

## ILLUSTRATIONS OF SYLOW'S THEOREMS ON GROUPS.

By Prof. Cayley.

THE theorems 1, 2, and 3 in the paper Sylow "Théorèmes sur les groupes de Substitutions," *Math. Ann.* t. v. (1872), pp. 584-594 apply to groups in general, and not only to groups of Substitutions. They are as follows:

**THEOREM 1.** If  $n^a$  be the highest power of the prime number  $n$  which divides the order of a group  $G$ , this group contains a group  $g$  of the order  $n^a$ : if, moreover,  $n^a v$  is the order of the highest group contained in  $G$ , the operations whereof are permutable with the group  $g$ , then the order of  $G$  is of the form  $n^a v (nk + 1)$ . [I write  $k$  for Sylow's  $p$ , since it is convenient to have  $p$  to denote a prime number, and for Sylow's "Substitutions" I write "Operations."]

**THEOREM 2.** Everything being as in the preceding theorem, the group  $G$  contains precisely  $nk + 1$  distinct groups of the order  $n^a$ , and these are obtained by transforming any one of them by the operations of  $G$ , each group being given by  $n^a v$  distinct transformations.

**THEOREM 3.** If the order of a group is  $n^a$ ,  $n$  being prime, then any operation  $\mathcal{S}$  whatever of the group may be expressed by the formula

$$\mathcal{S} = \theta_0^i \theta_1^k \theta_2^l \dots \theta_{a-1}^r,$$

where

$$\begin{aligned} \theta_0^n &= 1, \\ \theta_1^n &= \theta_0^a, \\ \theta_2^n &= \theta_0^b \theta_1^c, \\ \theta_3^n &= \theta_0^d \theta_1^e \theta_2^f, \\ &\vdots \end{aligned}$$

and where

$$\begin{aligned} \mathcal{S}^{-1} \theta_0 \mathcal{S} &= 1, \\ \mathcal{S}^{-1} \theta_1 \mathcal{S} &= \theta_0^\beta \theta_1, \\ \mathcal{S}^{-1} \theta_2 \mathcal{S} &= \theta_0^\gamma \theta_1^\delta \theta_2, \\ \mathcal{S}^{-1} \theta_3 \mathcal{S} &= \theta_0^\epsilon \theta_1^\zeta \theta_2^\eta \theta_3, \\ &\vdots \end{aligned}$$

But at present I attend only to the theorems 1 and 2.

For instance, consider the group  $G$  of the order  $n = 6$ ,  $1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2$  ( $\alpha^2 = 1, \beta^3 = 1, \alpha\beta^3 = \beta\alpha, \alpha\beta = \beta^2\alpha$ ). Here  $n = 2$  or  $3$ : if  $n = 2$ , we have  $N = n^\nu (nk + 1) = 2.1(2 + 1)$ ; if  $n = 3$ , we have  $N = n^\nu (nk + 1) = 3.2.1$ .

First,  $n = 2$ ; we should have a group  $g$  of the order 2; one such group is  $(1, \alpha)$ , and the only group the substitutions whereof are permutable with  $(1, \alpha)$  is the group  $(1, \alpha)$  itself: for, taking any other operation of the group, for instance  $\beta$ , it is not true that  $\beta(\gamma, \alpha) = (1, \alpha)\beta$ , in fact the left-hand is  $(\beta, \beta\alpha)$  and the right-hand is  $(\beta, \alpha\beta)$  or  $(\beta, \beta^2\alpha)$ : hence  $n^\nu \nu = 2\nu = 2$ , or  $\nu = 1$ .

Hence, also by theorem 2, there should be 3 groups of the order 2 such as  $(1, \alpha)$ , viz. these are  $(1, \alpha)$ ,  $(1, \alpha\beta)$ ,  $(1, \alpha\beta^2)$ ; derived from  $(1, \alpha)$  as follows:

$$1(1, \alpha)1^{-1} = (1, \alpha),$$

$$\alpha(1, \alpha)\alpha^{-1} = (1, \alpha),$$

$$\beta(1, \alpha)\beta^{-1} = (1, \alpha\beta),$$

$$\beta^2(1, \alpha)\beta^{-2} = (1, \alpha\beta^2),$$

$$\alpha\beta(1, \alpha)(\alpha\beta)^{-1} = (1, \alpha\beta^2),$$

$$\alpha\beta^2(1, \alpha)(\alpha\beta^2)^{-2} = (1, \alpha\beta),$$

since $\beta^{-1} = \beta^2$	= $\beta^2$	{ and therefore }	$\beta\alpha\beta^2 = \alpha\beta^2 \cdot \beta^2 = \alpha\beta,$
,, $\beta^{-2} = \beta$	= $\beta$	,, ,,	$\beta^2\alpha\beta = \alpha\beta \cdot \beta = \alpha\beta^2,$
,, $(\alpha\beta)^{-1} = \alpha\beta$	= $\alpha\beta$	,, ,,	$\alpha\beta\alpha\alpha\beta = \alpha\beta \cdot \beta = \alpha\beta^2,$
,, $(\alpha\beta^2)^{-1} = \alpha\beta^2$	= $\alpha\beta^2$	,, ,,	$\alpha\beta^2\alpha\alpha\beta^2 = \alpha\beta^2 \cdot \beta^2 = \alpha\beta,$

viz. the derivatives are  $(1, \alpha)$ ,  $(1, \alpha\beta)$ ,  $(1, \alpha\beta^2)$ , each twice.

Secondly,  $n = 3$ , there should be here a group of the order 3, viz. this is  $(1, \beta, \beta^2)$ . The group, the substitutions whereof are permutable with  $(1, \beta, \beta^2)$  is the entire group  $(1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2)$ ; in fact, taking any substitution hereof, for instance  $\alpha$ , we have  $\alpha(1, \beta, \beta^2) = (1, \beta, \beta^2)\alpha$ , viz. the left-hand side is  $(\alpha, \alpha\beta, \alpha\beta^2)$ , and the right-hand side is  $(\alpha, \beta\alpha, \beta^2\alpha) = (\alpha, \alpha\beta^2, \alpha\beta)$ , which is the left-hand side, *the change of order being immaterial*; this is the meaning of the expression used, "the operations whereof are permutable with the group  $g$ ." Hence, we have  $n^\nu \nu = 3\nu = 6$ , or  $\nu = 2$ ; and thence, also  $nk + 1 = 3k + 1 = 1$ , viz.  $k = 0$ . There is thus only a single group of the order 3, viz. the group  $(1, \beta, \beta^2)$ .

As another instance I take the group of the order 12 formed by the positive substitutions of four letters, viz. these are

$$\begin{aligned}
 &1, \quad ab.cd, \quad abc, \\
 &\quad \quad ac.bd, \quad acb, \\
 &\quad \quad ad.bc, \quad abd, \\
 &\quad \quad \quad \quad adb, \\
 &\quad \quad \quad \quad acd, \\
 &\quad \quad \quad \quad adc, \\
 &\quad \quad \quad \quad bcd, \\
 &\quad \quad \quad \quad bdc.
 \end{aligned}$$

Here, taking  $n=2$ , we have  $N=n^\nu(nk+1)=2^2.3.1$ ; there is a group  $g$  of the order 4, viz. this is

$$(1, ab.cd, ac.bd, ad.bc),$$

and the greatest group the substitutions whereof are permutable with this group  $g$ , is the entire group of the order 12; thus, considering any substitution thereof, for instance  $abc$ , we have

$$abc \left( \begin{array}{c} 1 \\ ab.cd \\ ac.bd \\ ad.bc \end{array} \right) = \left( \begin{array}{c} 1 \\ ab.cd \\ ac.bd \\ ad.bc \end{array} \right) abc,$$

$$\text{viz. left-hand is } \left( \begin{array}{c} abc \\ acd \\ bdc \\ adb \end{array} \right), \text{ right-hand is } \left( \begin{array}{c} abc \\ bdc \\ adb \\ acd \end{array} \right);$$

hence  $n^\nu \nu = 4\nu = 12$  or  $\nu = 3$ ; whence also  $nk+1, 2k+1, =1$ : and thus the foregoing group  $g$  is the only group of the order 4.

Similarly taking  $\nu = 3$ , we have  $N=n^\nu(nk+1), = 3.1.4$ ; there is a group  $g$  of the order 3, say  $(1, abc, acb)$ , the greatest group the substitutions whereof are permutable with  $g$  is the group  $g$  itself, viz. we have  $n^\nu \nu = 3\nu = 3$ , or  $\nu = 1$ ; and then  $nk+1, = 3k+1, = 4$ : there are thus 4 groups of the order 3, viz. these are

$$(1, abc, acb), (1, abd, adb), (1, acd, adc), (1, bcd, bdc).$$

Reverting to the before-mentioned group of the order 6, this not only contains each of the groups  $(1, \alpha)$ ,  $(1, \alpha\beta)$ ,  $(1, \alpha\beta^2)$  of order 2, and the group  $(1, \beta, \beta^2)$  of order 3, but it is the permutable product of a group of order 2 into a group of order 3, say it is

$$G = (1, \alpha) (1, \beta, \beta^2), = (1, \beta, \beta^2) (1, \alpha).$$

A group which is thus a permutable product of two factors is said to be a true product; and when it cannot be thus expressed as a permutable product of two factors it is prime or simple. A group, the order of which is equal to a prime number  $p$  (the cyclical group of the order  $p$ ) is simple, but the order may be a composite number and yet the group be simple—it was remarked by Galois (*Liouville*, t. XI. (1865), p. 409), that the order of the lowest simple group of composite order is 60,  $= 2^3 \cdot 3 \cdot 5$ , and it has been recently shown, Holder "Die einfache Gruppen in ersten und Zweiten Hundert der Ordnungszahlen," *Math. Ann.* t. XL. (1892), pp. 55–88, that the only other composite order of a simple group in the first 200 numbers is 168. Moreover, in the paper Cole "Simple groups from order 201 to order 500," *Amer. Math. Jour.* t. XIV. (1892), pp. 378–388, it is shown that within these limits the only numbers which can give a simple group or groups are 360 and 432. I take the opportunity of referring to two other important papers, Young "On the determination of Groups whose order is a power of a prime," *Amer. Math. Jour.* t. XV. (1893), pp. 124–178, and Cole and Glover "On Groups whose orders are products of three prime factors," pp. 191–220.

---

## COUNTER PEDALS.

By *K. Tsuruta*, Tokio, Japan.

1. WHEN a line is drawn from any point taken as origin parallel to the tangent at any point of a given curve, the locus of point of intersection of the line with the normal to the curve at that point is called the *counter pedal* of the curve with respect to the origin.\*

---

\* Craig, *Amer. Jour. of Math.* vol. IV. p. 358.