Note that the full covariant $(a^2d-3abc+2b^3)x^3+\ldots$, regarded as an absolute orthogonal covariant, is reducible in terms of the others.* With this exception the irreducible system of full covariants and invariants of a cubic and quadratic yield the equivalents of the above system upon taking the absolute x^2+y^2 for the quadratic.

(U) *One quartic* $(a, b, c, d, e)(x, y)^4$.—The R.G.F. A.O.C. is got by putting ξ, η for J_{-1}, J_1 in the R.G.F. of (L). The irreducible system consists then of x^2+y^2, the five invariants of § 11, and six covariants

$$I_2\xi^2 \pm I_{-2}\eta^2, \quad I_4 I_{-2}\xi^2 \pm I_{-4} I_2 \eta^2, \quad I_4\xi^4 \pm I_{-4}\eta^4.$$

These prove to be, on rejection of powers of 2 and ι as factors,

$$(a-e)(x^2-y^2)+4(b+d)\,xy,$$

$$(b+d)(x^2-y^2)-(a-e)\,xy,$$

$$\begin{aligned}&\{(a-6c+e)(a-e)+8(b^2-d^2)\}(x^2-y^2)\\ &\qquad\qquad -4\{(a-6c+e)(b+d)-2(a-e)(b-d)\}\,xy,\end{aligned}$$

$$\begin{aligned}&\{(a-6c+e)(b+d)-2(a-e)(b-d)\}(x^2-y^2)\\ &\qquad\qquad +\{(a-6c+e)(a-e)+8(b^2-d^2)\}\,xy,\end{aligned}$$

$$(a-6c+e)(x^4-6x^2y^2+y^4)+16(b-d)\,xy\,(x^2-y^2),$$
$$(b-d)(x^4-6x^2y^2+y^4)-(a-6c+e)\,xy\,(x^2-y^2).$$

On some Properties of Groups of Odd Order. (Second Paper.)

By W. Burnside. Communicated and received December 13th, 1900.

In the present paper I have extended the method used in the paper "On Groups of Degree n and Class $n-1$," communicated to the Society at the June meeting, so as to make it applicable to any transitive substitution group. As the title of the paper indicates, the method is considered mainly in its application to groups of odd

* [A remark by a referee leads me to emphasize the above. Absolute orthogonal invariants of a p-ic are invariants of the p-ic and x^2+y^2, and *vice versa*. It has therefore been hastily supposed elsewhere that the complete irreducible invariant system for a p-ic and quadratic produces exactly the complete (absolute) orthogonal system for the p-ic, when x^2+y^2 is taken for the quadratic. A first case of the redundancy of the former system for the latter purpose is exhibited above. The search for complete absolute orthogonal systems is not identical with the search for invariant systems of forms one of which is a quadratic.]

order; but the method itself and the general results of §§ 2 and 4 hold good whether the order is even or odd.

It has been known for some time that a group of order $2n$ (n odd) has a self-conjugate sub-group of order n. This is shown by noticing that when the group is represented as a regular substitution group in $2n$ symbols all its odd operations, and none of its even operations, belong to the alternating group. It is clear that no analogous method of treatment could be used to demonstrate a similar property for a group of order pn, where every prime factor of n is greater than the odd prime p. At the same time, the probability that such a group has an analogous property forces itself on the attention; and it is here shown that this expectation is well founded. The main result arrived at is to show that if p, an odd prime, is the smallest factor of the order of a group, the group must have a self-conjugate sub-group of index p, unless either p^4 or p^3q, where q is a prime factor of p^2+p+1, is a factor of the order.

It is also shown that no odd number less than 40,000 can be the order of a simple group.

1. Let G be a group of order n, and suppose that G is represented as a regular substitution group in the n symbols

$$x_1, x_2, \dots, x_n.$$

If H is any sub-group of G, whose order is μ ($n=\mu\nu$), the n x's will be interchanged regularly in ν sets of μ each by the operations of H. Let

$$x_1, x_2, \dots, x_\mu$$

be one of these sets. Then y_1 or

$$x_1+x_2+\dots+x_\mu$$

is a linear function of the x's which is invariant for each of the operations of H and for no other operations of G. It therefore takes ν distinct values for all the operations of G. Let these be

$$y_1, y_2, \dots, y_\nu.$$

Each y is the sum of μ x's, and no x occurs in two different y's. The y's therefore are permuted among themselves by the operations of G; and G can be represented as (*i.e.*, is simply or multiply isomorphic with) a permutation group of the y's. The group in the x's is simply or multiply isomorphic with the group in the y's, according as H does not or does contain a self-conjugate sub-group of G. The group of the y's will be represented by the scheme

$$y'_i = y^{(k)}_{i'}$$
$$(i, i' = 1, 2, \dots, \nu),$$
$$(k = 1, 2, \dots, n),$$

and will be called G'. If G is multiply isomorphic with G', then, for some two or more values of the affix k,

$$y^{(k)}_{i'} = y_i$$

for each i. In any case, for each affix k the ν symbols

$$y^{(k)}_1, \; y^{(k)}_2, \; \dots, \; y^{(k)}_\nu$$

are the y's in some altered sequence.

The preceding statement is only a slightly modified form of Dyck's procedure* for representing G as a non-regular substitution group.

Suppose now that H is simply or multiply isomorphic with a cyclical group. The necessary and sufficient condition for this is that H shall not be the same as its derived group. If k is the order of a cyclical group with which H is isomorphic, it must be possible to divide the set of symbols

$$x_1, \; x_2, \; \dots, \; x_\mu$$

which are regularly permuted by H into k sets of l each ($\mu = kl$),

$$\begin{array}{lll} x_1, & x_2, & \dots, \; x_l, \\ x_{l+1}, & x_{l+2}, & \dots, \; x_{2l}, \\ \dots & \dots & \dots \\ x_{(k-1)l+1}, & x_{(k-1)l+2}, & \dots, \; x_{kl}, \end{array}$$

which are cyclically permuted among themselves in the order written by every operation of H. Moreover, if ω is a k-th root of unity, the linear function η_1 or

$$x_1 + \dots + x_l + \omega\,(x_{l+1} + \dots + x_{2l}) + \dots + \omega^{k-1}\,(x_{(k-1)l+1} + \dots + x_{kl})$$

is a relative invariant for every operation of H; any operation of H changing it into $\omega'\eta_1$, where ω' is a power of ω. Hence η_1^k is an absolute invariant of H, and it therefore takes just ν distinct values for all the operations of G. Let

$$\eta_1^k, \; \eta_2^k, \; \dots, \; \eta_\nu^k$$

be these ν values, Each is the k-th power of a linear function of the x's, and no x occurs in two η's. Moreover, if their sequence is suitably

* *Math. Ann.*, Vol. xxii., pp. 90–92.

chosen, the x's which occur in η_i are the same as those which occur in y_i. Hence the ν k-th powers are permuted among themselves by every operation of G in exactly the same way as the y's.

Now, if any operation of G changes η_i^k into η_j^k, it must change η_i into $\omega'\eta_j$, where ω' is some power of ω. Hence G may be represented as a group of linear substitutions of the η's; and the scheme giving G when so represented will be

$$\eta_i' = \omega_{ki}\eta_{i'}^{(k)}$$
$$(i,\ i' = 1,\ 2,\ \ldots,\ \nu),$$
$$(k = 1,\ 2,\ \ldots,\ n),$$

where every symbol ω_{ki} represents a power of ω. This group will be called G''. If every ω_{ki} is replaced by unity, the group becomes identical with G', η_i being written everywhere for y_i. If G is simply isomorphic with G', so also is G''. If G is multiply isomorphic with G', G'' may also be so. This will, in fact, be the case if for an operation in which

$$\eta_{i'}^{(k)} = \eta_i \quad (i = 1,\ 2,\ \ldots,\ \nu)$$

the symbols ω_{ki} are not all unity.

Any operation of G'' replaces $\prod_1^\nu \eta_i$ by $\prod_{i=1}^{i=\nu} \omega_{ki} \prod_1^\nu \eta_i$. Hence, unless $\prod_{i=1}^{i=\nu} \omega_{ki}$ is unity for every operation of G'', then G'', and therefore also G, is isomorphic with a cyclical group.

The ν k-th roots of unity, $\omega_{k1}, \omega_{k2}, \ldots, \omega_{k_\nu}$, that occur in the specification of any operation of G'' will be called the *factors* of that operation; so that the totality of the operations of G'' for which the products of the factors are unity constitute a self-conjugate sub-group, which contains the derived group.

2. Let p^α be the highest power of a prime p that divides n, the order of G, and let H be a sub-group of order p^α of G. Let I be the greatest sub-group that contains H self-conjugately; and suppose that every operation of I is permutable with every operation of H, so that H must be Abelian. Let S be an operation of H of order p^β, such that there is no operation S' of H for which the relation $S = S'^p$ holds. Then H is isomorphic with a cyclical group of order p^β, and a relative linear invariant η_1 for H may be chosen, such that it is changed by S into $\omega\eta_1$, where ω is a primitive p^β-th root of unity; while it remains unaltered by every operation of that sub-group of H in respect of which H is isomorphic with $\{S\}$.

If S occurs in $1+kp$ sub-groups of order p^α, and if in G' each sub-group of order p^a leaves h symbols unchanged, then the operation of G' which corresponds to S will leave $(1+kp)h$ symbols unchanged. These symbols must be interchanged transitively by the greatest sub-group K in which S is self-conjugate. In fact, the h symbols unchanged by H are interchanged transitively by I, which is contained in K; and K contains operations transforming H into every other sub-group of order p^a in which S enters.

In G'', then, there are $(1+kp)\,h$ η's which are changed into multiples of themselves by S, and these η's are transformed among themselves with factors by K.

Suppose, if possible, that

$$\eta_1' = \omega\eta_1,\ \eta_2' = \omega^a\eta_2,\ \dots \quad (a \neq 1)$$

represents the effect of S on the η's which are changed into multiples of themselves. K must contain an operation Σ of the form

$$\eta_1' = \omega^b\eta_2,\ \dots,$$

and $\Sigma^{-1}S\Sigma$ would be $\quad \dots,\ \eta_2' = \omega\eta_2,\ \dots\,.$

This is impossible, since $\Sigma^{-1}S\Sigma = S$. Hence each factor, for the η's which are changed into multiples of themselves by S, must be ω; and, since h is not a multiple of p, their product is a primitive p^β-th root of unity. Suppose next that

$$(y_{s+1}y_{s+2}\dots y_{s+p^b}) \quad (b \leqslant \beta)$$

is any cycle of the operation that corresponds to S in G'. The corresponding part of S in G'' is

$$\begin{aligned} \eta_{s+1}' &= \omega_1\eta_{s+2}, \\ \eta_{s+2}' &= \omega_2\eta_{s+3}, \\ \dots\ &\ \dots\ \ \dots \\ \eta_{s+p^b} &= \omega_{p^b}\eta_{s+1}. \end{aligned}$$

Since the p^β-th power of this is identity,

$$(\omega_1\omega_2\dots\omega_{ph})^{p^{\beta-b}} = 1.$$

The product $\omega_1\omega_2\dots\omega_{p^b}$ cannot therefore be a primitive p^β-th root of unity; and a similar result holds for each cycle of S in G'.

The product of the factors of S is therefore a primitive p^β-th root of unity, multiplied by $p^{\beta-1}$-th roots; *i.e.*, a primitive p^β-th root of unity. Hence G'', and therefore also G, has a self-conjugate sub-group of index p^β in which neither S nor any of its powers occurs. The same reasoning may be repeated with this self-conjugate sub-group, leading at last to the result that G has a self-conjugate sub-group of index p^a.

From this general result the following particular ones are at once deduced. If p is the smallest prime, and p^a the highest power of p, which divide the order of a group G, and if the sub-groups of order p^a are Abelian groups with either one or two generating operations, then G has a self-conjugate group of index p^a.. The case $p = 2$, and 3 a factor of the order, is a possible exception.

In fact, when these conditions are satisfied, the order of the group of isomorphisms* of a sub-group of order p^a is not divisible by any prime greater than p, and therefore every operation of I (in the original statement) is necessarily permutable with every operation of H.

In particular, if G is a group of odd order $p^a m$ ($a = 1$ or 2), where p is less than any prime factor of m, then G has a self-conjugate sub-group of order m.

For in this case all the conditions are necessarily satisfied.

If G is a group of odd order $p^3 m$, where p is less than any prime factor of m, and if the sub-groups of order p^3 are Abelian, while m and p^2+p+1 contain no common factor, then G has a self-conjugate sub-group of order m.

For the only isomorphisms of order greater than p, which an Abelian group of order p^3 can admit, have factors of p^2+p+1 for their order.

Also, if the odd order of G contains an unrepeated prime factor q, of the form 2^n+1, then G has a self-conjugate sub-group of index q.

Another special result of the general theorem is the following, which applies alike to groups of odd and of even order:—

If p^a is the highest power of a prime p which divides the order $p^a m$ of a group G, and if every operation of a sub-group of G of order p^a is a self-conjugate operation of G, then G is the direct product of groups of orders p^a and m.

For in this case G has self-conjugate sub-groups of orders m and p^a.

3. Before proceeding to a second application of the general method of § 1, it will be necessary to prove a property of certain groups whose order is a power of a prime, when represented as substitution groups affected with "factors." I consider, first, the case in which the substitution group is a cyclical group in p symbols generated by $(x_1 x_2 \dots x_p)$, while the factors are p-th roots of unity. The general

* *Theory of Groups*, p. 251.

operation of such a group will be

$$x'_1 = \omega_1 x_{1+k},$$
$$x'_2 = \omega_2 x_{2+k},$$
$$\ldots \quad \ldots \quad \ldots$$
$$x'_p = \omega_p x_{p+k},$$

where $\omega_1, \omega_2, \ldots, \omega_p$ are p-th roots, and the suffixes of the x's are reduced mod. p. The total number of such operations, *i.e.*, the order of the most general group of the kind, is clearly p^{p+1}; and the order of the self-conjugate sub-group in which each symbol is merely multiplied by a factor is p^p. Suppose, now, that such a group contains an operation S,

$$x'_r = \omega^{a_r} x_r \quad (r = 1, 2, \ldots, p),$$

for which the product of the factors is not unity, so that

$$a_1 + a_2 + \ldots + a_p \not\equiv 0 \mod p.$$

The group then contains the p operations

$$x'_r = \omega^{a_{r+k}} x_r \quad (r = 1, \ldots, p),$$
$$(k = 0, 1, \ldots, p-1),$$

obtained by transforming S by the powers of $(x_1 x_2 \ldots x_p)$; and therefore also the operation

$$x'_r = \omega^{\sum_k y_k a_{r+k}} x_r \quad (r = 1, 2, \ldots, p).$$

where $y, y_1, \ldots, y_{p-1}$ are any integers. Consider now the system of congruences

$$\sum_k y_k a_{r+k} = z_r \quad (r = 1, 2, \ldots, p).$$

The determinant of the left-hand side

$$\begin{vmatrix} a_1 & a_2 & \ldots & a_p \\ a_p & a_1 & \ldots & a_{p-1} \\ \ldots & & \ldots & \ldots \\ a_2 & a_3 & \ldots & a_1 \end{vmatrix}$$

is easily shown to be congruent to $a_1 + a_2 + \ldots + a_p$; and, since by supposition this is not zero, mod. p, the system of congruences have a solution in integers for the y's, whatever integers the z's may be. The group therefore contains the p operations

$$x'_s = x_s \, (s \neq r); \quad x'_r = \omega x_r.$$

But these generate a sub-group of order p^p; and, combining this with

$(x_1 x_2 \dots x_p)$, the order of the group is p^{p+1}. Hence, if the order of a group of the kind considered is less than p^{p+1}, the product of the factors must be unity for every operation which changes each symbol into a multiple of itself. It is to be noticed that no inference can be drawn with respect to the operations which interchange the symbols cyclically.*

Still supposing that the factors are p-th roots of unity, I consider now the case where the substitution group is a transitive group of degree p^a. Let T be any self-conjugate operation of order p of the substitution group. The symbols left unchanged by any operation S of the substitution group are permuted in sets of p by T. If $x_1, x_2, \dots, x_p$ is such a set of symbols, then, in the group as affected by factors, each is replaced by a multiple of itself by the operation S. If the product of the p factors affecting these symbols were not unity, then T and S would, as regards these p symbols, generate a group of order p^{p+1} by the preceding result. Hence, again in this case, if the order of the group is less than p^{p+1}, the product of the factors of the unchanged symbols of any operation must be unity. Now, for an operation of order p, the product of the factors for a set of p symbols which are permuted cyclically by the operation is necessarily unity. In fact, let

$$x_1' = \omega_1 x_2, \; x_2' = \omega_2 x_3, \; \dots, \; x_p' = \omega_p x_1$$

be the operation, so far as it affects the symbols in question. The p-th power of this substitution is

$$x_r' = \omega_1 \omega_2 \dots \omega_p x_r \quad (r = 1, 2, \dots, p);$$

and, since this must be identity, the product of the factors is unity, as stated.

The general result of this discussion may then be stated thus:—If a group of order p^a $(a \leqslant p)$ be represented as a transitive substitution group affected by factors which are p-th roots of unity, the product of the factors for any operation of order p belonging to the group is unity.

4. Returning now to the general theorem, let p^a, as before, be the highest power of a prime p which divides the order $p^a m$ of a group G. Let H be a sub-group of order p^a, and let I be the greatest sub-group

* In fact, $x_1' = \omega x_2, \; x_2' = x_3, \; \dots, \; x_p' = x_1$
and $x_1' = x_1, \; x_2' = \omega x_2, \; \dots, \; x_p' = \omega^{p-1} x_p$
generate a group of order p^3 in which ω is the product of the factors for one of the cyclical operations.

that contains H self-conjugately. Suppose also that every operation of I, whose order is relatively prime to p, is permutable with every operation of H. Let η_1 be a relative invariant for H, which is unaltered by every operation of a self-conjugate sub-group of index p of H, and is changed into $\omega\eta_1$ by some operation S of H not occurring in this sub-group.

If in G' the sub-group H leaves μ symbols unchanged, they must be transitively permuted by the operations of I. In G'' each of these symbols is changed into a multiple of itself by every operation of H. Moreover, S changes η_1 into $\omega\eta_1$; and therefore each of the other $\mu-1$ must be changed by S into ω times itself, as otherwise S could not be permutable with every operation of I whose order is relatively prime to p. The remaining $m-\mu$ symbols are permuted transitively in sets of p^a, p^b, ... by the operations of H in G'. Hence, by the result obtained above, if the order of S is p, and if $\alpha \leqslant p$, the product of the factors of S, so far as these $m-\mu$ symbols are concerned, is unity. Under these conditions, then, the product of all the factors of S is ω^{μ}, and μ is necessarily relatively prime to p. Hence G'', and therefore also G, has a self-conjugate sub-group of index p.

If $p\,(>2)$ is the smallest prime which divides the order of G, and if $\alpha = 3$, while the sub-groups of order p^3 are not Abelian, all the conditions imposed are satisfied. In fact, the primes dividing the order of the group of isomorphisms of H must be factors of $(p-1)\,(p^2-1)$; while the only two types of non-Abelian groups of order p^3 both contain operations of order p which do not enter in a suitably chosen sub-group of order p^2. Hence:—

If p is the smallest prime dividing the order of a group G of odd order, and if p^3 is the highest power of p which divides the order, then, if the sub-groups of order p^3 are not Abelian, the group has a self-conjugate sub-group of index p^3.

Combining this with the previous result, it follows that, if $p\,(>2)$ be the smallest prime and p^{α} the highest power of p which divide the order of a group, then the group must have a self-conjugate sub-group of index p^{α}, unless (i) $\alpha \geqslant 4$ or (ii) $\alpha = 3$, and a factor of p^2+p+1 divides the order.

5. From the preceding results it is not difficult to show that no odd number which is the product of six primes can be the order of a simple group.

If $p_1, p_2, p_3, \ldots$ denote odd primes in ascending order of magnitude, it follows from the preceding theorems and from the results contained in chap. xv. of my book on the *Theory of Groups* (especially Theorem iv.) that, (i) $p_1^4p_2p_3$, (ii) $p_1^3p_2^3$, (iii) $p_1^3p_2^2p_3$, (iv) $p_1^3p_2p_3^2$, (v) $p_1^3p_2p_3p_4$ are the only possible forms for the order of such a group. Moreover, in the last four, a sub-group of order p_1^3 must be Abelian with no operations of order p_1^2; and one of the primes p_2, p_3, p_4 must be a factor of $p_1^2+p_1+1$.

(i) *Order* $p_1^4p_2p_3$.—There must be p_2p_3 sub-groups of order p_1^4; otherwise the group can be represented as of prime degree and is certainly soluble (*Proc. Lond. Math. Soc.*, Vol. xxxiii., p. 177). If the operations of these sub-groups were all distinct, there would be a self-conjugate sub-group of order p_2p_3. If some, or all, of the self-conjugate operations of a sub-group of order p_1^4 occur in no other sub-group of order p_1^4, every operation common to two sub-groups of order p_1^4 must be permutable with an operation of order p_2 or p_3. In this case there would be exactly p_2p_3-1 operations whose orders are divisible by p_2 or p_3, and the group would be composite. If any operation were self-conjugate in more than one sub-group of order p_1^4, it would be one of p_2 or p_3 conjugate operations, and again the group would be composite. Lastly, if an operation P of order p_1 is self-conjugate in one sub-group of order p_1^4, and enters in another as one of p_1 or more conjugate operations, there must be* an operation Q (of order p_2 or p_3) such that P, $Q^{-1}PQ$, $Q^{-2}PQ^2$, ... are permutable with each other. These would generate a sub-group of order p_1^3, which would be common to several sub-groups of order p_1^4, and would therefore be one of p_3 or p_2 conjugate sub-groups. The group again therefore would be composite.

(ii) *Order* $p_1^3p_2^3$.—If there are p_1^3 sub-groups of order p_2^3, they must, if the group be simple, have common operations; and, since p_1^3 is the only factor of the order which is congruent to unity, mod. p_2, the totality of these common operations form a self-conjugate sub-group. The group is therefore composite.

(iii) and (iv) *Order* $p_1^3p_\beta^2p_\gamma$.—If an operation of order p_1 is permutable with one of order p_β, there must be a sub-group of order $p_1^3p_\beta$, and this must contain a sub-group of order p_β self-conjugately. This sub-group would be one of p_γ conjugate sub-groups, and the

* *Theory of Groups*, p. 100.

group would therefore be composite. It may be assumed therefore that there are no operations of order p_1p_β.

If an operation of order p_γ is conjugate with one of its own powers, then $p_1^2p_\beta^2(p_\gamma-1)$ is the greatest number of operations the group can contain whose orders are divisible by p_γ. If a sub-group of order p_β^2 is contained self-conjugately in a greater sub-group, then $p_1^2r_\gamma(p_\beta^2-1)$ is the greatest number of operations, whose orders are powers of p_β, that can be contained in the group. Lastly, $p_\beta p_\gamma(p_1^3-1)$ or $p_\beta^2(p_1^3-1)$ is the greatest number of operations of order p_1 the group can contain. Now the sum of these numbers is less than $\frac{2}{p_1}+\frac{1}{p_\beta}$ times the order of the group; and, since $\frac{2}{p_1}+\frac{1}{p_\beta}$ is necessarily less than unity, this is impossible. Hence either an operation of order p_γ is not conjugate with any of its powers or a sub-group of order p_β^2 is contained self-conjugately in no greater sub-group. In either case the group is composite, from the results of § 2.

(v) *Order* $p_1^3p_2p_3p_4$. — Unless operations of each of the orders p_2, p_3, p_4 are conjugate to powers of themselves, the group is certainly composite, by § 2. If the condition is satisfied, the greatest possible numbers of operations contained in the group whose orders are divisible by p_2, p_3, and p_4 respectively are

$$p_1^2p_3p_4(p_2-1),\quad p_1^2p_2p_4(p_3-1),\quad p_1^2p_2p_3(p_4-1).$$

The greatest possible number of operations of order p_1 is $p_3p_4(p_1^3-1)$. The sum of unity with these four numbers must be equal to or greater than the order of the group. This sum is, however, less than $\frac{3}{p_1}+\frac{1}{p_2}$ times the order. Hence, unless p_1 is 3, the group is certainly composite.*

If p_1 is 3, the group is composite unless one of the other prime factors is 13. The order must therefore be $3^3.13.pq$: and the group has a sub-group of order $3^3.13$, in which there are just 13 sub-groups of order 3 all conjugate to each other.

* [*Note, January* 19*th*, 1901.—This method, combined with the results of § 2, may be used to prove in a somewhat similar way that a group of order $p_1^{a_1}p_2^{a_2}\,..\,p_n^{a_n}$, where each of the indices $a_2, a_3, \ldots, a_n$ is either 1 or 2, and where $p_1 > n-1$, is composite, with a possible exception in the case where there are $p_2^{a_2}p_3^{a_3}\ldots p_n^{a_n}$ sub-groups of order $p_1^{a_1}$.]

The discussion of this particular case presents no serious difficulty. It may be shown at once that the group is composite if it contains operations of composite order; and that the only constitution of the group, which is consistent with its being simple, is one in which there are

$$\begin{array}{llll} & 3^2.13p & \text{sub-groups of order} & q, \\ & 3^2.13q & \quad ,, \qquad\quad ,, & p, \\ & 3^2.p.q & \quad ,, \qquad\quad ,, & 13, \\ \text{and} & pq & \quad ,, \qquad\quad ,, & 3^3, \end{array}$$

without common operations. This leads to the equation

$$17pq-117(p+q)+1=0;$$

and 7 and 409 is the only pair of primes satisfying this equation. The group would then contain $1+2.409$ sub-groups of order 409; and it could be represented as a piimitive group of degree $1+2.409$, in which the sub-groups that leave one symbol unchanged permute the remaining ones in two equal transitive sets. The group would also contain operations of order 13 which permute all the symbols. That such a group is non-existent is shown on p. 179 of my paper, " On Some Properties of Groups of Odd Order " (*Proc. Lond. Math. Soc.*, Vol. XXXIII., pp. 162–185).

6. The number of prime factors in the order of a simple group of odd order is thus shown to be not less than 7. Combining this with the limitations on the order involved by the results of § 2, it will be found that the only odd numbers less than 40,000 which can possibly be the order of such a group are:—$3^5.7.13$, $3^5.7.19$, $3^4.5^3$, $3^4.5^2.7$, $3^4.5^2.11$, $3^4.5^2.13$, $3^4.5^2.19$. There is no difficulty in verifying that no one of these numbers can be the order of a simple group; so that 40,000 is a lower limit for the order, if odd, of a simple group. There is no doubt that by a similar detailed examination this limit might be carried a good deal further; but, in view of the possibility of some more general properties of groups of odd order being discovered, it seems hardly worth while to carry a mere method of enumeration beyond the point reached.