243.

ON THE THEORY OF GROUPS AS DEPENDING ON THE SYMBOLIC EQUATION $\theta^n = 1$. THIRD PART.

[From the *Philosophical Magazine*, vol. XVIII. (1859), pp. 34—37 : Sequel to **125** and **126.**]

THE following is, I believe, a complete enumeration of the groups of 8 :

I. $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7 \quad (\alpha^8 = 1)$.

II. $1, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3 \quad (\alpha^4 = 1,\ \beta^2 = 1,\ \alpha\beta = \beta\alpha)$.

III. $1, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3 \quad (\alpha^4 = 1,\ \beta^2 = 1,\ \alpha\beta = \beta\alpha^3)$.

IV. $1, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3 \quad (\alpha^4 = 1,\ \beta^2 = \alpha^2,\ \alpha\beta = \beta\alpha^3)$.

V. $1, \alpha, \beta, \beta\alpha, \gamma, \gamma\alpha, \gamma\beta, \gamma\beta\alpha \quad (\alpha^2 = 1,\ \beta^2 = 1,\ \gamma^2 = 1,\ \alpha\beta = \beta\alpha,\ \alpha\gamma = \gamma\alpha,\ \beta\gamma = \gamma\beta)$.

That the groups are really distinct is perhaps most readily seen by writing down the indices of the different terms of each group; these are

I. 1, 8, 4, 8, 2, 8, 4, 8.

II. 1, 4, 2, 4, 2, 4, 2, 4.

III. 1, 4, 2, 4, 2, 2, 2, 2.

IV. 1, 4, 2, 4, 4, 4, 4, 4.

V. 1, 2, 2, 2, 2, 2, 2, 2.

It will be presently seen why there is no group where the symbols α, β are such that $\alpha^4 = 1$, $\beta^2 = 1$, $\alpha\beta = \beta\alpha^2$. A group which presents itself for consideration is

$$1, \alpha, \alpha^2, \alpha^4, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3 \quad (\alpha^4 = 1,\ \beta^2 = \alpha^2,\ \alpha\beta = \beta\alpha);$$

but the indices of the different terms of this group are

$$1,\ 4,\ 2,\ 4,\ 2,\ 4,\ 2,\ 4,$$

and if we write $\beta\alpha = \gamma$, then we find $\gamma^2 = \beta\alpha\beta\alpha = \beta\beta\alpha\alpha = \alpha^4 = 1$, $\alpha\gamma = \alpha\beta\alpha = \beta\alpha\alpha = \gamma\alpha$; and the group is

$$1,\ \alpha,\ \alpha^2,\ \alpha^3,\ \gamma,\ \gamma\alpha,\ \gamma\alpha^2,\ \gamma\alpha^3\ (\alpha^4 = 1,\ \gamma^2 = 1,\ \alpha\gamma = \gamma\alpha),$$

which is the group II.

The group IV is a remarkable one; it appears to arise from the circumstance that the factors 2 and 4 of the number 8 are not prime to each other; this can only happen when the number which denotes the order of the group contains a square factor. But the nature of the group in question will be better understood by presenting it under a different form. In fact, if we write $\beta\alpha^3 = \gamma$, $\alpha^2 = \beta^2 = \vartheta$, then we find $\alpha^3 = \vartheta\alpha$, $\beta\alpha^2 = \vartheta\beta$, $\beta\alpha = \vartheta\gamma$, and the group will be

$$1,\ \alpha,\ \beta,\ \gamma,\ \vartheta,\ \vartheta\alpha,\ \vartheta\beta,\ \vartheta\gamma,$$

where the laws of combination are

$$\vartheta^2 = 1, \quad \alpha^2 = \beta^2 = \gamma^2 = \vartheta,$$

$$\beta\gamma = \alpha, \qquad \gamma\alpha = \beta, \qquad \alpha\beta = \gamma,$$

$$\gamma\beta = \alpha\vartheta = \vartheta\alpha, \quad \alpha\gamma = \beta\vartheta = \vartheta\beta, \quad \beta\alpha = \gamma\vartheta = \vartheta\gamma.$$

Observe that ϑ is a symbol of operation such that $\vartheta^2 = 1$, and that ϑ is convertible with each of the other symbols α, β, γ. It will be not so much a restrictive assumption in regard to ϑ, as a definition of -1 considered as a symbol of operation if we write $\vartheta = -1$; the group thus becomes

$$1,\ \alpha,\ \beta,\ \gamma,\ -1,\ -\alpha,\ -\beta,\ -\gamma,$$

where

$$\alpha^2 = \beta^2 = \gamma^2 = -1,$$

$$\alpha = \beta\gamma = -\gamma\beta, \quad \beta = \gamma\alpha = \alpha\gamma, \quad \gamma = \alpha\beta = \beta\alpha.$$

Hence α, β, γ combine according to the laws of the quaternion symbols i, j, k; and it is only the point of view from which the question is here considered which obliges us to consider the symbols as belonging to a group of 8, instead of (as in the theory of quaternions) a group of 4.

Suppose in general that the symbols α, β are such that

$$\alpha^m = 1, \quad \beta^n = 1, \quad \alpha\beta = \beta\alpha^s,$$

then we find

$$\alpha^u\beta^v = \beta^v\alpha^{us^v};$$

and therefore if $v = n$, $\alpha^u = \alpha^{us^n}$ or $\alpha^{u(s^n-1)} = 1$, whence $u(s^n - 1) \equiv 0 \pmod{m}$; or since u is arbitrary, $s^n - 1 \equiv 0 \pmod{m}$, an equation which, if m, n are given, determines the admissible values of s; thus, for example, if $n = 2$, and m is a prime number, then $s = 1$ or $s = m - 1$. The equation $\alpha^u \beta^v = \beta^v \alpha^{us^v}$ shows that any combination whatever of the symbols α, β can be expressed in the form $\beta^q \alpha^p$ (or, if we please, in the form $\alpha^p \beta^q$). It is proper to show that the assumed law is consistent with the associative law, viz. that the expression

$$\beta^b \alpha^a \,.\, \beta^d \alpha^c \,.\, \beta^f \alpha^e$$

can be transformed in one way only into the form $\beta^q \alpha^p$. We in fact have

$$\beta^b \alpha^a \,.\, \beta^d \alpha^c = \beta^b \,.\, \alpha^a \beta^d \,.\, \alpha^c = \beta^b \,.\, \beta^d \alpha^{as^d} \,.\, \alpha^c = \beta^{b+d} \alpha^{as^d + c};$$

and multiplying this by the remaining factor $\beta^f \alpha^e$, we have

$$\beta^{b+d} \,.\, \alpha^{as^d + c} \beta^f \,.\, \alpha^e,$$

which is equal to

$$\beta^{b+d} \,.\, \beta^f \alpha^{as^{d+f} + cs^f} \,.\, \alpha^e,$$

or finally to

$$\beta^{b+d+f} \alpha^{as^{d+f} + cs^f + e};$$

and the result would have been precisely the same if, instead of thus combining together the first and second factors and the product with the third factor, we had combined the first factor with the product of the second and third factors, so that the associative law is satisfied.

It is now easy to see that if, as before,

$$\alpha^m = 1, \quad \beta^n = 1, \quad \alpha\beta = \beta\alpha^s,$$

conditions which it has been shown imply $s^n \equiv 1 \pmod{m}$, then the symbols $\beta^q \alpha^p$ (or, if we please, $\alpha^p \beta^q$), where p has the values $0, 1, 2, \ldots, m-1$, and q the values $0, 1, 2, \ldots, n-1$, form a group of mn terms. In particular, as already noticed, if $n = 2$ and m is prime, then $s = 1$ or $s = m - 1$; the two groups so obtained are essentially distinct from each other. If $n = 2$, but m is not prime, then s has in general more than two values: thus for $m = 12$, $s^2 \equiv 1 \pmod{12}$, which is satisfied by $s = 1$, 5, 7 and 11; the group corresponding to $s = 1$ is distinct from that for any other value of s, but I have not ascertained whether the values other than unity do, or do not, give groups distinct from each other.

For the sake of an observation to which it gives rise, I write down an example of a group corresponding to $n = 2$, $s = m - 1$, say $m = 5$, and therefore $s = 4$, so that we have

$$\alpha^5 = 1, \quad \beta^2 = 1, \quad \alpha\beta = \beta\alpha^4,$$

and the group is

$$1, \ \alpha, \ \alpha^2, \ \alpha^3, \ \alpha^4, \ \beta, \ \beta\alpha, \ \beta\alpha^2, \ \beta\alpha^3, \ \beta\alpha^4,$$

the indices of the several terms being

$$1,\ 5,\ 5,\ 5,\ 5,\ 2,\ 2,\ 2,\ 2,\ 2.$$

The group is here expressed by means of the symbols α, β, having the indices 5 and 2 respectively, but it may be expressed by means of two symbols having each of them the index 2. Thus putting $\beta\alpha = \gamma$, we find $\beta^2 = 1$, $\gamma^2 = 1$, $(\beta\gamma)^5 = 1$, which is equivalent to $(\gamma\beta)^5 = 1$, and the group may be represented in the form

$$1,\ \beta,\ \gamma,\ \beta\gamma,\ \gamma\beta,\ \beta\gamma\beta,\ \gamma\beta\gamma,\ \beta\gamma\beta\gamma,\ \gamma\beta\gamma\beta,\ \beta\gamma\beta\gamma\beta = \gamma\beta\gamma\beta\gamma,$$

the equality of the last two symbols being an obvious consequence of the equation $(\beta\gamma)^5 = 1$. It is clear that for any even number $2p$ whatever, there is always a group which can be expressed in this form.

2, *Stone Buildings, W.C., June* 9, 1859.