On infinite simple permutation groups.

By GRAHAM HIGMAN in Manchester.

§ 1. Introduction.

Let G be a group of permutations of a set E (which will need to be infinite if our considerations are to be non-trivial). If α is an element of G, the set of elements of E such that $x\alpha \neq x$ is called the *domain of instability* of α and is written $D(\alpha)$. If G happens to be simple, the domains of instability of its elements enjoy a certain homogeneity property. Precisely, if α and β are two elements of G (other than 1) there is a relation of the form

$$\beta = \varrho_1^{-1}\alpha^{\pm 1}\varrho_1 \cdot \varrho_2^{-1}\alpha^{\pm 1}\varrho_2 \ldots \varrho_r^{-1}\alpha^{\pm 1}\varrho_r$$

between them, whence

$$D(\beta) \subset \{D(\alpha)\varrho_1\} \cup \{D(\alpha)\varrho_2\} \cup \ldots \cup \{D(\alpha)\varrho_r\}.$$

This implies, for instance, that if one of the elements of G has an infinite domain of instability so do they all (apart from 1), and all the domains of instability have the same cardinal. The main theorem of this note is in the opposite direction; that is, we assume a homogeneity property, and deduce that G is nearly simple. To state the theorem we need one more definition. The subset X of E is *totally unstable* with respect to α if the intersection of X and $X\alpha$ is empty. Then the theorem is:

Theorem 1. *If to every set α, β, γ $(\gamma \neq 1)$ of elements of G corresponds an element ϱ such that $\{D(\alpha) \cup D(\beta)\}\varrho$ is totally unstable with respect to γ, then the derived group of G is simple.*

From theorem 1 it is fairly easy to deduce the following

Theorem 2. *If* $\mathbf{a}, \mathbf{b}$, *are infinite cardinals, the necessary and sufficient condition that there exists a simple group of cardinal* $\mathbf{a}$ *with a subgroup of index* $\mathbf{b}$ *is that*

$$\mathbf{b} \leqq \mathbf{a} \leqq 2^{\mathbf{b}}.$$

But it is easy to prove directly:

Theorem 3. *If* $\mathbf{a}$ *is an infinite cardinal, there exists a simple group of cardinal* $\mathbf{a}$ *all of whose proper subgroups have index* $\mathbf{a}$.

If, as well as the axiom of choice, we assume the generalized continuum hypothesis, then theorems 2 and 3 give us a complete picture of the possibilities for the indices of the subgroups of a simple group of given cardinal. For if the order is $\aleph_\lambda$ and λ is a limit ordinal, then by the hypothesis $\mathfrak{b} < \aleph_\lambda$ implies $2^{\mathfrak{b}} < \aleph_\lambda$, so that by theorem 2, all proper subgroups have index $\aleph_\lambda$. But if the order is $\aleph_{\lambda+1}$, then a proper subgroup may have index $\aleph_{\lambda+1}$ or $\aleph_\lambda$. Obviously the first possibility always occurs; the second occurs in some groups by theorem 2, and does not occur in others, by theorem 3.

§ 2. Proof of theorem 1.

First we show that if N is a normal subgroup of G not consisting of the unit element only, then N contains the derived group G'. To that end, let $\gamma \neq 1$ be an element of N, and let α, β be elements of G. Let ϱ be the element whose existence the hypothesis of the theorem assures, and write $\delta = \varrho\gamma\varrho^{-1}$. Then the intersection of $D(\alpha)\varrho\gamma$ and $D(\beta)\varrho$, and hence of $D(\alpha)\delta$ and $D(\beta)$, is empty. But $D(\alpha)\delta$ is, of course, $D(\delta^{-1}\alpha\delta)$, so that $D(\delta^{-1}\alpha\delta)$ and $D(\beta)$ do not meet, which implies that $\delta^{-1}\alpha\delta$ and β commute. Thus

$$\begin{aligned}\alpha^{-1}\beta^{-1}\alpha\beta &= \alpha^{-1}\cdot\delta^{-1}\alpha\delta\cdot\beta^{-1}\cdot\delta^{-1}\alpha^{-1}\delta\cdot\alpha\beta \\ &= \alpha^{-1}\delta^{-1}\alpha\cdot\delta\cdot\beta^{-1}\delta^{-1}\beta\cdot\beta^{-1}\alpha^{-1}\delta\alpha\beta.\end{aligned}$$

But δ is conjugate to γ and so belonges to N, and hence so does $\alpha^{-1}\beta^{-1}\alpha\beta$. Thus N contains G', as required.

Next, we prove that the second derived group G'' coincides with G'. Obviously we may assume $G' \neq 1$, and, since G'' is a normal subgroup of G, it is only necessary, by the first part of the proof, to show that $G'' \neq 1$. We take $\alpha = \beta = \gamma$ in the above discussion to be an element not 1 in G'. Then, as we have seen, for a suitable conjugate δ of γ, $D(\gamma)$ and $D(\delta^{-1}\gamma\delta)$ are disjoint. Evidently, $\gamma \neq \delta^{-1}\gamma\delta$, so that $\gamma^{-1}\delta^{-1}\gamma\delta$ is an element of G'' which is not 1. Thus $G'' = G'$.

Lastly, we show that the property assumed for G holds automatically also for G'. Indeed, given $\alpha, \beta, \gamma\,(\gamma \neq 1)$, in G we choose ϱ as in the statement of the theorem, and then σ so that $\{D(\gamma) \cup D(\varrho)\}\sigma$ is totally unstable with respect to γ. As before, this implies that if we set $\eta = \sigma\gamma\sigma^{-1}$, then $D(\gamma)$ and $D(\eta^{-1}\varrho\eta)$ are disjoint. In particular, $\eta^{-1}\varrho\eta$ is the identity on $\{D(\alpha) \cup D(\beta)\}\varrho$, which is contained in $D(\gamma)$. Thus

$$\{D(\alpha) \cup D(\beta)\}\varrho\eta^{-1}\varrho^{-1}\eta = \{D(\alpha) \cup D(\beta)\}\varrho.$$

That is, ϱ, in the statement of theorem 1, can be chosen in G'.

Now if N is any normal subgroup of G' which is not 1, we can apply the first part of the proof to deduce that $N \supset G''$. Since $G'' = G', N = G'$, so that G' is simple, as required.

§ 3. Examples.

The simplest example of a group G satisfying the conditions of theorem 1 is perhaps the following. Let R be the real line, and let G be the group of those homeomorphisms α of R into itself for which $D(\alpha)$ is bounded. Here if α and β belong to G, $D(\alpha) \cup D(\beta)$ is contained in an interval of R, and if $\gamma \neq 1$ there is an interval of R which is totally unstable for γ. Since the closed intervals of R are permuted transitively by G, G satisfies the conditions of the theorem. In this case, as we shall see below, G is its own derived group, and so is simple.

This example can be generalized in several directions. First, we may replace R by Euclidean n-dimensional space R^n, the definition of G being otherwise unchanged. In the verification that G satisfies the condition of the theorem, we need only replace the word interval by sphere. Thus G' is simple; but in this case I do not know whether G and G' are distinct.

Secondly, we may take instead of R any linearly ordered set E in which all closed intervals are similar, and which has neither greatest nor least member; and then G is the group of similarities (order isomorphisms) α of E onto itself with $D(\alpha)$ bounded. Here again $G' = G$, so that G is simple.

Lastly, keeping to the real line R, we may include in G not only homomorphisms, but all upper semicontinuous mappings α of R onto itself with $D(\alpha)$ bounded. The interest of this example is that it shows that the hypotheses of theorem 1 do not imply that G, or even G', has no elements of finite order.

§ 4. Deduction of theorem 2.

We note first that if there exists a simple group of cardinal $\mathbf{a}$ with a subgroup of index $\mathbf{b}$, then certainly

$$\mathbf{b} \leqq \mathbf{a} \leqq 2^{\mathbf{b}}.$$

The first inequality is evident. To prove the second, we recall that G can be represented as a transitive group of permutations of the cosets of H. Because G is simple, this representation is faithful, so that G is isomorphic to a subgroup of the group of all permutations of a set of $\mathbf{b}$ elements, which has order $2^{\mathbf{b}}$.

Conversely, suppose that $\mathbf{a}$ and $\mathbf{b}$ satisfy the inequalities. We shall construct a simple group of order $\mathbf{a}$ with a subgroup of index $\mathbf{b}$. We begin by constructing a linearly ordered set E of cardinal $\mathbf{b}$ with the properties: (i) all closed intervals of E are similar, (ii) E has neither a first nor a last element, and (iii) E has a bounded family of $\mathbf{b}$ disjoint closed intervals. It

is convenient to take E to be the element set of a linearly ordered field, because (i) and (ii) are then automatic. We recall that if K is a linearly ordered field the simple transcendental extension $K(t)$ can be linearly ordered by taking t to be infinitely small compared to any element of K. (A non-zero element of $K(t)$ can be written as a power series in ascending powers of t, and is positive if the first non-zero coefficient is positive.) Now let K_0 be the ordered rational field, and T a set of cardinal $\mathbf{b}$ of independent transcendents over K_0. We suppose that T is given an arbitrary linear order. If $t_1, t_2, \ldots, t_n$ are any finite set of elements of T, with $t_1 > t_2 > \cdots > t_n$, we may adjoin them one by one, in order, to K_0, and by extending the order in the above manner at each stage we obtain a linear order for $K(t_1, t_2, \ldots, t_n)$. It is not hard to see that the orders obtained in this way for subfields of $K(T)$ are coherent, and give a linear order for $K(T)$. Moreover the closed intervals $t_\alpha \leqq x \leqq 2t_\alpha$, t_α in T, are disjoint and lie in the closed interval $0 \leqq x \leqq 1$. Thus we may take E to be the element set of $K(T)$, and have all the properties (i) to (iii).

Now let G be the group of all similarities α of E with $D(\alpha)$ bounded. We shall show that G is its own derived group. If α is an element of G, we define an equivalence relation between the elements of E by putting

$$x \equiv y(\alpha)$$

if and only if for some integers m, n (positive, negative, or zero)

$$x\alpha^m \leqq y \leqq x\alpha^n.$$

That this is an equivalence relation is easily verified. If $x\alpha = x$, then x is the only element in its equivalence class; if $x\alpha \neq x$, then for all elements y equivalent to x, $y\alpha > y$ or $y\alpha < y$ according as $x\alpha > x$ or $x\alpha < x$, and we call the class an ascending or a descending class accordingly. Now if β is an element of G which determines the same equivalence relation as α, and if the ascending classes for α are ascending for β and vice versa, then we can choose ϱ in G so that $\beta = \varrho^{-1}\alpha\varrho$. If $x\alpha = x$, we put $x\varrho = x$. Then in each ascending class we choose an element x_0, and similarity ϱ_0 of the interval $x_0 \leqq x \leqq x_0\alpha$ on the interval $x_0 \leqq x \leqq x_0\beta$. The intervals

$$x_0\alpha^n \leqq x \leqq x_0\alpha^{n+1} \qquad (n = 0, \pm 1, \pm 2, \ldots)$$

cover the equivalence class; and on this interval we put

$$x\varrho = x\alpha^{-n}\varrho_0\beta^n.$$

Thus we define ϱ on each ascending class, and descending classes are treated in a similar way. That ϱ is a similarity of E, that $\beta = \varrho^{-1}\alpha\varrho$, and that $D(\varrho) \subset D(\alpha)$, so that ϱ belongs to G, are easily verified. We may, in particular, take $\beta = \alpha^2$, and obtain $\alpha = \alpha^{-1}\varrho^{-1}\alpha\varrho$, so that G is its own derived group, as asserted.

Next, by condition (iii) above, G has order $2^{\mathbf{b}}$. Moreover, by conditions (i) and (ii), G permutes the closed intervals of E transitively. Since the number of these intervals is **b**, we can choose a set of **b** elements of G which already permute them transitively, and since $\mathbf{b} \leqq \mathbf{a} \leqq 2^{\mathbf{b}}$, we can enlarge this set to a set containing **a** elements. This subset generates a subgroup of G of order **a**, and since G is its own derived group, this subgroup can be enlarged to one, still of order **a**, which also is its own derived group. Call this last group G_0. By its construction, G_0 permutes the closed intervals of E transitively, so that we can apply theorem 1 to prove that its derived group, that is, G_0 itself, is simple. But G_0 is of order **a**, and the subgroup leaving fixed some particular element of E is of index **b**. Thus we have proved theorem 2.

§ 5. Proof of theorem 3.

Let E be a set containing **a** elements, and let $S(E)$ be the group of all permutations α of E for which $D(\alpha)$ is finite. The elements of $S(E)$ can be divided into odd and even permutations exactly as in the case when E is finite, and the even permutations form a subgroup $A(E)$ of index two in $S(E)$. That $A(E)$ is simple is a corollary of the same fact for a finite set E with at least five elements, and $A(E)$ has order **a**. Thus it is sufficient to prove that $A(E)$ has no proper subgroup of index less than **a**.

Suppose then that G is a subgroup of $A(E)$ of index less than **a**. We show first that G permutes the elements of E transitively. For if not, E is the union of two non-empty disjoint sets A and B, each of which admits G. Let A_i, where i runs over a suitable index set, be all the subsets of E of the form $A \cup (x) - (y)$, with x in B and y in A. Since at least one of A and B has cardinal **a**, there are **a** distinct sets A_i. But for each A_i we can evidently choose α_i in $A(E)$ such that $A\alpha_i = A_i$. Because A is invariant under G, the cosets $G\alpha_i$ are all distinct, so that G has index **a**, contrary to assumption. Hence G must permute E transitively.

Next, it follows by induction on n that G is n-tuply transitive for each positive integer n. For suppose $n > 1$, and that we already know that G is $(n-1)$-tuply transitive. If E' is a subset of E whose complement has $n-1$ elements, the subgroup of $A(E)$ consisting of elements α for which $D(\alpha)$ is contained in E' can be identified with $A(E')$. Then $G \cap A(E')$ is a subgroup of $A(E')$ of index less than **a**, and E' has cardinal **a**. Hence $G \cap A(E')$ permutes E' transitively, and so G permutes E n-tuply transitively.

Finally, a subgroup of $A(E)$ which is n-tuply transitive for all n is easily seen to be normal and hence to coincide with $A(E)$. That is, a proper subgroup of $A(E)$ has necessarily index **a**.

It is a pleasure to acknowledge that all the considerations of this paper arose from a question of T. SZELE, who asked, in a letter to B. H. NEUMANN, whether every infinite group has a subgroup of countable index. That this is not so is clear from theorem 2, and even more from theorem 3. I should also like to acknowledge that most of the ideas involved have been clarified in discussion with Professor NEUMANN.

(Received June 14, 1954.)