NOTE ON THE THEORY OF GROUPS.

By *W. Burnside.*

THE following note gives a very simple illustration of the graphical method of discussing groups of discrete operations, whether of finite or infinite order, which Herr Dyck explains at length in a memoir in vol. XX. of the *Math. Annalen*, and which is used directly or indirectly in many of the recent researches in connection with automorphic functions.

Let P and Q be two non-commutative symbols satisfying the relations

$$P^3 = 1, \quad Q^3 = 1, \quad (PQ)^3 = 1.$$

The series of powers and products that can be formed from P and Q, such as

$$1, P, Q, P^2, Q^2, PQ, P^2Q, PQP, QPQ^2 \ldots$$

will not all be different in consequence of the relation $(PQ)^3 = 1$; for instance, it immediately follows from this relation that

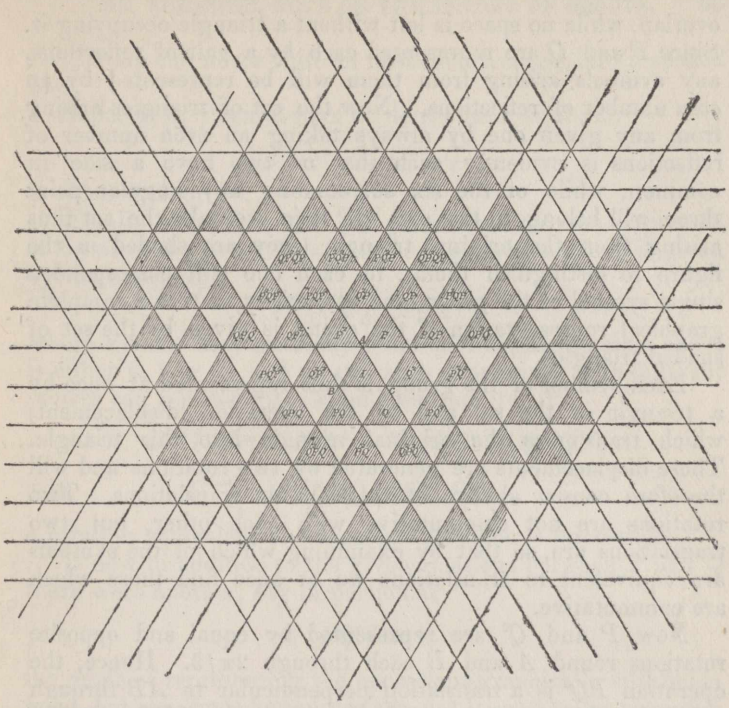
$$PQPQ = Q^2P^2.$$

It is, however, easy to see that an infinite number of them will be distinct, or in other words that the group of symbols arising from P and Q is of infinite order. When such a complete set of distinct symbols has been chosen, the product of every two must again be one of the set, or it would not otherwise be complete.

To arrive at expressions giving such a complete set in terms of P and Q, which are spoken of as the generating symbols, is one of the questions it is proposed to discuss; and also to determine what further relation or relations between P and Q must be given, that the group may be of finite order, *i.e.* that the number of distinct symbols may be finite.

Let ABC be an equilateral triangle, and denote by α, β, γ the operations of reflection in BC, CA, AB respectively. The operation $\beta\gamma$ consisting of successive reflections in AC and AB is easily seen to be equivalent to a rotation through $2\pi/3$, about the angle A of the triangle, the direction in the accompanying figure being that of the hand of a watch. The operation $\beta\gamma$ repeated three times leads to no change at all; this may be represented by the equation

$$(\beta\gamma)^3 = 1.$$



Similarly $\gamma\alpha$ and $\alpha\beta$ represent rotations through $2\pi/3$ round B and C, and we have

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

But $$(\alpha\beta)^3 = 1,$$

or $(\beta\alpha)^3 = 1$, which is equivalent to it, may be written

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

since γ^2 representing two successive reflections in AB evidently produces no change.

It follows that the relations which $\beta\gamma$ and $\gamma\alpha$ satisfy are precisely the same as those holding between P and Q; and that P and Q may be interpreted graphically as pairs of reflections in the sides of an equilateral triangle.

If we now form from the original triangle a complete figure by continually drawing its reflections and the reflections of its reflections in the sides, the whole plane of the diagram will be divided into equilateral triangles no two of which

overlap, while no space is left without a triangle occupying it. Since P and Q are represented each by a pair of reflections, any symbols arising from them will be represented by an *even* number of reflections. Now the set of triangles arising from any given one by always taking an even number of reflections is evidently such that no two have a side in common, while of the six surrounding any angular point three will belong to the set. If then we take the set thus arising from the original triangle (they are shaded in the figure to distinguish them), to each one will correspond a single symbol of the group, and conversely, so that a complete graphical representation of the group is given by the set of shaded triangles.

Each symbol of the group is thus represented at once by a triangle of the set and by the operation (displacement) which transforms the original triangle into this triangle. These displacements are generated by two rotations and will therefore consist always of rotations or translations. Two rotations are not commutative with each other, but two translations are, so that by examining which of the symbols are equivalent to translations we at once find those which are commutative.

Now P and Q^2 are represented by equal and opposite rotations round A and B each through $2\pi/3$. Hence, the operation PQ^2 is a translation perpendicular to AB through twice the altitude of the triangle. Similarly QPQ and Q^2P represent equal translations perpendicular to BC and CA. These are of course not independent operations, that is, one can be expressed in terms of the other two, for

$$PQ^2 . QPQ . Q^2P = PQ^3PQ^3P = 1.$$

Any translation can therefore be expressed by

$$(PQ^2)^\alpha (QPQ)^\beta (Q^2P)^\gamma,$$

where the three brackets are commutative, and one may be got rid of by the preceding relation.

Suppose now that S is any symbol of the set. The triangle corresponding to S can by such a translation as that just written be brought to coincide with one of the three 1, P, P^2. For the hexagon formed by these and the intermediate unshaded triangles is bounded by three pairs of parallel lines whose directions are perpendicular to the three translations and whose distances apart are equal to the least translations possible; while an inspection of the figure shews that such a

translation can never shift an unshaded triangle into a shaded one.

Hence α, β, γ can always be determined, so that

$$S(PQ^2)^\alpha (QPQ)^\beta (Q^2P)^\gamma$$

is either 1, P or P^2.

Finally then, since the last translation may be expressed in terms of the two others, every symbol of the group is given by the expression

$$P^n (PQ^2)^\alpha (QPQ)^\beta,$$

where α and β may have any positive or negative values and n is either 0, 1 or 2: and no two such expressions with different indices can represent the same operation, for if

$$P^n (PQ^2)^\alpha (QPQ)^\beta = P^{n'} (PQ^2)^{\alpha'} (QPQ)^{\beta'},$$

then $$P^{n-n'} = (PQ^2)^{\alpha'-\alpha} (QPQ)^{\beta'-\beta},$$

a rotation equivalent to a translation, which is impossible.

If now in addition to the given relations between P and Q there were another, say in particular

$$(PQ^2)^m = 1,$$

the mode of representing the operations graphically still holds good, but the shaded triangles are not longer to be regarded as all distinct. Thus, if S be any triangle

$$S = S(PQ^2)^m,$$

or two triangles are to be regarded as identical if one can be derived from the other by a translation through $2m$ times the altitude of ABC.

Hence, if a line be drawn parallel to AB and at this distance from it, the actually distinct triangles are contained between these two lines.

Moreover $$Q^2 (PQ^2)^m Q = Q^3 = 1,$$

and $$Q (PQ^2)^m Q^2 = Q^3 = 1,$$

and therefore $$(Q^2P)^m = 1, \quad (QPQ)^m = 1;$$

so that all distinct triangles are also contained between pairs of lines parallel to BC and CA and at the same distance apart as the former pair; and all distinct triangles are therefore contained within a regular hexagon, the distance between whose pairs of opposite sides is $2m$ times the altitude of a triangle.

Such a further relation between P and Q as that assumed therefore reduces the group to one of finite order. Finally it may be shewn that any further single relation between P and Q has this effect; and that, if P and Q are independent symbols, any such relation necessarily reduces to the one considered above.

Thus, any further relation can be written in the form

$$1 = P^n (Q^2P)^\alpha (QPQ)^\beta.$$

Suppose first $n = 1$.

Then $1 = P(Q^2P)^{\alpha-\beta}(Q^2PQPQ)^\beta$,

since the two brackets are commutative,

$$= P(Q^2P)^{\alpha-\beta}(QP^2)^\beta$$
$$= (PQ^2)^{\alpha-\beta}P(QP^2)^\beta$$
$$= P(PQ^2)^{\alpha-\beta}(QP^2)^\beta$$
$$= P(PQ^2)^{\alpha-2\beta} = P(QP^2)^{2\beta-\alpha},$$

therefore $P^2 = (QP^2)^{2\beta-\alpha}$

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

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

so that P and Q are not independent; and it may be easily shewn that $n = 2$ leads to the same result.

If, lastly, $1 = (Q^2P)^\alpha (QPQ)^\beta$,

then, as above,

$$1 = (QPQ)^\alpha (PQ^2)^\beta,$$

and $1 = (PQ^2)^\alpha (Q^2P)^\beta$,

so that three different translations lead from any triangle to one that is not distinct from it. The group is therefore again finite, and hence Q^2P must be of finite order.

Now the equation of conditions may be written

$$(Q^2P)^{-\alpha} = (QPQ)^\beta.$$

If α and β are not multiples of the order of Q^2P the two sides of this equation represent finite translations in two different directions, and these are not equivalent. Hence, the equation gives

$$(Q^2P)^m = 1,$$

where m is the G. C. M. of α and β.

The case in which $m = 3$ is of special interest.

The group is then of order 27, and there is no difficulty in verifying that all its operations are of order 3. The theory of groups whose order is the power of a prime shews that in this case there should be two operations besides identity which are commutative with all the operations of the group, and it is easy to verify that this is true of

$$Q^2P^2QP \text{ and } QP^2Q^2P,$$

of which either is the square of the other.

Moreover, in this case PQ and QP are commutative and the operations of the group are all included in the form

$$P^\alpha (PQ)^\beta (QP)^\gamma,$$

the indices being 0, 1 or 2.

The figure gives the complete graphical representation of this finite group of order 27.

There are two other cases in which a plane may be regularly divided into similar triangles derived by repeated reflections from a single triangle, the angles of the triangles being respectively $\pi/4$, $\pi/4$, $\pi/2$ in the one case, and $\pi/6$, $\pi/3$, $\pi/2$ in the other.

Corresponding to each of these there is an infinite group of operations, arising from two generating operations connected by a single relation: and in each case a single further relation suffices to reduce the group to one of finite order.

Corresponding to the first case we may put

$$P^4 = 1, \quad Q^2 = 1, \quad (PQ)^4 = 1.$$

Every operation of the group is then given once and once only by the expression

$$P^n (P^2Q)^\alpha (PQP)^\beta,$$

where α and β take all positive and negative values, and n is 0, 1, 2 or 3.

Since $$PQP = P^3 . P^2Q . P,$$

the relation $$(P^2Q)^m = 1$$

gives $$(PQP)^m = 1,$$

and the group is then a finite one of order $4m^2$.

For the second case we take

$$P^3 = 1, \quad Q^2 = 1, \quad (PQ)^6 = 1.$$

Every operation is then given once and once only by

$$Q^m P^n (PQP^2Q)^\alpha (P^2QPQ)^\beta,$$

where $m = 0, 1$; $n = 0, 1, 2$; and α, β take all positive or negative values.

Again in this case a relation

$$(PQP^2Q)^m = 1$$

obviously reduces the group to one of order $6m^2$.

The distinct triangles corresponding to the finite groups in these cases can always be chosen so as to fill a square in the one case and a regular hexagon in the other. The figure corresponding to the last case is a particularly interesting one.

TWO THEOREMS ON PRIME NUMBERS.

By *N. M. Ferrers.*

1. If $2p + 1$ be any prime number, the sum of the products of the integers 1, 2, ..., $2p$, taken r together, r being any integer less than $2p$ is divisible by $2p + 1$.

For, x denoting any integer whatever,

$$x(x+1)...(x+2p) \text{ is divisible by } 2p+1,$$

therefore if x be not divisible by $2p + 1$,

$$(x+1)(x+2)...(x+2p) \text{ is so,}$$

or, denoting the sum of the products of the integers 1, 2, ..., $2p$ taken r together by S_r,

$$x^{2p} + S_1x^{2p-1} + ... + S_{2p-1}x + 1.2...2p$$

is divisible by $2p + 1$.

But by Fermat's Theorem,

$$x^{2p} - 1 \text{ is so divisible,}$$

and by Wilson's Theorem,

$$1.2...2p + 1 \text{ is so divisible,}$$

therefore $x^{2p} + 1.2...2p$ is so.

Therefore removing these terms, and dividing by x,

$$S_1x^{2p-2} + S_2x^{2p-3} + ... + S_{2p-1}$$

is divisible by $2p + 1$ for all values of x, from 1 to $2p$ inclusive.