125.

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

[From the *Philosophical Magazine*, vol. VII. (1854), pp. 40—47.]

LET θ be a symbol of operation, which may, if we please, have for its operand, not a single quantity x, but a system $(x, y, \ldots)$, so that

$$\theta(x, y, \ldots) = (x', y', \ldots),$$

where $x', y', \ldots$ are any functions whatever of $x, y, \ldots$, it is not even necessary that $x', y', \ldots$ should be the same in number with $x, y, \ldots$. In particular x', y', &c. may represent a permutation of x, y, &c., θ is in this case what is termed a substitution; and if, instead of a set $x, y, \ldots$, the operand is a single quantity x, so that $\theta x = x' = fx$, θ is an ordinary functional symbol. It is not necessary (even if this could be done) to attach any meaning to a symbol such as $\theta \pm \phi$, or to the symbol 0, nor consequently to an equation such as $\theta = 0$, or $\theta \pm \phi = 0$; but the symbol 1 will naturally denote an operation which (either generally or in regard to the particular operand) leaves the operand unaltered, and the equation $\theta = \phi$ will denote that the operation θ is (either generally or in regard to the particular operand) equivalent to ϕ, and of course $\theta = 1$ will in like manner denote the equivalence of the operation θ to the operation 1. A symbol $\theta\phi$ denotes the compound operation, the performance of which is equivalent to the performance, first of the operation ϕ, and then of the operation θ; $\theta\phi$ is of course in general different from $\phi\theta$. But the symbols $\theta, \phi, \ldots$ are in general such that $\theta . \phi\chi = \theta\phi . \chi$, &c., so that $\theta\phi\chi$, $\theta\phi\chi\omega$, &c. have a definite signification independent of the particular mode of compounding the symbols; this will be the case even if the functional operations involved in the symbols θ, ϕ, &c. contain parameters such as the quaternion imaginaries i, j, k; but not if these functional operations contain parameters such as the imaginaries which enter into the theory of octaves, &c., and for which, e.g. $\alpha . \beta\gamma$ is something different from $\alpha\beta . \gamma$, a supposition which is altogether excluded from the present paper. The order of the factors of a product $\theta\phi\chi\ldots$ must of course be attended to, since even in the case of a product of two factors the order is material; it is very convenient to speak of the symbols θ, $\phi\ldots$ as the first or furthest, second, third, &c., and last or nearest factor. What precedes may be almost entirely summed up in the remark, that the distributive law has no application to the symbols $\theta\phi\ldots$; and that these symbols are not in general convertible, but are associative. It is easy to see that $\theta^0 = 1$, and that the index law $\theta^m . \theta^n = \theta^{m+n}$, holds for all positive or negative integer values, not excluding 0. It should be noticed also, that if $\theta = \phi$, then, whatever the symbols α, β may be, $\alpha\theta\beta = \alpha\phi\beta$, and conversely.

A set of symbols,

$$1,\ \alpha,\ \beta,\ldots$$

all of them different, and such that the product of any two of them (no matter in what order), or the product of any one of them into itself, belongs to the set, is said to be a *group*[1]. It follows that if the entire group is multiplied by any one of the symbols, either as further or nearer factor, the effect is simply to reproduce the group; or what is the same thing, that if the symbols of the group are multiplied together so as to form a table, thus:

		Further factors			
		1	α	β	..
Nearer factors	1	1	α	β	..
	α	α	α^2	$\beta\alpha$	
	β	β	$\alpha\beta$	β^2	
		:			

that as well each line as each column of the square will contain all the symbols $1, \alpha, \beta, \ldots$. It also follows that the product of any number of the symbols, with or without repetitions, and in any order whatever, is a symbol of the group. Suppose that the group

$$1,\ \alpha,\ \beta,\ \ldots$$

contains n symbols, it may be shown that each of these symbols satisfies the equation

$$\theta^n = 1\,;$$

so that a group may be considered as representing a system of roots of this symbolic binomial equation. It is, moreover, easy to show that if any symbol α of the group

[1] The idea of a group as applied to permutations or substitutions is due to Galois, and the introduction of it may be considered as marking an epoch in the progress of the theory of algebraical equations.

satisfies the equation $\theta^r = 1$, where r is less that n, then that r must be a submultiple of n; it follows that when n is a prime number, the group is of necessity of the form

$$1,\ \alpha,\ \alpha^2, \ldots\ \alpha^{n-1},\ (\alpha^n = 1);$$

and the same may be (but is not necessarily) the case, when n is a composite number. But whether n be prime or composite, the group, *assumed to be of the form in question*, is in every respect analogous to the system of the roots of the ordinary binomial equation $x^n - 1 = 0$; thus, when n is prime, all the roots (except the root 1) are prime roots; but when n is composite, there are only as many prime roots as there are numbers less than n and prime to it, &c.

The distinction between the theory of the symbolic equation $\theta^n = 1$, and that of the ordinary equation $x^n - 1 = 0$, presents itself in the very simplest case, $n = 4$. For, consider the group

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

which are a system of roots of the symbolic equation

$$\theta^4 = 1.$$

There is, it is clear, at least one root β, such that $\beta^2 = 1$; we may therefore represent the group thus,

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

then multiplying each term by α as further factor, we have for the group $1,\ \alpha^2,\ \alpha\beta,\ \alpha^2\beta$, so that α^2 must be equal either to β or else to 1. In the former case the group is

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

which is analogous to the system of roots of the ordinary equation $x^4 - 1 = 0$. For the sake of comparison with what follows, I remark, that, representing the last-mentioned group by

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

we have the table

	1,	α,	β,	γ
1	1	α	β	γ
α	α	β	γ	1
β	β	γ	1	α
γ	γ	1	α	β

If, on the other hand, $\alpha^2=1$, then it is easy by similar reasoning to show that we must have $\alpha\beta=\beta\alpha$, so that the group in the case is

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

or if we represent the group by

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

we have the table

	1	α	β	γ
1	1	α	β	γ
α	α	1	γ	β
β	β	γ	1	α
γ	γ	β	α	1

,

or, if we please, the symbols are such that

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

[and we have thus a group essentially distinct from that of the system of roots of the ordinary equation $x^4-1=0$].

Systems of this form are of frequent occurrence in analysis, and it is only on account of their extreme simplicity that they have not been expressly remarked. For instance, in the theory of elliptic functions, if n be the parameter, and

$$\alpha(n)=\frac{c^2}{n}\quad \beta(n)=-\frac{c^2+n}{1+n}\quad \gamma(n)=-\frac{c^2(1+n)}{c^2+n},$$

then $\alpha,\ \beta,\ \gamma$ form a group of the species in question. So in the theory of quadratic forms, if

$$\alpha(a,\ b,\ c)=(c,\quad b,\ a)$$
$$\beta(a,\ b,\ c)=(a,\ -b,\ c)$$
$$\gamma(a,\ b,\ c)=(c,\ -b,\ a);$$

although, indeed, in this case (treating forms which are properly equivalent as identical) we have $\alpha=\beta$, and therefore $\gamma=1$, in which point of view the group is simply a group of two symbols $1,\ \alpha,\ (\alpha^2=1)$.

Again, in the theory of matrices, if I denote the operation of inversion, and tr that of transposition, (I do not stop to explain the terms as the example may be passed over), we may write

$$\alpha = I, \quad \beta = \text{tr}, \quad \gamma = I \,.\, \text{tr} = \text{tr} \,.\, I.$$

I proceed to the case of a group of six symbols,

$$1, \alpha, \beta, \gamma, \delta, \epsilon,$$

which may be considered as representing a system of roots of the symbolic equation

$$\theta^6 = 1.$$

It is in the first place to be shown that there is at least one root which is a prime root of $\theta^3 = 1$, or (to use a simpler expression) a root having the index 3. It is clear that if there were a prime root, or root having the index 6, the square of this root would have the index 3, it is therefore only necessary to show that it is impossible that *all* the roots should have the index 2. This may be done by means of a theorem which I shall for the present assume, viz. that if among the roots of the symbolic equation $\theta^n = 1$, there are contained a system of roots of the symbolic equation $\theta^p = 1$ (or, in other words, if among the symbols forming a group of the order there are contained symbols forming a group of the order p), then p is a submultiple of n. In the particular case in question, a group of the order 4 cannot form part of the group of the order 6. Suppose, then, that γ, δ are two roots of $\theta^6 = 1$, having each of them the index 2; then if $\gamma\delta$ had also the index 2, we should have $\gamma\delta = \delta\gamma$; and $1, \gamma, \delta, \delta\gamma$, which is part of the group of the order 6, would be a group of the order 4. It is easy to see that $\gamma\delta$ must have the index 3, and that the group is, in fact, $1, \gamma\delta, \delta\gamma, \gamma, \delta, \gamma\delta\gamma$, which is, in fact, one of the groups to be presently obtained; I prefer commencing with the assumption of a root having the index 3. Suppose that α is such a root, the group must clearly be of the form

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

and multiplying the entire group by γ as nearer factor, it becomes $\gamma, \alpha\gamma, \alpha^2\gamma, \gamma^2, \alpha\gamma^2, \alpha^2\gamma^2$; we must therefore have $\gamma^2 = 1$, α, or α^2. But the supposition $\gamma^2 = \alpha^2$ gives $\gamma^4 = \alpha^4 = \alpha$, and the group is in this case $1, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5 \, (\gamma^6 = 1)$; and the supposition $\gamma^2 = \alpha$ gives also this same group. It only remains, therefore, to assume $\gamma^2 = 1$; then we must have either $\gamma\alpha = \alpha\gamma$ or else $\gamma\alpha = \alpha^2\gamma$. The former assumption leads to the group

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

which is, in fact, analogous to the system of roots of the ordinary equation $x^6 - 1 = 0$; and by putting $\alpha\gamma = \lambda$, might be exhibited in the form $1, \lambda, \lambda^2, \lambda^3, \lambda^4, \lambda^5, \ (\lambda^6 = 1)$, under which this system has previously been considered. The latter assumption leads to the group

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

and we have thus two, and only two, essentially distinct forms of a group of six.

If we represent the first of these two forms, viz. the group

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

by the general symbols

$$1, \alpha, \beta, \gamma, \delta, \epsilon,$$

we have the table

	1	α	β	γ	δ	ϵ
1	1	α	β	γ	δ	ϵ ;
α	α	β	γ	δ	ϵ	1
β	β	γ	δ	ϵ	1	α
γ	γ	δ	ϵ	1	α	β
δ	δ	ϵ	1	α	β	γ
ϵ	ϵ	1	α	β	γ	δ

while if we represent the second of these two forms, viz. the group

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

by the same general symbols

$$1, \alpha, \beta, \gamma, \delta, \epsilon,$$

we have the table

	1	α	β	γ	δ	ϵ
1	1	α	β	γ	δ	ϵ ;
α	α	β	1	ϵ	γ	δ
β	β	1	α	δ	ϵ	γ
γ	γ	δ	ϵ	1	α	β
δ	δ	ϵ	γ	β	1	α
ϵ	ϵ	γ	δ	α	β	1

or, what is the same thing, the system of equations is

$$\begin{aligned}
1 &= \beta\alpha = \alpha\beta = \gamma^2 = \delta^2 = \epsilon^2,\\
\alpha &= \beta^2 = \delta\gamma = \epsilon\delta = \gamma\epsilon,\\
\beta &= \alpha^2 = \epsilon\gamma = \gamma\delta = \delta\epsilon,\\
\gamma &= \delta\alpha = \epsilon\beta = \beta\delta = \alpha\epsilon,\\
\delta &= \epsilon\alpha = \gamma\beta = \alpha\gamma = \beta\epsilon,\\
\epsilon &= \gamma\alpha = \delta\beta = \beta\gamma = \alpha\delta.
\end{aligned}$$

An instance of a group of this kind is given by the permutation of three letters; the group

$$1,\ \alpha,\ \beta,\ \gamma,\ \delta,\ \epsilon$$

may represent a group of substitutions as follows:—

$$\frac{abc,\ cab,\ bca,\ acb,\ cba,\ bac}{abc\ \ abc\ \ abc\ \ abc\ \ abc\ \ abc.}$$

Another singular instance is given by the optical theorem proved in my paper "On a property of the Caustic by refraction of a Circle, [124]."

It is, I think, worth noticing, that if, instead of considering α, β, &c. as symbols of operation, we consider them as quantities (or, to use a more abstract term, 'cogitables') such as the quaternion imaginaries; the equations expressing the existence of the group are, in fact, the equations defining the meaning of the product of two complex quantities of the form

$$w + a\alpha + b\beta + \dots;$$

thus, in the system just considered,

$$(w + a\alpha + b\beta + c\gamma + d\delta + e\epsilon)(w' + a'\alpha + b'\beta + c'\gamma + d'\delta + e'\epsilon) = W + A\alpha + B\beta + C\gamma + D\delta + E\epsilon,$$

where

$$\begin{aligned}
W &= ww' + ab' + a'b + cc' + dd' + ee',\\
A &= wa' + w'a + bb' + dc' + ed' + ce',\\
B &= wb' + w'b + aa' + ec' + cd' + de',\\
C &= wc' + w'c + da' + eb' + bd' + ae',\\
D &= wd' + w'd + ea' + cb' + ac' + be',\\
E &= we' + w'e + ca' + db' + bc' + ad'.
\end{aligned}$$

It does not appear that there is in this system anything analogous to the modulus $w^2 + x^2 + y^2 + z^2$, so important in the theory of quaternions.

I hope shortly to resume the subject of the present paper, which is closely connected, not only with the theory of algebraical equations, but also with that of the composition of quadratic forms, and the 'irregularity' in certain cases of the determinants of these forms. But I conclude for the present with the following two examples of groups of higher orders. The first of these is a group of eighteen, viz.

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

where

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

and the other a group of twenty-seven, viz.

$$\begin{aligned}&1,\ \alpha,\ \alpha^2,\ \gamma,\ \gamma^2,\ \gamma\alpha,\ \alpha\gamma,\ \gamma\alpha^2,\ \alpha^2\gamma,\ \gamma^2\alpha,\ \alpha\gamma^2,\ \gamma^2\alpha^2,\ \alpha^2\gamma^2,\\ &\alpha\gamma\alpha,\ \alpha\gamma^2\alpha,\ \alpha^2\gamma\alpha,\ \alpha^2\gamma^2\alpha,\ \alpha\gamma\alpha^2,\ \alpha\gamma^2\alpha^2,\ \alpha^2\gamma\alpha^2,\ \alpha^2\gamma^2\alpha^2,\ \gamma\alpha\gamma^2,\ \gamma\alpha^2\gamma^2,\ \gamma^2\alpha\gamma,\ \gamma^2\alpha^2\gamma,\ \gamma^2\alpha\gamma\alpha^2,\ \gamma\alpha\gamma^2\alpha^2,\end{aligned}$$

where

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

It is hardly necessary to remark, that each of these groups is in reality perfectly symmetric, the omitted terms being, in virtue of the equations defining the nature of the symbols, identical with some of the terms of the group: thus, in the group of 18, the equations $\alpha^2=1$, $\beta^2=1$, $\gamma^2=1$, $(\alpha\beta\gamma)^2=1$ give $\alpha\beta\gamma=\gamma\beta\alpha$, and similarly for all the other omitted terms. It is easy to see that in the group of 18 the index of each term is 2 or else 3, while in the group of 27 the index of each term is 3.

2 *Stone Buildings, Nov.* 2, 1853.