ON PRIMITIVE GROUPS OF ODD ORDER. A THESIS PRESENTED TO THE UNIVERSITY FACULTY OF CORNELL UNIVERSITY IN CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

Published @ 2017 Trieste Publishing Pty Ltd

ISBN 9780649165209

On Primitive Groups of Odd Order. A Thesis Presented to the University Faculty of Cornell University in Candidacy for the Degree of Doctor of Philosophy by Henry Lewis Rietz

Except for use in any review, the reproduction or utilisation of this work in whole or in part in any form by any electronic, mechanical or other means, now known or hereafter invented, including xerography, photocopying and recording, or in any information storage or retrieval system, is forbidden without the permission of the publisher, Trieste Publishing Pty Ltd, PO Box 1576 Collingwood, Victoria 3066 Australia.

All rights reserved.

Edited by Trieste Publishing Pty Ltd.
Cover @ 2017

This book is sold subject to the condition that it shall not, by way of trade or otherwise, be lent, re-sold, hired out, or otherwise circulated without the publisher's prior consent in any form or binding or cover other than that in which it is published and without a similar condition including this condition being imposed on the subsequent purchaser.

www.triestepublishing.com

HENRY LEWIS RIETZ

ON PRIMITIVE GROUPS OF ODD ORDER. A THESIS PRESENTED TO THE UNIVERSITY FACULTY OF CORNELL UNIVERSITY IN CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

Trieste

Math 2319.04.7

ON PRIMITIVE GROUPS OF ODD ORDER

A THESIS

PRESENTED TO THE UNIVERSITY FACULTY OF CORNELL UNIVERSITY IN CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

BY

HENRY LEWIS RIETZ

BALTIMORE
The Lord Baltimore Press
THE FRIEDENWALD COMPANY
1904

On Primitive Groups of Odd Order.

By Henry Lewis Rietz.

Introduction.

In his "Theory of Groups of Finite Order" (1897), p. 379, Burnside has called attention to the fact that no simple group of odd composite order is known to exist. Several articles* have recently appeared bearing on this question, in which, among other things, it was proved that no such group can be represented as a substitution group whose degree does not exceed 100. This result was obtained by showing that there is no simple primitive group of odd composite order whose degree falls within the given limits. Burnside determined all the primitive groups of odd order of degree less than 100.†

Since any primitive group of odd order is simply transitive, a study of simply transitive primitive groups may throw light on the question of simple groups of odd order. Some important properties of simply transitive primitive groups have been given by Jordan, Miller, and Burnside.‡

The main objects of the present paper are; first, to make a further study of primitive groups with special reference to those of odd order; secondly, to extend the determination of the primitive groups of odd order to all degrees less than 243.

It results that all groups arrived at in this determination are solvable. From this result it is evident that no simple group of odd composite order can occur

---

* Miller, Proc. Lond. Math. Soc., Vol. 33, pp. 6–10. Burnside, Proc. Lond. Math. Soc., Vol. 33, pp. 162–185; 257–268. Frobenius, Berliner Sitzungsberichte (1901), pp. 849–858; 1216–1230.

† At the time of the publication of this work, I had also made this determination with the same results.

‡ Jordan, "Traité des Substitutions," pp. 281–284. Miller, Proc. Lond. Math. Soc., Vol. 28, pp. 533–542. Burnside, loc. cit., pp. 162–185.

as a substitution group of degree less than 243, since if a simple group is represented as a substitution group on the minimum number of letters, it is primitive.

Part I contains a number of theorems, most of which apply to primitive groups whether the order is even or odd, but some use can be made of nearly all of them in determining all the primitive groups of odd order of a given degree. Part II contains the determination of the primitive groups of odd order whose degrees lie between 100 and 243.

I desire to acknowledge my indebtedness to Professor G. A. Miller for helpful suggestions and criticisms during the preparation of this paper.

PART I.

§1.—*On the Number of Substitutions of Degree less than n contained in any Transitive Group of Degree n.*

Let G be any primitive group of composite order g on the elements $a_1, a_2, \ldots, a_n$, and G_s the subgroup leaving a given letter a_s fixed. If $n - \lambda_\alpha$ is the degree of any substitution of G_s, and μ_α the number of substitutions of G_s of this degree, then the total number of substitutions of degree less than n contained in G is

$$\frac{n\mu_1}{\lambda_1} + \frac{n\mu_2}{\lambda_2} + \frac{n\mu_3}{\lambda_3} + \ldots + \frac{n\mu_\rho}{\lambda_\rho}\text{*} \quad \text{or} \quad n\left(\frac{\mu_1}{\lambda_1} + \frac{\mu_2}{\lambda_2} + \frac{\mu_3}{\lambda_3} + \ldots + \frac{\mu_\rho}{\lambda_\rho}\right),$$

where ρ is the number of different degrees occurring among the substitutions of G_s. Since $\mu_1 + \mu_2 + \mu_3 + \ldots + \mu_\rho = \frac{g}{n}$, the above summation in the parentheses may be considered as the sum of just $\frac{g}{n}$ terms of the form $\frac{1}{\lambda}$. We may then rewrite the above expression for the number of substitutions of degree less than n in the form

$$n\sum_{\alpha=1}^{\alpha=\frac{g}{n}} \frac{1}{\lambda_\alpha}. \tag{1}$$

Let x denote the number of systems of intransitivity of G_s, and look upon G_s as having just one system of intransitivity when it is transitive. Then $x + 1$

* Jordan, Liouville's Journal, Vol. 17 (1872), p. 352.

is the average value of λ_α since the average number of letters in the substitutions of an intransitive group is equal to the excess of the degree over the number of systems of intransitivity.* Hence we have

$$x + 1 = \frac{\sum_{\alpha=1}^{\alpha=\frac{g}{n}} \lambda_\alpha}{\frac{g}{n}}. \tag{2}$$

The λ's in this summation cannot all be equal, since identity is included among the substitutions of G_s. Since the arithmetic mean of any number of positive quantities which are not all equal is greater than their geometric mean, it follows that

$$\frac{\sum_{\alpha=1}^{\alpha=\frac{g}{n}} \lambda_\alpha}{\frac{g}{n}} > \sqrt[\frac{g}{n}]{\lambda_1 \lambda_2 \cdots \lambda_{\frac{g}{n}}} \tag{3}$$

and

$$\frac{\sum_{\alpha=1}^{\alpha=\frac{g}{n}} \frac{1}{\lambda_\alpha}}{\frac{g}{n}} > \sqrt[\frac{g}{n}]{\frac{1}{\lambda_1} \cdot \frac{1}{\lambda_2} \cdots \frac{1}{\lambda_{\frac{g}{n}}}}. \tag{4}$$

From (3) and (4) it follows that

$$\frac{\left(\frac{g}{n}\right)^2}{\sum_{\alpha=1}^{\alpha=\frac{g}{n}} \lambda_\alpha} < \sum_{\alpha=1}^{\alpha=\frac{g}{n}} \frac{1}{\lambda_\alpha}. \tag{5}$$

From (2) and (5) it follows that

$$\frac{g}{n(x+1)} < \sum_{\alpha=1}^{\alpha=\frac{g}{n}} \frac{1}{\lambda_\alpha} \quad \text{or} \quad \frac{g}{x+1} < n \sum_{\alpha=1}^{\alpha=\frac{g}{n}} \frac{1}{\lambda_\alpha}. \tag{6}$$

* Jordan, Comptes Rendus, Vol. 74 (1872), p. 977. Frobenius, Crelle's Journal, Vol. 101 (1887), p. 288.

From (1) and (6) we obtain

THEOREM 1.—*In any primitive group G of degree n of composite order g there are more than $\frac{g}{x+1}$ substitutions of degree less than n, where x is the number of systems of intransitivity of the subgroup which leaves a given letter fixed.*

In particular, for a multiply transitive group, $x = 1$. Hence,

Cor. 1. *In a multiply transitive group of degree n more than one-half of the substitutions are of degree less than n.*

Cor. 2. *If G is of degree kp (p a prime) and of order mp (m prime to p and $p-1$), the subgroup G_s has at least $p+1$ transitive constituents.*

For a group of this order contains exactly m operators whose orders divide m.* But all the substitutions of degree less than kp would be of orders prime to p. Hence from the above theorem we have $x > \frac{mp}{x+1}$ or $x > p - 1$.

Since mp must clearly be an odd number, x must be even. Hence, $x \geqq p + 1$.

While it is not our object to treat imprimitive groups, the above theorem can at once be extended to any non-regular transitive group. The only change in the argument is the substitution of $x + m$ in expression (1) for $x + 1$, where m represents the number of letters of the transitive group left fixed by the subgroup which leaves a given letter fixed. Hence,

THEOREM 2.—*In any non-regular transitive group of degree n of order g there are more than $\frac{g}{x+m}$ substitutions of degree less than n, where x and m are defined as above.*

When applied to known groups, I find that in many cases this simple formula gives very nearly the actual number of substitutions of degree less than the degree of the group.

---

* Frobenius, Berliner Sitzungsberichte (1895), p. 1085.

§2.—*Restrictions on the Order of G, when G_s has a Transitive Constituent of Degree p, p^a, pm or pq (p and q primes and $m < p$).*

If G is simply transitive, G_s is intransitive and conversely. Use will frequently be made of the following known theorems:

1. If G_s contains an invariant subgroup H_s of degree $n - \alpha$, H_s is intransitive, and of the n conjugates to which it belongs under G just $\alpha - 1$, besides H_s (H_{s_1}, H_{s_2}, ..., $H_{s_{\alpha-1}}$) occur in G_s. These $\alpha - 1$ subgroups generate a group of degree $n - 1$. Furthermore, G_s transforms H_{s_1}, H_{s_2}, ..., $H_{s_{\alpha-1}}$ in the same manner as the elements of one of its constituent groups are permuted.*

2. Every prime which divides the order of one transitive constituent of G_s divides the order of each of its constituents.†

THEOREM 3.—*If in G_s all the transitive constituents T_1, T_2, T_3, ... of a given degree t are of orders s_1, s_2, s_3, ..., and if $\frac{s_1}{t}$, $\frac{s_2}{t}$, $\frac{s_3}{t}$, ... do not contain a given prime p occurring as a factor in t, the order of G_s is of the form tk, where k is prime to p.*

We shall assume that the invariant subgroup H_s of G_s corresponding to identity in T_1 is of order $h = \lambda p^m$ (λ prime to p, $m > 0$); this must be the case if the theorem is not true. It will be shown that this hypothesis leads to a contradiction. In H_s all the substitutions whose orders are powers of p would generate a group H'_s of order $\lambda' p^m$ invariant in G_s. In the conjugate G_r of G_s, leaving fixed an element of T_1, there occurs just $1/t$ of the substitutions of G_s. Hence the subgroup H'_s would be one of a set of t conjugates transformed by G_r according to one of its transitive constituents T of degree t. In the invariant subgroup H'_r of G_r corresponding to identity in T, all the substitutions are common to G_r and G_s, since they transform H'_s into itself. Now H'_r would be of order $\lambda'' p^m$ (λ'' prime to p). Since in T_1 all the substitutions whose orders are not prime to p are of degree t, all the substitutions whose orders are powers of p common to G_r and G_s are contained in H_s.

If H'_r contained all the substitutions whose orders are powers of p which occur in H_s, the subgroup H'_r would be invariant in G_s and G_r. But this is impossible, since these subgroups are maximal. If H'_r contains only part of these substitutions, let P be such a substitution not contained in H'_r. The order of

* Miller, loc. cit., pp. 584, 585.

† Jordan, loc. cit., p. 284.

$\{H'_r, P\}$ would then be divisible by p^{m+1} and there would be common to G_s and G_r subgroups of order p^{m+1}, which is impossible, since, by hypothesis, the order of H_s is not divisible by p^{m+1}. Hence the theorem.

Cor. 1. *If G_s has a transitive constituent of prime degree p, the order of G_s is not divisible by p^2.*

Cor. 2. *If any number of the transitive constituents of H_s are of a given prime degree p, the constituent group formed of all these transitive constituents is formed by establishing a simple isomorphism between them.*

Cor. 3. *If in G_s all the transitive constituents of a given degree p^a are of class $p^a - 1$, the order of G_s is not divisible by p^{a+1}.*

Cor. 4. *If in G_s all the transitive constituents of degree $mp\,(p > m)$ have p systems of imprimitivity, the order of G_s is not divisible by p^2.*

Lemma. When p and q are distinct primes each of the form $2^m + 1$, there is no imprimitive group of degree pq of odd order whose order is divisible by both p^2 and q^2; and there is no primitive group of degree pq involving in its order only the primes p and q.

The part of this lemma which relates to the imprimitive groups follows at once from the fact, that the only transitive groups of degrees p and q whose orders are odd are the cyclical groups of orders p and q. Suppose there is a primitive group of degree pq of order $p^{a_1}q^{a_2}$. The maximal subgroup G_1, leaving a given letter fixed, is then of degree $pq - 1$ and of order $p^{a_1-1}q^{a_2-1}$. Take $p > q$, then, since $p^2 > pq - 1$, no transitive constituent can be of degree $p^\gamma (\gamma > 1)$. The transitive constituents cannot all be of degree p, since p is not a divisor of $pq - 1$. Since $pq - 1$ is not divisible by q, we may assume that some of the transitive constituents are of degree p while others are of degrees equal to a power of q. But the order of a transitive constituent of degree p is p, and would therefore not contain q as a factor, but every prime which divides the order one transitive constituent of G_1 divides the order of each of its transitive constituent.

THEOREM 4.—*If p and q are distinct primes of the form $2^m + 1$, and if G_s is of odd order, and has as a transitive constituent an imprimitive group of degree pq; then, according as T has p or q systems of imprimitivity, the order of G_s is not divisible by p^2 or q^2.*

To make the conditions definite, suppose that T has q systems of imprimitivity. These systems are then permuted according to the cyclical group of