ON GROUPS IN WHICH CERTAIN COMMUTATIVE OPERATIONS ARE CONJUGATE*

BY

H. L. RIETZ

Introduction.

The groups in which every two conjugate operators are commutative have recently been considered by BURNSIDE.† In the first section of the present paper, the converse limitation is imposed on a group of operations. It is assumed that every two commutative operations are conjugate, provided neither is identity,‡ and the groups which are possible under this hypothesis are determined. It results that the group of order 2 § and the symmetric group of order 6 are the only groups which have the property in question.

In sections 2–6, somewhat similar but smaller limitations are imposed on the group. The condition is imposed in sections 2–5 that every two commutative operations of the same order are conjugate, and in section 6 that every two commutative operations (identity excluded) are so related that each of them is conjugate to some power of the other. Some of the chief properties of the groups which are possible under these limitations are derived.

The sections 7–8 deal with problems closely related to the preceding. If it is assumed that a certain simple relation exists between the number λ of complete sets of conjugate operations, and the number n of distinct prime factors in the order of the group, certain commutative operations are conjugate. Much use is made of this fact in showing what groups are possible under the given hypothesis.

The symbol $G \equiv (S_1 = 1), S_2, S_3, \cdots, S_g$ will be used to represent the group of order g under consideration, and $p_1, p_2, \cdots, p_n$ to represent distinct primes in ascending order of magnitude so that $g = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$.

* Presented to the Society (Chicago) December 31, 1903. Received for publication January 18, 1904.

† Proceedings of the London Mathematical Society, vol. 35 (1903), pp. 28–37.

‡ Without making an exception of identity, clearly no groups are possible.

§ The group of order 2 may be regarded as a trivial case.

§ 1. *Groups in which every two commutative operations, apart from the identical operation, are conjugate.*

§ 1. It is assumed, in case

$$S_a S_b = S_b S_a \qquad (a > 1, b > 1), \tag{1}$$

that there is in G an operation S_c such that

$$S_c^{-1} S_a S_c = S_b. \tag{2}$$

Then S_a and S_b must be of the same order, that is, any two commutative operations of G, neither of which is the identical operation, must be of the same order. Since an operation is commutative with all its powers, all the powers of an operation, except identity, must be of the same order. But this is clearly true only of operations of prime order. Hence, all operations in G must be of prime order. Any Sylow subgroup H of order $p_r^{\alpha_r}$ contains at least p_r operations invariant in H. Hence all the operations in H, except identity, belong to the same conjugate set under G. Since the Sylow subgroups are themselves conjugate, all the operations of order p_r are conjugate, and each is invariant in a subgroup of order $p_r^{\alpha_r}$. Hence the operations of G, aside from identity, are distributed into just as many complete sets of conjugates as there are distinct prime factors in g, and $g/p_r^{\alpha_r}$ is the number of operations of G of order p_r.

Hence

$$\sum_{r=1}^{r=n} \frac{g}{p_r^{\alpha_r}} = g - 1. \tag{3}$$

Remembering that p_n is the largest prime number contained in g, let S_n be an operation of order p_n. Since there must be in G operations which transform S_n into its $p_n - 1$ powers of order p_n, let

$$S_t^{-1} S_n S_t = S_n^{\alpha},$$

where α is a primitive root of p_n. Then

$$S_t^{-q} S_n S_t^q = S_n^{\alpha^q}.$$

If q is the order of S_t,

$$\alpha^q \equiv 1 \quad \text{mod } p_n,$$

and

$$q = p_n - 1.$$

But p_n and $p_n - 1$ cannot both be prime numbers unless $p_n = 3$ or 2. Hence

$$g = 2^{\alpha_1} 3^{\alpha_2} \qquad (\alpha_1 \geqq 1, \alpha_2 \geqq 0). \tag{4}$$

If $\alpha_2 = 0$, we have from (3) and (4)

$$g=2^{\alpha_1}, \qquad \frac{g}{2^{\alpha_1}}=g-1,$$

and so, in this case, the group G would be of order 2. The group of order 2 does satisfy the prescribed condition (1, 2) since it has only one operation besides identity.

If $\alpha_2 > 0$, we have from (3) and (4)

$$g = 2^{\alpha_1}3^{\alpha_2}, \qquad \frac{g}{2^{\alpha_1}}+\frac{g}{3^{\alpha_2}}=g-1,$$

and so

$$3^{\alpha_2}=1+\frac{2}{2^{\alpha_1}-1}, \qquad \alpha_1=1, \alpha_2=1.$$

We thus find that $g = 6$. It is easy to verify that the symmetric group of order 6 satisfies the prescribed condition (1, 2), while the cyclic group of order 6 does not. Hence,

The symmetric group of order 6, *and the group of order* 2 *are the only groups in which every two commutative operations, apart from identity, are conjugate.*

It also follows at once, from the method of proof, that

These two groups are the only groups which have both the properties that all their operations are of prime order, and all those of the same order are conjugate.

§§ 2–6. *Groups in which every two commutative operations of the same order are conjugate.*

§ 2. It is now assumed, in case

$$S_a S_b = S_b S_a, \tag{1}$$

S_a and S_b being of the same order, that there is in G an operation S_c such that

$$S_c^{-1} S_a S_c = S_b. \tag{2}$$

From (1),

$$S_a S_b^{-1} = S_b^{-1} S_a,$$

and there must therefore be in G an operation S such that

$$S^{-1} S_b^{-1} S = S_a. \tag{3}$$

Multiplying both members of (3) by S_b, we have

$$S^{-1} S_b^{-1} S S_b = S_a S_b.$$

Hence the product of any two commutative operations of the same order is a commutator. In particular, *the square of every operation is a commutator.*

Therefore, if we represent the commutator subgroup by C, and it does not include all the operations of G, the abelian* quotient group G/C contains only operations of order 2 besides identity. Hence:

A group in which every two commutative operations of the same order are conjugate, is either a perfect† group, or isomorphic to the abelian group of order 2^α *of type* $(1, 1, 1, \cdots, 1)$.

§ 3. If g is restricted to be a power of a single prime, it is easy to show what groups are possible under the given limitations. Since any group of order p^α (p any prime number) contains invariant operations besides identity, suppose S is such an operation of G. Since every two commutative operations of the same order are conjugate, G can contain no other operations of the same order as S. Hence $S^2 = 1$ and $p = 2$.

With $g = 2^\alpha$, G must either be the cyclic group ‡ or the type defined by

$$P^{2^{\alpha-1}} = 1, \qquad Q^2 = P^{2^{\alpha-2}}, \qquad Q^{-1}PQ = P^{-1},$$

in order to contain a single substitution of order 2. If G is cyclic, obviously $g = 2$. If, however, G has the defining relations just written, there can be only two operations of order $2^{\alpha-1}$ in the subgroups defined by $P^{2^{\alpha-1}} = 1$, since these operations must be conjugate under G. From this it readily follows that $\alpha = 3$, and the defining relations of G are

$$P^4 = 1, \qquad Q^2 = P^2, \qquad Q^{-1}PQ = P^{-1},$$

so that G is the quaternion group. Hence,

The group of order 2 *and the quaternion group are the only groups of order* p^α (p *any prime number*) *in which every two commutative operations of the same order are conjugate.*

§ 4. Suppose that in the group G every two operations of the same order are conjugate, whether commutative or non-commutative. By extending the argument of § 2 it is easy to establish an important property of these groups. These groups are, of course, a special class of the groups we have been considering. Corresponding to any operation S of order 2 in G/C (§ 2), there must be in G an operation S_1 of order 2^{α_1} ($\alpha_1 \geqq 1$), while S_1^2 of order 2^{α_1-1} is contained in C and no operation of order 2^{α_1} can be contained in C if all operations of the same order are conjugate. Corresponding to any operations S' of order 2 in G/C, the group G must contain operations of order 2^{α_1}. Since G/C is abelian, these

* MILLER, Quarterly Journal of Mathematics, vol. 28 (1896), pp. 266–268.

† A group identical with its commutator subgroup is a perfect group. Cf. LIE, *Transformationsgruppen*, vol. 3, p. 679.

‡ BURNSIDE, *Theory of Groups of Finite Order* (1897), p. 75.

operations could not be conjugate to the operations of the same order which correspond to S. Hence S is the only operation in G/C besides the identical operation. It results, therefore, that

A group in which every two operations of the same order are conjugate is a perfect group, or else the commutator subgroup contains just one half the operations of the group.

§ 5. In the article by BURNSIDE referred to in the introduction to this paper, it is shown that in a group in which every two conjugate operations are commutative the commutators are invariants unless the order of the group is a power of 3. Combining this result with the one just stated in § 4 we are enabled to state that

The group of order 2 is the only group in which all operations of the same order are both conjugate and commutative.

§ 6.* *Groups in which every two commutative operations (identity excluded) are so related that each of them is conjugate to some power of the other.*†

If S_a and S_b are any two operations of G such that $S_a S_b = S_b S_a$, we now assume that there occur in G operations S_c and S'_c such that

$$S_c^{-1} S_a S_c = S_b^{\alpha} \tag{1}$$

and

$$S_c'^{-1} S_b S'_c = S_a^{\beta}. \tag{2}$$

From (1) and (2), S_a and S_b are of the same order. Since every two commutative operations (identity excluded) are of the same order, as in § 1, all the operations of the group are of prime order. Consider a Sylow subgroup H_r of order $p_r^{\alpha_r}$. Since any group of order $p_r^{\alpha_r}$ contains invariant operations, it follows that all subgroups of order p_r contained in H_r are conjugate under G. Since the Sylow subgroups are themselves conjugates, it follows that *all subgroups of the same prime order contained in G are conjugate, and that every operation of G is invariant in a Sylow subgroup.*

Let C represent the commutator subgroup of G. Since G/C is abelian and has all its operations of prime order, it must be a group of order $p_r^{\alpha_r}$ of type $(1, 1, \cdots, 1)$. If $\alpha_r > 1$, it is clearly impossible for all the subgroups of order p_r contained in G to be conjugate. Hence

A group in which every two commutative operations, apart from the identity, are each conjugate to some power of the other is a perfect group or else its commutator subgroup is of prime index.

---

* Added July, 1904.

† The groups of § 8 have this property

§§ 7–8. *On the complete sets of conjugate operations in a group.*

§ 7. In § 1 we found that the groups under consideration have just as many complete sets of conjugate operations, aside from identity, as there are distinct prime factors in the order. Since G contains, by Cauchy's theorem, operations of orders $p_1, p_2, \cdots, p_n$, it cannot have fewer complete sets of conjugate operations, even if we neglect identity, than there are distinct prime factors in g. Hence, if λ is the number of complete sets of conjugates without identity, $\lambda \geqq n$. If $\lambda = n$, every operation must be of prime order, and must be conjugate to every other operation of the same order.

From the reasoning of § 1, we have that *the group of order* 2, *and the symmetric group of order* 6 *are the only groups in which the number of complete sets of conjugate operations* (*without identity*) *is exactly equal to the number of distinct prime factors in the order.*

§ 8. It may be of interest to determine what groups are possible when $\lambda = n + 1$, as the solution of this problem can be made to depend largely upon the fact that certain commutative operations must be conjugate. For $n = 1$, the group of order 3 is the only one with $\lambda = n + 1$. We consider a group G with $n \geqq 2$ and $\lambda = n + 1$. The operations of G, apart from those of one conjugate set, must be of prime order. The order of the operations of this conjugate set cannot contain more than two prime factors, or there would occur in G operations of more than $n + 1$ different orders.

We shall divide the consideration of these groups into three parts:

1°. When G contains an operation of order $p_r p_s$ (p_r and p_s distinct). In this case all operations of the same order are conjugate.

Since an operation of order p_n must be transformed into all its powers except identity, just as in § 1, G must contain operations of order $p_n - 1$. Hence

$$p_n - 1 = 2p_t \qquad (p_t \text{ a prime} \neq 2).$$

If $p_t > 1$, $p_t - 1 = 2$, since G cannot contain operations of two different composite orders. Hence $g = 2^{\alpha_1}3^{\alpha_2}$, or $2^{\alpha_1}3^{\alpha_2}7^{\alpha_3}$. If $g = 2^{\alpha_1}3^{\alpha_2}$, each operation is clearly transformed into itself by at least 6 operations. In each case to be considered we shall write some inequalities or equations from the distribution of operations into conjugate sets without detailed explanation. Thus, in this case,

$$(A) \qquad \frac{g}{6} + \frac{g}{6} + \frac{g}{6} \geqq g - 1.$$

Similarly, if $g = 2^{\alpha_1}3^{\alpha_2}7^{\alpha_3}$

$$(B) \qquad \frac{g}{7} + \frac{g}{6} + \frac{g}{6} + \frac{g}{6} + 1 \geqq g.$$

2°. When G contains an operation of order p_r^2.

By the method employed in 1°, $p_n - 1 = 2^2$ or 2. Hence

$$g = 2^{\alpha_1} 3^{\alpha_2} \qquad \text{or} \qquad g = 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3} \qquad (\alpha_2 \geqq 0).$$

If $g = 2^{\alpha_1} 3^{\alpha_2}$, either

$$(C) \qquad \frac{g}{2} + \frac{g}{9} + \frac{g}{9} + 1 \geqq g, \qquad \text{or} \qquad \frac{g}{2^2} + \frac{g}{2^2} + \frac{g}{3} + 1 \geqq g.$$

If $g = 2^{\alpha_1} 5^{\alpha_3}$,

$$(D) \qquad \frac{g}{2^2} + \frac{g}{2^2} + \frac{g}{5} \geqq g - 1.$$

If $g = 2^{\alpha_1} 3^{\alpha_2} 5^{\alpha_3}$,

$$(E) \qquad \frac{g}{2^{\alpha_1}} + \frac{g}{2^{\beta}} + \frac{g}{3^{\alpha_2}} + \frac{g}{5^{\alpha_3}} = g - 1 \qquad (\alpha_1 \geqq 2,\ \beta \geqq 2,\ \alpha_2 \geqq 1,\ \alpha_3 \geqq 1).$$

It is easily seen that (A), (B), (C), (D) and (E) cannot be satisfied by the given values of g. There is, therefore, no group with $\lambda = n + 1$ which contains operations of composite order.

3°. When all the operations of G are of prime order. There can be only one prime which is the order of two operations that are not conjugate. If this prime is not the largest prime factor in g, by the reasoning of § 1, the largest prime factor is 3 and

$$g = 2^{\alpha_1} 3^{\alpha_2} \qquad (\alpha_1 \geqq 2,\ \alpha_2 \geqq 1).*$$

Hence,

$$(F) \qquad \frac{g}{2^2} + \frac{g}{2^2} + \frac{g}{3} \geqq g - 1, \ \cdots.$$

But (F) cannot be satisfied by

$$g = 2^{\alpha_1} 3^{\alpha_2} \qquad (\alpha_1 \geqq 2,\ \alpha_2 \geqq 1).$$

The prime which is the order of two operations that are not conjugate is then p_n, and from the argument of § 1, $p_{n-1} \ngtr 3$. Hence,

$$g = 2^{\alpha_1} 3^{\alpha_2} p_3^{\alpha_3} \qquad (\alpha_1 \geqq 1,\ \alpha_2 \geqq 0,\ \alpha_3 \geqq 0).$$

We shall first consider the case where $\alpha_3 > 0$. Then every operation must be invariant in a Sylow subgroup. This statement follows at once from the fact that every Sylow subgroup contains invariant operations, except in the case of the one conjugate set of operations of order p_3. An invariant operation P of order p_3 and P^{α} where α is a primitive root of p_3 must belong to different conjugate sets. Since P is invariant, P^{α} is also invariant.

If $\alpha_2 = 0$ while $\alpha_3 > 0$,

$$\frac{g}{2^{\alpha_1}} + \frac{g}{p_3^{\alpha_3}} + \frac{g}{p_3^{\alpha_3}} = g - 1,$$

* $\alpha_1 \geqq 2$, for if $\alpha_1 = 1$ the operators of order 2 are conjugates, by Sylow's theorem.

and therefore

$$(G) \qquad p_3^{\alpha_3} + 2^{\alpha_1} + 2^{\alpha_1} = 2^{\alpha_1} p_3^{\alpha_3} - 1 \qquad \text{or} \qquad p_3^{\alpha_3} = 2 + \frac{3}{2^{\alpha_1} - 1}.$$

Hence $\alpha_1 = 1$, $\alpha_3 = 1$, and $g = 10$ since $p_3 > 3$.

If $\alpha_2 > 0$ while $\alpha_3 > 0$,

$$(H) \qquad 3^{\alpha_2} p_3^{\alpha_3} + 2^{\alpha_1} p_3^{\alpha_3} + 2^{\alpha_1} 3^{\alpha_2} + 2^{\alpha_1} 3^{\alpha_2} = 2^{\alpha_1} 3^{\alpha_2} p_3^{\alpha_3} - 1,$$

so that

$$(H') \qquad p_3^{\alpha_3} = \frac{2^{\alpha_1+1} 3^{\alpha_2} + 1}{2^{\alpha_1} 3^{\alpha_2} - 2^{\alpha_1} - 3^{\alpha_2}}.$$

If λ_0 is the largest of the four terms in the left member of (H)

$$4\lambda_0 > g \qquad \text{or} \qquad \lambda_0 > \frac{g}{4}.$$

That is, either one half or one third of the operations in g belong to one conjugate set. Hence either $\alpha_1 = 1$ or $\alpha_2 = 1$.

If $\alpha_1 = 1$, (H') becomes

$$p_3^{\alpha_3} = \frac{2^2 3^{\alpha_2} + 1}{3^{\alpha_2} - 2} = 4 + \frac{9}{3^{\alpha_2} - 2}.$$

Hence

$$\alpha_2 = 1, \; \alpha_3 = 1 \text{ and } g = 2 \cdot 3 \cdot 13.$$

It is easy to verify that no group G exists of this order.

If $\alpha_2 = 1$, (H') becomes

$$p_3^{\alpha_3} = \frac{2^{\alpha_1+1} 3 + 1}{2^{\alpha_1+1} - 3} = 3 + \frac{10}{2^{\alpha_1+1} - 3}.$$

From this, if $\alpha_1 > 1$, $p_3^{\alpha_3} = 5$ and $g = 2^2\ 3\ 5$

If, however, $\alpha_3 = 0$,

$$\frac{g}{2^{\alpha_1}} + \frac{g}{3^{\alpha_2}} + \frac{g}{3^{\beta_2}} = g - 1,$$

where

$$\beta_2 = \alpha_2 \text{ unless } \alpha_2 > 2.$$

But this equation cannot be satisfied when $\alpha_2 > 2$. Hence it may be written

$$3^{\alpha_2} + 2^{\alpha_1} + 2^{\alpha_1} = 2^{\alpha_1} 3^{\alpha_2} - 1,$$

$$3^{\alpha_2} = 2 + \frac{3}{2^{\alpha_1} - 1}.$$

Hence,

$$\alpha_1 = 2, \qquad \alpha_2 = 1 \qquad \text{and} \qquad g = 12.$$

Thus we have the result that $g = 3, 10, 12$, or 60. Of each of these orders there is just one such group.

The group of order 3, *the dihedron group of order* 10, *the tetrahedron group, and the icosahedron group are the only groups which have just one more complete set of conjugate operations, apart from identity, than there are distinct prime factors in the order of the group.*

THE UNIVERSITY OF ILLINOIS.