c_{pq s};$$

adding this equation and (2), we see that

$$c'_{i\kappa t} + c'_{\kappa it} = 0$$

from conditions (1).

3. Suppose now that we have a group with the composition constants $c_{i\kappa h} \dots$, the corresponding infinitesimal transformations being X_1, \dots, X_r .

If we take X'_1, \dots, X'_r as a new set of r independent infinitesimal transformations defined by

$$X'_i = \sum_{\kappa=1}^{\kappa=r} a_{i\kappa} X_{\kappa},$$

then it can be at once verified that $c'_{ik\kappa} \dots$ are the composition constants of the group corresponding to the above infinitesimal transformations; the conclusion we draw is that when we can find a group with the composition constants $c_{ik\kappa} \dots$ it has also the composition constants $c'_{ik\kappa} \dots$, and conversely.

4. Suppose now we are given a set of composition constants $c_{ik\kappa} \dots$, such that all $r-s+1$ rowed determinants, but not all $r-s$ rowed determinants, vanish of the matrix

$$\begin{vmatrix} c_{j1\kappa} & \dots \\ c_{j2\kappa} & \dots \\ \vdots & \dots \\ c_{jr\kappa} & \dots \end{vmatrix}$$

(in any row all positive integral values of j and κ are to be taken from 1 up to r); then we can choose

$$a_{11}, \dots, a_{1r},$$

$$a_{21}, \dots, a_{2r},$$

$$\vdots$$

$$a_{s1}, \dots, a_{sr}$$

so that

$$a_{h1}c_{j1\kappa} + a_{h2}c_{j2\kappa} + \dots + a_{hr}c_{jr\kappa} = 0,$$

where j, κ may have any values from 1 up to r inclusive, and h any value from 1 up to s inclusive.

To complete the determinant of the $a_{p,q}$'s we can take $a_{m\kappa}$ arbitrarily, only providing that the determinant does not vanish ($m = s+1, \dots, r$; $\kappa = 1, \dots, r$).

If we now apply the transformation (2), we get a new set of composition constants $c'_{ik\kappa}$ with the property

$$c'_{ik\kappa} = d_{ik\kappa},$$

where i, κ, h may have any values from $s+1$ up to r , and $d_{ik\kappa}$ are a set of composition constants of the n -th order, n being written for $r-s$;

$$c'_{ik\kappa} = 0,$$

if either i or κ is less than $s+1$, h having any value from 1 up to

r inclusive;

$$c'_{i\kappa m},$$

where i and κ both exceed s , and m does not, being such that

$$c'_{i\kappa m} + c'_{\kappa im} = 0,$$

$$\sum_{h=s+1}^{h=r} (d_{i\kappa h} c'_{hjm} + d_{\kappa jh} c'_{him} + d_{jih} c'_{h\kappa m}) = 0.$$

5. We may therefore say (with the slight change of notation which consists in writing $d_{i\kappa h} = c_{r-i, r-\kappa, r-h}$ and $c'_{i\kappa m} = d_{r-i, r-\kappa, r-m}$) that the problem of finding a group with the given composition is now reduced to that of finding a group with the composition constants

$$d'_{i\kappa h} \dots,$$

where

$$d'_{i\kappa h} = c_{i\kappa h},$$

if none of the suffixes i, κ, h exceed n , and the c 's are composition constants of the n -th order, such that not all n rowed determinants vanish of the matrix

$$\begin{vmatrix} c_{j1\kappa} \dots \\ c_{j2\kappa} \dots \\ \vdots \\ c_{jn\kappa} \dots \end{vmatrix} \quad (j, \kappa = 1, \dots, n); \quad (3)$$

$$d'_{i\kappa h} = 0,$$

if either i or κ exceeds n , h having any value from 1 up to r ;

$$d'_{i\kappa m} = d_{i\kappa m},$$

if neither i nor κ exceeds n , and m does exceed n , and

$$d_{i\kappa m} + d_{\kappa im} = 0,$$

$$\sum_{h=1}^{h=n} (c_{i\kappa h} d_{hjm} + c_{\kappa jh} d_{him} + c_{jih} d_{h\kappa m}) = 0. \quad (4)$$

Now, it may at once be verified that

$$X_1, \dots, X_n,$$

where

$$X_i = \sum_{p,q} c_{piq} x_p \frac{\partial}{\partial x_q}$$

(the summation being for all values of p and q from 1 up to n inclusive), is a group of the n -th order with the composition constants $c_{ih\kappa}$; for, by (3), X_1, \dots, X_n are independent, and by forming its alternants we verify the group property. This is Lie's group adjoint. Its parameter group is simply transitive and of like com-

position with it; we have therefore proved the existence of a simply transitive group with the composition constants $c_{ikh} \dots$.

6. It will now be shown how a simply transitive group with the composition constants $d'_{ikh} \dots$ may be deduced.

Let X_1, \dots, X_n be the simply transitive group with the composition constants $c_{ikh} \dots$.

Let $u_{1m}, u_{2m}, \dots, u_{nm}$ be any set of solutions of the simultaneous equation system

$$X_i u_{\kappa m} - X_\kappa u_{im} = d_{i\kappa m} + \sum_{h=1}^{h=n} c_{ikh} u_{hm}, \quad (5)$$

where i, κ may have all values from 1 up to n , and m has all values from $n+1$ up to r . We can at once verify that

$$X_i + u_{in+1} \frac{\partial}{\partial x_{n+1}} + \dots + u_{ir} \frac{\partial}{\partial x_r} \quad (i = 1, \dots, n),$$

$$\frac{\partial}{\partial x_{n+1}}, \dots, \frac{\partial}{\partial x_r},$$

is a simply transitive group of order r with the composition constants $d'_{ikh} \dots$.

7. We must now prove that the equation system (5) is self-consistent. This may be done by the method explained in the *Proc. of the Lond. Math. Soc.*, Vol. xxxi., p. 235, or independently by a less general but more direct method as follows:—

Since X_1, \dots, X_n is a simply transitive group, $\frac{\partial}{\partial x_1}, \dots, \frac{\partial}{\partial x_n}$ can each be expressed in the form

$$\frac{\partial}{\partial x_i} = \lambda_{i1} X_1 + \dots + \lambda_{in} X_n,$$

where $\lambda_{i\kappa} \dots$ are a known set of functions in x_1, \dots, x_n . From the fact that

$$\frac{\partial}{\partial x_i} \frac{\partial}{\partial x_\kappa} = \frac{\partial}{\partial x_\kappa} \frac{\partial}{\partial x_i},$$

and that X_1, \dots, X_n form a group, we see that $\lambda_{i\kappa} \dots$ are functions satisfying the equation system

$$\frac{\partial \lambda_{j\kappa}}{\partial x_i} - \frac{\partial \lambda_{ji}}{\partial x_\kappa} = \sum_{\alpha, \beta} c_{\alpha\beta} \lambda_{\alpha\kappa} \lambda_{\beta i} \quad (6)$$

(the summation being for all values of α, β from 1 up to n inclusive).

8. It must first be verified that

$$\frac{\partial}{\partial x_i} \Sigma d_{\alpha\beta\gamma} \lambda_{\alpha j} \lambda_{\beta \kappa} + \frac{\partial}{\partial x_j} \Sigma d_{\alpha\beta\gamma} \lambda_{\alpha \kappa} \lambda_{\beta i} + \frac{\partial}{\partial x_{\kappa}} \Sigma d_{\alpha\beta\gamma} \lambda_{\alpha i} \lambda_{\beta j} \quad (7)$$

is identically zero for all values of $ij\kappa$, the summation in Σ being for all values of α, β . We have

$$\begin{aligned} \frac{\partial}{\partial x_i} \lambda_{\alpha j} \lambda_{\beta \kappa} &= \lambda_{\alpha j} \frac{\partial}{\partial x} \lambda_{\beta \kappa} + \lambda_{\beta \kappa} \frac{\partial}{\partial x_i} \lambda_{\alpha i}, \\ \frac{\partial}{\partial x_j} \lambda_{\alpha \kappa} \lambda_{\beta i} &= \lambda_{\alpha \kappa} \frac{\partial}{\partial x_j} \lambda_{\beta i} + \lambda_{\beta i} \frac{\partial}{\partial x_j} \lambda_{\alpha \kappa}, \\ \frac{\partial}{\partial x_{\kappa}} \lambda_{\alpha i} \lambda_{\beta j} &= \lambda_{\alpha i} \frac{\partial}{\partial x_{\kappa}} \lambda_{\beta j} + \lambda_{\beta j} \frac{\partial}{\partial x_{\kappa}} \lambda_{\alpha i}. \end{aligned}$$

Remembering that $d_{\alpha\beta\gamma} + d_{\beta\alpha\gamma} = 0$,

we see that (7) may be written

$$\begin{aligned} \Sigma_{\alpha, \beta} \lambda_{\alpha j} d_{\alpha\beta\gamma} \left(\frac{\partial}{\partial x_i} \lambda_{\beta \kappa} - \frac{\partial}{\partial x_{\kappa}} \lambda_{\beta i} \right) &+ \Sigma_{\alpha, \beta} \lambda_{\beta \kappa} d_{\alpha\beta\gamma} \left(\frac{\partial}{\partial x_i} \lambda_{\alpha j} - \frac{\partial}{\partial x_j} \lambda_{\alpha i} \right) \\ &+ \Sigma_{\alpha, \beta} \lambda_{\beta i} d_{\alpha\beta\gamma} \left(\frac{\partial}{\partial x_j} \lambda_{\alpha \kappa} - \frac{\partial}{\partial x_{\kappa}} \lambda_{\alpha j} \right). \end{aligned}$$

Writing the second and third of these sums in the equivalent forms

$$\Sigma_{\gamma, \beta} \lambda_{\gamma \kappa} d_{\gamma\beta\gamma} \left(\frac{\partial}{\partial x_j} \lambda_{\beta i} - \frac{\partial}{\partial x_i} \lambda_{\beta j} \right)$$

and

$$\Sigma_{b, \beta} \lambda_{bi} d_{b\beta\gamma} \left(\frac{\partial}{\partial x_{\kappa}} \lambda_{\beta j} - \frac{\partial}{\partial x_j} \lambda_{\beta \kappa} \right),$$

and substituting from (6), we see that the coefficient of $\lambda_{\alpha j} \lambda_{\gamma \kappa} \lambda_{bi}$ in (7) is

$$- \sum_{\beta=1}^{\beta=n} (d_{\beta\alpha\gamma} c_{\gamma b\beta} + d_{\beta\gamma\gamma} c_{b\gamma\beta} + d_{\beta b\gamma} c_{\alpha\gamma\beta}),$$

which is zero from (4); and therefore, since all these coefficients vanish, the identical relation required is now proved.

9. In order to prove that the simultaneous equation system (5) can be satisfied, multiply (5) by $\lambda_{ip} \lambda_{\kappa q}$, and sum for all values of i, κ ; then, if the new set of equations—there will be one for each pair of values of p, q —can be satisfied, so can the old; to see this we have only to notice that for the equation with a given pair of values of i, κ the multiplier is $\lambda_{ip} \lambda_{\kappa q} - \lambda_{\kappa p} \lambda_{iq}$, and the determinant of this

cannot vanish since the determinant of λ_{pq} does not vanish (Forsyth, *Differential Equations*, § 212).

Let
$$v_{im} = \lambda_{1i}u_{1m} + \dots + \lambda_{ni}u_{nm} \quad (i = 1, \dots, n);$$

then the simultaneous equation system takes the simple form

$$\frac{\partial}{\partial x_p} v_{qm} - \frac{\partial}{\partial x_q} v_{pm} = \sum_{ik} d_{ikm} \lambda_{ip} \lambda_{kq} = \sigma_{pqm}, \text{ say.} \quad (8)$$

10. To solve these equations, consider the following lemma:—

If we have $\frac{n(n-1)}{2}$ functions $\sigma_{ik} \dots$ of the variables x_1, \dots, x_n such that

$$\begin{aligned} \sigma_{ik} + \sigma_{ki} &= 0, \\ \frac{\partial}{\partial x_i} \sigma_{jk} + \frac{\partial}{\partial x_j} \sigma_{ki} + \frac{\partial}{\partial x_k} \sigma_{ij} &= 0, \end{aligned}$$

where the suffixes may have any values from 1 up to n inclusive, then n functions u_1, \dots, u_n can be found such that

$$\sigma_{ik} = \frac{\partial^2}{\partial x_i \partial x_k} (u_i - u_k).$$

To see that this is true when $n = 3$, let

$$\sigma_{12} = \frac{\partial^2}{\partial x_1 \partial x_2} (u_2 - u_1), \quad \sigma_{13} = \frac{\partial^2}{\partial x_1 \partial x_3} (u_1 - u_3).$$

This is clearly justifiable, and we can take u_1 arbitrarily and obtain u_2 and u_3 by integration.

Since $\sigma_{12} + \sigma_{21} = 0$ and $\sigma_{13} + \sigma_{31} = 0$,

$$\sigma_{21} = \frac{\partial^2}{\partial x_1 \partial x_2} (u_2 - u_1), \quad \sigma_{31} = \frac{\partial^2}{\partial x_1 \partial x_3} (u_3 - u_1).$$

Now
$$\frac{\partial}{\partial x_1} \sigma_{23} + \frac{\partial}{\partial x_2} \sigma_{31} + \frac{\partial}{\partial x_3} \sigma_{12} = 0;$$

therefore
$$\frac{\partial}{\partial x_1} \sigma_{23} + \frac{\partial^3}{\partial x_1 \partial x_2 \partial x_3} (u_3 - u_2) = 0,$$

and therefore
$$\sigma_{23} = \frac{\partial^2}{\partial x_2 \partial x_3} (u_3 - u_2) + f(x_2, x_3).$$

It is clear that we can write $f(x_2, x_3)$ in the form

$$f = \frac{\partial^2}{\partial x_2 \partial x_3} (w_2 - w_3),$$

where w_2 and w_3 are functions of x_2, x_3 only, and w_2 can be taken

arbitrarily and then w_3 be obtained by integration; therefore

$$\sigma_{23} = \frac{\partial^2}{\partial x_2 \partial x_3} (u_3 + w_3 - u_3 - w_3).$$

Since, then, u_3 and w_3 do not involve x_1 , we see that u_1 , $u_2 + w_2$, $u_3 + w_3$ are three functions in terms of which σ_{23} , σ_{31} and σ_{12} can be expressed in the required form.

The extension to n variables is now obvious. Assuming that the theorem has been proved for the case of $n-1$ variables, let

$$\sigma_{1\kappa} = \frac{\partial^2}{\partial x_1 \partial x_\kappa} (u_1 - u_\kappa) \quad (\kappa = 1, \dots, n),$$

where, as before, u_1 is arbitrary.

From
$$\frac{\partial}{\partial x_1} \sigma_{\kappa h} + \frac{\partial}{\partial x_\kappa} \sigma_{h1} + \frac{\partial}{\partial x_h} \sigma_{1\kappa} = 0$$

we get
$$\frac{\partial}{\partial x_1} \sigma_{\kappa h} = \frac{\partial^2}{\partial x_1 \partial x_\kappa \partial x_h} (u_\kappa - u_h),$$

and therefore
$$\sigma_{\kappa h} = \frac{\partial^2}{\partial x_\kappa \partial x_h} (u_\kappa - u_h) + \rho_{\kappa h},$$

where $\rho_{\kappa h}$ is a function of x_2, \dots, x_n , only.

We now have

$$\begin{aligned} \rho_{\kappa h} + \rho_{h\kappa} &= 0, \\ \frac{\partial}{\partial x_i} \rho_{\kappa h} + \frac{\partial}{\partial x_h} \rho_{\kappa i} + \frac{\partial}{\partial x_\kappa} \rho_{ih} &= 0 \quad (i, h, \kappa = 2, \dots, n); \end{aligned}$$

and therefore, since we now have only $n-1$ variables,

$$\rho_{\kappa h} = \frac{\partial^2}{\partial x_h \partial x_\kappa} (w_\kappa - w_h),$$

where w_2, \dots, w_n do not involve x_1 .

It follows, as before, that

$$u_1, u_2 + w_2, \dots, u_n + w_n$$

will be a set of functions in terms of which we can express in the required manner $\sigma_{i\kappa} \dots$.

We can now write down the solutions of (8); for we have

$$\begin{aligned} \sigma_{i\kappa m} + \sigma_{\kappa i m} &= 0, \\ \frac{\partial}{\partial x_i} \sigma_{j\kappa m} + \frac{\partial}{\partial x_j} \sigma_{\kappa i m} + \frac{\partial}{\partial x_\kappa} \sigma_{ij m} &= 0; \end{aligned}$$

the first being true, since $d_{i\kappa m} + d_{\kappa i m} = 0$, and the second being

merely the identity (7); and therefore by the above reasoning we can write

$$\sigma_{ikm} = \frac{\partial^2}{\partial x_i \partial x_k} (V_{im} - V_{km}),$$

where $V_{ik} \dots$ are a set of functions obtainable by quadratures; then

$$v_{im} = -\frac{\partial}{\partial x_i} V_{im}$$

is clearly a system of solutions of the system (8).

We have thus proved that, given any set of composition constants, we can in all cases obtain a simply transitive group of that composition; and that the process of obtaining it involves merely algebraic operations and quadratures.

On some cases of the Solution of the Congruence $z^{p^n-1} \equiv 1, \text{ mod } p$.

By F. S. CAREY. Received January 2nd, 1901. Communicated January 10th, 1901.

Let p be a prime, and x, y integers chosen from amongst

$$0, \pm 1, \pm 2, \dots, \pm \frac{1}{2}(p-1);$$

further, let j be a quantity such that j^2 is congruent to a certain selected quadratic non-residue of p ; then $x+yj$ is a symbol which includes p^2 numbers; also for the same modulus p all such numbers are represented by a single j ; to prove this, it is sufficient to remark that, if b_1 and b_2 are two quadratic non-residues, and $b_1 = j_1^2$, $b_2 = j_2^2$, then, since $b_1 \equiv a^2 b_2$, it follows that $j_1 = aj_2$ and the p^2 numbers $x+yj_1$ are identical with the p^2 numbers $x+yj_2$. In case $p = 4n+1$, -1 is a non-residue, and the symbol i is used instead of j .

The objects of this paper are (1) to discuss the solution of $z^{p^n} \equiv z,^*$ mod p , by means of the numbers $x+yj$; (2) to discuss the solution of $z^{p^n} \equiv z$, when p^3-1 is divisible by n ; (3) to examine the reduction

* Reference may be made to Serret, *Cours d'Algebre superieure*, section iii., chapter iii.