659.

A THEOREM ON GROUPS.

[From the *Mathematische Annalen*, t. XIII. (1878), pp. 561—565.]

THE following theorem is very simple; but it seems to belong to a class of theorems, the investigation of which is desirable.

I consider a substitution-group of a given order upon a given number of letters; and I seek to *double* the group, that is to derive from it a group of twice the order upon twice the number of letters. This can be effected for *any* group, in a manner which is self-evident and in nowise interesting: but in a different manner for a *commutative* group (or group such that any two of its substitutions satisfy the condition $AB = BA$): it is to be observed that the double group is not in general commutative.

Let the letters of the original group be *abcde* ..., we may for shortness write $U = abcde\ldots$; and take U as the primitive arrangement: and let the group then be $1, A, B, \ldots$ where $A, B, \ldots$ represent substitutions: the corresponding arrangements are $U, AU, BU, \ldots$ and these may for shortness be represented by $1, A, B, \ldots$; viz. $1, A, B, \ldots$ represent, properly and in the first instance, substitutions; but when it is explained that they represent arrangements, then they represent the arrangements $U, AU, BU, \ldots$.

For the double group the letters are taken to be $a_1b_1c_1d_1e_1\ldots$ and $a_2b_2c_2d_2e_2\ldots$, $= U_1$ and U_2 suppose, and U_1U_2 is regarded as the primitive arrangement; A_1 and A_2 denote the same substitutions in regard to U_1 and U_2 respectively, that A denotes in regard to U: and so for B_1, B_2, etc.; moreover 12 denotes the substitution $(a_1a_2)(b_1b_2)(c_1c_2)(d_1d_2)(e_1e_2)\ldots$, or interchange of the suffixes 1 and 2. The substitutions A_1, A_2, or any powers of these A_1^α, A_2^β, are obviously commutative; applying them to the primitive arrangement U_1U_2, we have $A_1^\alpha A_2^\beta U_1U_2$ and $A_2^\beta A_1^\alpha U_1U_2$ each $= A_1^\alpha U_1 A_2^\beta U_2$. But A_1^α, A_2^β are not commutative with 12: we have for instance $12A_1^\alpha . U_1U_2 = 12A_1^\alpha U_1 . U_2 = A_1^\alpha U_2 . U_1$, but $A_1^\alpha 12 U_1U_2 = A_1^\alpha . U_2U_1 = U_2 . A_1^\alpha U_1$. If instead of the substitutions we consider the arrangements obtained by operating upon U_1U_2, then we may for shortness consider for instance A_1A_2 as denoting the arrangement $A_1U_1 . A_2U_2$. But observe that in this use of the symbols the A_1, A_2 are not commutative, A_2A_1 would denote the different arrangement $A_2U_2 . A_1U_1$: in this use of the symbols, 1 would denote U_1U_2, and 12 would denote U_2U_1, but it would be clearer to use 12, 21 as denoting U_1U_2 and U_2U_1 respectively.

These explanations having been given, I remark that in every case the substitution-group 1, A, B,... gives the double group

$$\begin{array}{lll} 1, & A_1A_2, & B_1B_2, \ldots \\ 12, & 12A_1A_2, & 12B_1B_2, \ldots \end{array}$$

as is at once seen to be true: but further when the original group 1, A, B, ... is commutative, then if m be any integer number, such that $m^2 \equiv 1$ (mod. the order of the original group), we have also the double group

$$\begin{array}{lll} 1, & A_1A_2^m, & B_1B_2^m, \ldots \\ 12, & 12A_1A_2^m, & 12B_1B_2^m, \ldots \end{array}$$

where of course if the order of the original group ($=\mu$ suppose) be prime, we have $m \equiv 1$ or else $m \equiv -1$ (mod. μ), say $m = 1$ or $\mu - 1$; but if the order μ be composite, then the number of solutions may be greater.

The condition in order to the existence of the double group of course is that, in the system of substitutions just written down, the combination of any two substitutions may give a substitution of the system. And this is in fact the case in virtue of the formulæ

$$\begin{array}{ll} 1^\circ. & A_1A_2^m \,.\, \quad B_1B_2^m = A_1B_1\,(A_2B_2)^m, \\ 2^\circ. & A_1A_2^m \,.\, 12B_1B_2^m = 12A_1^mB_1\,(A_2^mB_2)^m, \\ 3^\circ. & 12A_1A_2^m \,.\, \quad B_1B_2^m = 12\,(A_1B_1)\,(A_2B_2)^m, \\ 4^\circ. & 12A_1A_2^m \,.\, 12B_1B_2^m = A_1^mB_1\,(A_2^mB_2)^m, \end{array}$$

inasmuch as 1, A, B,... being a group, AB and A^mB are each of them a substitution of the group, $= C$ suppose; we have of course in like manner $A_1B_1 = C_1$, $A_2B_2 = C_2$, etc., and the right-hand sides of the four formulæ are thus of the forms $C_1C_2^m$, $12C_1C_2^m$, $12C_1C_2^m$, $C_1C_2^m$ respectively, viz. these are substitutions of the system.

To prove for instance the formula 2°, considering the arrangements obtained by operating upon U_1U_2, we have

$$B_1B_2^mU_1U_2 = B_1B_2^m,\ 12B_1B_2^mU_1U_2 = B_2B_1^m,\quad A_1A_2^m\,12B_1B_2^mU_1U_2 = A_2^mB_2\,A_1B_1^m,$$

where of course the expressions on the right-hand side denote arrangements. By reason that the original group is commutative $(A^mB)^m$ is $= A^{m^2}B^m$ or since $m^2 \equiv 1$ (mod. μ) this is $= AB^m$; hence also $(A_2^mB_2)^m = A_2B_2^m$: hence, considering as before the arrangements obtained by operating on U_1U_2, we have

$$(A_2^m B_2)^m\, U_1 U_2 = 1\,.\,A_2 B_2^m\,;\;\; A_1^m B_1\,(A_2^m B_2)^m\, U_1 U_2 = A_1^m B_1 A_2 B_2^m,$$

and

$$12 A_1^m B_1\,(A_2^m B_2)^m\, U_1 U_2 = A_2^m B_2 A_1 B_1^m,$$

where of course the right-hand sides denote arrangements. Hence in the formula 2°, the two substitutions operating on $U_1 U_2$ give each of them the same arrangement $A_2^m B_2 A_1 B_1^m$, that is, the two substitutions are equal. And similarly the other formulæ 1°, 3°, 4° may be proved.

By interchanging A and B, in the formulæ I obtain

$$1°.\quad A_1 A_2^m\,.\quad B_1 B_2^m = \quad A_1 B_1\,(A_2 B_2)^m\,;$$

$$B_1 B_2^m\,.\quad A_1 A_2^m = \quad B_1 A_1\,(B_2 A_2)^m = A_1 B_1\,(A_2 B_2)^m,$$

which is

$$= \quad A_1 A_2^m\,.\,B_1 B_2^m\,;$$

$$2° \text{ and } 3°.\quad A_1 A_2^m\,.\,12 B_1 B_2^m = 12 A_1^m B_1\,(A_2^m B_2)^m\,;$$

$$12 B_1 B_2^m\,.\quad A_1 A_2^m = 12 B_1 A_1\,(B_2 A_2)^m = 12 A_1 B_1\,(A_2 B_2)^m,$$

which is not

$$= \quad A_1 A_2^m\,.\,12 B_1 B_2^m\,;$$

$$3° \text{ and } 2°.\quad 12 A_1 A_2^m\,.\quad B_1 B_2^m = 12 A_1 B_1\,(A_2 B_2)^m\,;$$

$$B_1 B_2^m\,.\,12 A_1 A_2^m = 12 A_1 B_1^m\,(A_2 B_2^m)^m = 12 A_1 B_1^m\, A_2^m B_2,$$

which is not

$$= 12 A_1 A_2^m\,.\,B_1 B_2^m\,;$$

$$4°.\quad 12 A_1 A_2^m\,.\,12 B_1 B_2^m = \quad A_1^m B_1\,(A_2^m B_2)^m\,;$$

$$12 B_1 B_2^m\,.\,12 A_1 A_2^m = \quad A_1 B_1^m\,(A_2 B_2^m)^m = (A_1^m B_1)^m\, A_2^m B_2,$$

which is not

$$= 12 A_1 A_2^m\,.\,12 B_1 B_2^m.$$

That is, in the double group any two substitutions of the form $A_1 A_2^m$ are commutative, but a substitution of this form is not in general commutative with a substitution of the form $12 B_1 B_2^m$, nor are two substitutions of the last-mentioned form $12 A_1 A_2^m$ in general commutative with each other; hence the double group is not in general commutative.

In the formula 4°, writing $B = A$, we have

$$(12 A_1 A_2^m)^2 = A_1^{m+1}\, A_2^{m^2+m} = A_1^{m+1}\,.\,A_2^{m+1}\,;$$

hence, if λ is the least integer value such that

$$\lambda\,(m+1) \equiv 0 \pmod{\mu},$$

we have $(12 A_1 A_2^m)^{2\lambda} = 1$, viz. in the double group the substitutions of the second row are each of them of an order not exceeding 2λ, the substitution 12 being of course of the order 2. In particular, if $m = \mu - 1$, then $\lambda = 1$: and the substitutions of the second row are each of them of the order 2.

As the most simple instance of the theorem, suppose that the original group is the group 1, (abc), (acb), or say 1, Θ, Θ^2, of the cyclical substitutions upon the 3 letters abc. Here $m^2 \equiv 1$ (mod. 3) or except $m = 1$ the only solution is $m = 2$, and thence $\lambda = 1$. The double group is a group of the order 6 on the letters $a_1b_1c_1a_2b_2c_2$: viz. writing $\Theta = (abc)$, and therefore $\Theta_1 = (a_1b_1c_1)$, $\Theta_1^2 = (a_1c_1b_1)$, $\Theta_2 = (a_2b_2c_2)$, $\Theta_2^2 = (a_2c_2b_2)$, also writing $12 = \alpha$, the substitutions are

$$1,\quad \Theta_1\Theta_2^2,\quad \Theta_1^2\Theta_2,$$

$$\alpha,\quad \alpha\Theta_1\Theta_2^2,\quad \alpha\Theta_1^2\Theta_2,$$

the arrangements corresponding to the second row of substitutions are $a_2b_2c_2a_1b_1c_1$, $b_2c_2a_2c_1a_1b_1$, $c_2a_2b_2b_1c_1a_1$, viz. the substitutions are $(a_1a_2)(b_1b_2)(c_1c_2)$, $(a_1b_2)(b_1c_2)(c_1a_2)$, $(a_1c_2)(b_1a_2)(c_1b_2)$, each of them of the second order as they should be.

I take the opportunity of mentioning a further theorem. Let μ be the order of the group, and a the order of any term A thereof, a being of course a submultiple of μ: and let the term A be called quasi-positive when $\mu\left(1 - \frac{1}{a}\right)$ is even, quasi-negative when $\mu\left(1 - \frac{1}{a}\right)$ is odd. The theorem is that the product of two quasi-positive terms, or of two quasi-negative terms, is quasi-positive; but the product of a quasi-positive term and a quasi-negative term is quasi-negative. And it follows hence that, either the terms of a group are all quasi-positive, or else one half of them are quasi-positive and the other half of them are quasi-negative.

The proof is very simple: a term A of the group operating on the μ terms $(1, A, B, C, \ldots)$ of the group, gives these same terms in a different order, or it may be regarded as a substitution upon the μ symbols $1, A, B, C, \ldots$; so regarded it is a *regular* substitution (this is a fundamental theorem, which I do not stop to prove), and hence since it must be of the order a it is a substitution composed of $\frac{\mu}{a}$ cycles, each of a letters. But in general a substitution is positive or negative according as it is equivalent to an even or an odd number of inversions; a cyclical substitution upon a letters is positive or negative according as $a - 1$ is even or odd; and the substitution composed of the $\frac{\mu}{a}$ cycles is positive or negative according as $\frac{\mu}{a}(a-1)$, that is, $\mu\left(1 - \frac{1}{a}\right)$, is even or odd. Hence by the foregoing definition, the term A, according as it is quasi-positive or quasi-negative, corresponds to a positive substitution or to a negative substitution; and such terms combine together in like manner with positive and negative substitutions.

Cambridge, 3rd April, 1878.