ON FINITE GROUPS AND THEIR CHARACTERS

RICHARD BRAUER

The idea of a presidential address seems to require a lecture delivered in the most refined and dignified scientific atmosphere yet understandable to the layman, a lecture which treats a difficult field of mathematics in such a complete manner that the audience has the excitement, the aesthetic enjoyment of seeing a mystery resolved, perhaps only with the slightly bitter feeling, of asking afterwards: Why did I not think of that myself?

Well, I don't know how my predecessors did it, but I know that I can't do it. Since the founding fathers of the Society have placed the presidential address at the time in the life of the president when he disappears into anonymity among the ranks of the Society, I shall not even try it. The choice of the field about which I am going to speak was a natural one for me, not only because of my own work in the theory of groups of finite order, but because of the new life which has appeared in this field in recent years. However, in spite of all our efforts, we know very little about finite groups. The mystery has not been resolved, we cannot even say for sure whether order or chaos reigns. If any excitement can be derived from what I have to say, it should come from the feeling of being at a frontier across which we can see many landmarks, but which as a whole is unexplored, of planning ways to find out about the unknown, even if the pieces we can put together are few and far apart. My hope then is that some of you may go out with the idea: "Now let me think of something better myself."

Let me first mention one difficulty of the theory. We have not learned yet how to describe properties of groups very well; we lack an appropriate language. One of the things we can do is to speak about the characters of a group G. I cannot define characters here. Let me only mention that we have a partitioning of the group G into disjoint sets $K_1, K_2, \cdots, K_k$, the classes of conjugate elements. The characters then are k complex-valued functions $\chi_1, \cdots, \chi_k$, each constant on each class K_i. They have a number of properties which connect them with properties of the group. These characters can be used to prove general theorems on groups, but we seem to have little control about what can be done and what not. You will see this more clearly later when I discuss specific results. I can give two reasons

Presidential address delivered before the Annual Meeting of the Society, January 28, 1960; received by the editors November 19, 1962.

for this particular behavior of the characters. The first is that I believe that we don't know all about characters that we should know. My reason for this statement is the following: If you take groups of a special type, groups whose order g contains some prime number p only to the first power

$$g = pg_0, \qquad (p, g_0) = 1,$$

some powerful results can be proved. The groups G have a subgroup P of order p. If N is the normalizer of P, i.e. the subgroup of all σ in G with $\sigma P = P\sigma$, and if the characters of N are known, the values of the characters of G for the so-called p-singular classes of G can be given (apart from certain $\pm$ signs). It is this type of connection between groups and subgroups we are looking for. Where our assumptions are satisfied, this result can be used very well to explore groups. Now it seems natural to assume that this result must be a special case of some general result where

$$g = p^a g_0 \quad \text{with} \quad (p, g_0) = 1 \quad \text{and} \quad a \geqq 1.$$

Actually, this idea has motivated a good deal of my work for quite a number of years. While many things can be proved, the part which would be most desirable for applications is lacking; there are not even conjectures about what one should try to prove. I may perhaps mention in passing that the results in the special case $a = 1$ in some sense are not quite as special as it may seem. Conditions can be given for groups of an order $g = pg_0$, $(p, g_0) = 1$, with p no longer a prime number where many of the results for the special case still hold. It may not be unreasonable to conjecture that all or almost all simple groups are of this type; there are some heuristic reasons for such a statement.

There is a second reason which may explain why the characters may fall short of our expectations. This is that there is a notion, more general than that of a group, where we have characters. I may call these objects pseudo-groups just to have a name. Perhaps, I should explain briefly how a group G qualifies as a pseudo-group. Suppose you observe somebody who has a group and who picks elements σ, τ and forms the product $\sigma\tau$. You don't see actually what the elements are, but you observe to which classes K_α the elements σ, τ, $\sigma\tau$ belong. You may then be able to determine what the probability is that the product of an element of K_α with an element of K_β lies in a given class K_γ. Whenever you have a setup of this kind and some further conditions are satisfied, you have a pseudo-group. (This description is not quite honest, because the further conditions do not look very natural in this language.) Theorems which we may want to prove for groups

may not hold for pseudo-groups, and in such cases, characters are not the appropriate tool.

We shall now turn to a discussion of groups themselves. Since we assume that the order is finite, an inductive approach seems indicated. Suppose we know certain subgroups H_i of a group G, what can we say about G? If we ask the question in this form, the answer is: Not very much. Obviously, a group H can be imbedded in many different groups G which have little in common. What we have to do is to assume that the given subgroups H_i play a particular rôle in G. For instance, in the theory of characters, the centralizers $C(\sigma)$ of elements σ are important. This is the set of all elements τ of G which commute with σ. To formulate a definite question, let me ask:

Given the centralizers

$$C(\sigma_1), C(\sigma_2), \cdots, C(\sigma_r)$$

of all elements of prime orders, and suppose we know the intersections of any two of them. If G has center 1, these are proper subgroups of G. If we could say what G is, we would have an inductive approach. Actually, we can say something about G. For instance, it is trivial to see that the order of G is determined. It is not so trivial to see that the characters of G are determined, and this shows that we can do even a bit in putting the pieces together. However, we are far from being able to prove an isomorphism theorem stating that our pieces determine G up to isomorphism.

I should mention that the question posed can be modified in many ways. The form given above is not the best possible one, but one which can be stated quickly.

Since we are not able to put the pieces together, one may ask: How much does information about a single $C(\sigma)$ help with a discussion of G? I will show later that in some concrete cases, we can say amazingly much about G.

I shall next discuss a general principle by which relations between groups G and subgroups H can be discussed. I mentioned earlier that many group theoretical properties or quantities can be expressed in terms of characters. Clearly, there are many such quantities which have the same value for G and for suitable subgroups. Each will then give a relation between the characters of G and those of suitable subgroups H.

For instance, let σ be an element of G, let n be an integer and denote by $A_G^{(n)}(\sigma)$ the number of solutions of $\xi^n = \sigma$ in G. Clearly each such ξ lies in $C(\sigma)$. So if $H \supseteq C(\sigma)$,

$$A_G^{(n)}(\sigma) = A_H^{(n)}(\sigma).$$

On the other hand, $A_G^{(n)}(\sigma)$ can be expressed in terms of the characters of G and we obtain relations between characters of G and H. Unfortunately, they are too complicated to be exploited except in special cases.

Another application of the same principle yields some of the results mentioned above, but an actual statement would require too many definitions and be too technical.

I come now to still another application of the same principle which leads to the program I mentioned in the beginning. This application works only for groups of even order. There is an old conjecture to the effect that all groups of odd order are solvable. The program would require a proof of this so that groups of odd order could be discarded. We are far from a proof, but recently, more progress has been made on this problem first by John Thompson and later by him, M. Hall and W. Feit so that it may not be daydreaming to say that some day this question will be cleared up.[1]

So then I will concentrate on groups of even order. The quantity which we use here is the following one. If σ is an element of G, let $B_G(\sigma)$ denote the number of elements ξ of order 2 which satisfy the equation

$$\xi^{-1}\sigma\xi = \sigma^{-1}.$$

Clearly, the elements y of G satisfying $y^{-1}\sigma y = \sigma^{\pm 1}$ form a group $C^*(\sigma)$ which is either $C(\sigma)$ or has twice the order. Then if H is any subgroup of G with $H \supseteq C^*(\sigma)$, we have

$$B_G(\sigma) = B_H(\sigma).$$

Again, $B_G(\sigma)$ can be expressed by the characters of G. The method then yields relations

$$g \sum_{\chi_\mu} \frac{h_\mu^2}{\chi_\mu^{(1)}} \chi_\mu(\sigma) = \cdots$$

where g is the order of G, the h_μ are certain rational integers formed by means of the characters and where on the right the same expressions for the group H appear. The sum extends over all characters of G. The method is to use combinations of these formulas for various elements σ in which only relatively few characters appear. This re-

[1] See the note added at the end of the paper.

quires some deep results on characters which I cannot describe in detail without becoming too technical. The outcome is that we obtain estimates for the order g by means of certain subgroups. As I mentioned, the general result requires concepts from the theory of group representations which are beyond the scope of this lecture. Rather than tiring you with them, I shall describe some particular cases in which the results can be brought into an explicit form. In principle, we have corresponding statements whenever we know the 2-Sylow group P of G. For the sake of simplicity, I assume that G does not have a normal subgroup H of half its order, since in the excluded case more direct methods for constructing G out of H are available.

Let first P be a dihedral group of order 2^n

$$P = \{\rho, \sigma\}, \qquad \rho^{2^{n-1}} = 1, \qquad \sigma^2 = 1, \qquad \sigma^{-1}\rho\sigma = \rho^{-1}.$$

Here, set $\tau = \rho^{2^{n-2}}$. This is an element of order 2. If $n \geqq 3$, g has the form

$$g = 2\alpha c(\tau)^3 \left(\frac{1}{c(\tau, \sigma)} + \frac{1}{c(\tau, \rho\sigma)}\right)^2$$

where $c(\xi)$, $c(\xi, \eta)$ denote the number of elements commuting with ξ or with ξ and η. Here, α is a rational number which satisfies the inequalities

$$\left(1 - \frac{1}{2^{n-1}}\right)\left(1 - \frac{1}{2^n}\right) \leqq \alpha \leqq \left(1 + \frac{1}{2^{n-1}}\right)\left(1 + \frac{1}{2^n}\right),$$

i.e. which is close to 1. In fact, α has the form $x(x+\delta)/(x-\delta)^2$ where $\delta = \pm 1$ and where x is the degree of an irreducible representation, $x \equiv \delta \pmod{2^n}$, $x > 1$. Of course, if $C(\tau)$ is known, $c(\tau, \sigma)$ and $c(\tau, \rho\sigma)$ are known. We say that we have a regular case, if $c(\tau, \sigma) = c(\tau, \rho\sigma)$. Here, g can be brought into the form

$$g = \beta \frac{x(x+1)(x-1)}{2}, \qquad \beta \text{ integral.}$$

The groups $L_2(x)$, x a prime power, form an example. It is not known whether there exist examples where x is not a prime power.

In the irregular case, $c(\tau, \sigma)/c(\tau, \rho\sigma)$ can be shown to lie close to 1. The only known example of an irregular group is the simple group of order 2520.

There are similar results, somewhat more complicated in the case $n = 2$.

As a second example, I mention the 2-Sylow group

$$P = \{\sigma, \tau, \rho\},$$
$$\rho^{-1}\sigma\rho = \tau, \quad \rho^{-1}\tau\rho = \sigma, \quad \tau\sigma = \sigma\tau,$$
$$\sigma^{2^m} = 1, \quad \tau^{2^m} = 1, \quad \rho^2 = 1, \quad m \geqq 2.$$

Then P is somewhat more complicated, the discussion is far more difficult, but the results are far simpler. It turns out that g is completely determined, if we know $C(\rho)$, in fact when we know the orders of certain subgroups of $C(\rho)$. As an example, I mention the projective groups $LF(3, q)$ of a projective geometry over a finite field with $q \equiv 1 \pmod 4$. Actually the group can be characterized within this framework. The other cases of q have been treated before. There also is the unitary group $HO(3, q^2)$.

Returning to the general case, let me say what the general program of treating groups of even order is to which these methods lead. We consider a group H which contains an element σ of order 2 in its center and we consider groups $G \supset H$ for which $C(\sigma) = H$ and which have the same 2-Sylow group P as H. The construction of H can be reduced to that of $H/\{\sigma\}$, a group of smaller order. On the other hand as I have indicated, once H is known, properties of G can be obtained, in particular, the order g of G can be estimated. Of course, this is not enough, but my examples above indicate that it seems feasible to characterize the simple groups of finite order in this manner.

Added November, 1962. The hope which I expressed in my address has been fulfilled. Recently, W. Feit and John G. Thompson announced that they succeeded in proving the famous conjecture stating that groups of odd order are solvable (Proc. Nat. Acad. Sci. U.S.A. **48** (1962), 968–970). It is already evident that the deep methods developed by these authors will have far reaching consequences for other problems in group theory. For instance, D. Gorenstein and J. Walter have made progress with the question of groups with dihedral 2-Sylow groups discussed as an example in this lecture. There is every indication that this case will be cleared up soon.

Originally, I had not intended to submit the manuscript of my talk for publication. I have changed my mind since the hope for progress on the problem is now far greater.

HARVARD UNIVERSITY