I. Introduction. Finite simple groups. The title of my talk described a problem in which I have been interested for a very long time:

Given a prime number $p$. We wish to find the relations between the properties of the $p$-blocks of characters of a finite group $G$ and structural properties of $G$.

Only the case is of interest that $G$ is $p$-singular, i.e., that the order $g = |G|$ is divisible by $p$.

The problem of finding all simple finite groups is still unsolved. During the last few years, very significant progress has been made by John Thompson, Daniel Gorenstein, John Walter, Helmut Bender, Michael Aschbacher, and others. It seems that most group theorists feel that it is only a matter of time until all finite simple groups will be classified. Jonathan Alperin wrote to me recently:

"It is a good guess that within five years everything should be pretty clear. But how long it will take to clean up and correct all the papers—and they do need that—is anybody's guess."

I may add that there may be some doubt about the exact meaning of a classification of the finite simple groups. We shall come back to this point in more detail below. While in our problem, we are concerned with arbitrary finite groups, not only simple finite groups, there cannot be any doubt about the importance of the recent developments for our problem.

Our notation will be more or less standard. By a group, we shall usually mean a finite group without mentioning this explicitly. By a character $\chi$ of a group $G$, we shall always mean a complex character. The set of irreducible characters of $G$ will be denoted by $\text{Char}(G)$. The symbol $\text{Cl}(G)$ will be used for the set of conjugacy classes of $G$. Since characters $\chi$ are constant on each $K \in \text{Cl}(G)$, it suffices to know the value of $\chi$ for a class representative $\sigma_K \in K$. We then have the character matrix $X_G$ of $G$,

$$X_G = (\chi(\sigma_K)), \quad (\chi \in \text{Char}(G), K \in \text{Cl}(G)). \quad (1.1)$$

The rows here are indexed by the $\chi \in \text{Char}(G)$ and the columns are indexed by the $K \in \text{Cl}(G)$. Since $\text{Char}(G)$ and $\text{Cl}(G)$ both consist of the same...
number \( k(G) \) of elements, \( X_G \) is a square matrix of degree \( k(G) \); the number \( k(G) \) is the class number of \( G \).

We conclude this introductory section with a discussion of the terminology used in connection with the simple groups. We distinguish the following cases

1. The simple groups \( G \) of prime order \( p \). Since they are of little interest, we shall usually exclude them without mentioning this explicitly. In other words, we shall restrict our attention to the nonsolvable simple groups.

2. The alternating permutation groups \( A_n \), \( n > 5 \). These are the groups of particular interest in Galois theory since \( A_n \) is the Galois group of the general algebraic equation of degree \( n \) and the nonsolvability of \( A_n \) is equivalent with the fact that the equation cannot be solved by radicals. It was already known to Galois that a nonsolvable group of order at most 60 was isomorphic to \( A_5 \).

3. The Chevalley groups (simple groups of Lie type). These are the groups described in the celebrated paper [25] of Claude Chevalley. We find it convenient to include their twisted analogues discovered by Robert Steinberg, Jacques Tits, Michio Suzuki, and Rimhak Ree. Among the simple groups of Lie type, we have the classical groups, i.e., the linear, symplectic, orthogonal and unitary simple groups. The first cases of classical groups were already discussed by Galois. A more systematic study was made by C. Jordan [F] and by L. E. Dickson [A], [29], and [30].

4. Sporadic groups. It has been known for more than a hundred years that there exist simple groups, not of the types discussed so far. It has become customary to refer to these additional simple groups as "sporadic groups".

The first five sporadic groups, the Mathieu groups, were described by E. Mathieu in 1861 and 1873. The next sporadic group was discovered by Zvonimir Janko in 1965, after a gap of almost one hundred years. Today, twenty-four sporadic groups are known, and it seems probable that there are at least two more such groups. On the other hand, it is quite possible that there are infinitely many (nonisomorphic) sporadic groups.

The crux of the matter then is the question:

"Are there finitely many or infinitely many sporadic groups?"

The optimists among us will be inclined to accept the first alternative. If they succeed in finding an upper bound for the order of sporadic groups, then the whole problem can be handled by a computer, though the costs of the project may very well be prohibitive. If they succeed only in establishing an upper bound for the number of sporadic groups, but not for their order, there is still a possibility that a kind of inductive procedure will be able to solve the problem.

We have already indicated that if the pessimists are right and there are infinitely many sporadic groups, this in itself need not be a disaster. After all, there are infinitely many simple groups of Lie type, but we have an excellent classification. On the other hand, it is quite possible that we have an infinite sequence \( \{G_n\} \) with the orders \( |G_n| \) strictly increasing and that infinitely often, entirely new types of groups occur in our sequence (or, as some people

\footnote{It is interesting to note that Jordan in the introduction of his fundamental book [F] refers to the book as a "commentary" on the work of Galois. Historians of mathematics have remarked that this is one of the most modest statements ever made by a mathematician.}
say, new monsters appear). Then, indeed, it may become necessary to state more clearly what we mean by a classification of the simple groups. It is not even impossible that no classification exists.

I have to confess that I find the uncertainty delightful. If it should be shown, say in ten years, that the 26 sporadic groups mentioned above are all there is, the theory of simple groups would lose much of its interest. It would still require a lot of work such as the question of finding better and shorter proofs, but the real excitement would be gone.

II. Centralizers of elements of prime order. Suppose that $G$ is a simple group, not of prime order. A celebrated theorem of Feit and Thompson [33] states that $|G| = g$ is even. Hence $G$ contains elements $z$ of order 2 or, as we say, involutions $z$.

Now, I have shown in [7] that

$$g < (|\mathcal{O}_G(z)| + 2)^2!;$$

(2.1)

the proof is quite elementary. It follows that there exists only a finite number of (nonisomorphic) simple groups $G$ in which the centralizer of an involution is isomorphic to a given group $H$. Actually, it was this fact which formed the starting point of the recent developments. We may also mention that, for many particular choices of $H$, the problem of finding the simple groups satisfying the condition has been solved. For an example of such a case, we may refer to [47] in which Z. Janko constructed the first sporadic group $J$ which was not a Mathieu group.

As a first application of block theory, the following result can be proved, cf. [9V, (6D)].

**Theorem (2A).** Let $G$ be an arbitrary group of even order $g$. Let $P$ be a Sylow 2-group of $G$ and let $\varepsilon > 0$ be a real number. Then there exists an involution $z$ in the center $\mathcal{Z}(S)$ of $S$ such that

$$|G: O_2^e(G)| < [2(1 + \varepsilon)|S|^2|\mathcal{O}_G(z)|^{3/2}]!. \quad (2.2)$$

Here, $O_2^e(G)$ is the core of $G$, i.e., the unique maximal normal subgroup of $G$ of odd order.

Involutions in the center of a Sylow 2-group of $G$ are often termed central involutions of $G$. The following remark is obvious since $|S| \leq |\mathcal{O}_G(z)|$.

**Corollary (2B).** The right side of (2.2) is at most equal to

$$[2(1 + \varepsilon)|\mathcal{O}_G(z)|^{1/2}]!.$$

The Theorem (2A) shows that we have inequalities such as (2.1) not only for simple groups $G$ but for all finite groups $G$ which do not have a normal subgroup of odd order larger than 1. The upper bound in (2.2) may or may not be smaller than that in (2.1). No direct proof of (2A) avoiding block theory is known.

Already in [7], it was remarked that no result of the type of (2.1) was known in which elements of odd prime order $p$ figured instead of involutions.
This was an obvious point, since in simple Lie groups of odd characteristic $p$, one would naturally be more interested in elements of order $p$ and their centralizers than in involutions.

In a recent paper, Paul Fong and I proved the following result [19, Theorem 2]:

**Theorem (2C).** Let $p$ be a prime integer. At least one of the following holds:
(a) There exists a real-valued function $f$ of a real argument with the following property: If $G$ is a finite group of order divisible by $p$ and if $c$ is the maximum of the orders $|\varphi_G(x)|$ for elements $x \in G$ of order $p$, then

$$|G: O_p(G)| < f(c).$$

(b) There exist infinitely many sporadic simple groups of order divisible by $p$.

If we have case (a), we have a generalization of (2.1) and (2A). The function $f$ can actually be constructed. However, we may also have the alternative (b) and we don't know whether or not we then have inequalities of the type (2.1).

We study the situation further if we have case (b).

We can show, cf. [19]:

**Theorem (2D).** If we have case (b) in Theorem (2C), there exists an infinite sequence $\{G_n\}$ of sporadic groups $G_n$ such that the sequence $\{|G_n|\}$ is strictly increasing, that all $|G_n|$ are divisible by $p$ and that the Sylow-$p$-subgroup $S_n$ of $G_n$ are all isomorphic. Moreover, the degrees of all $p$-modular nonprincipal characters of $G_n$ tend to $\infty$ for $n \to \infty$.

Theorem (2D) indicates that rather dreadful types of sporadic groups exist, if we have case (b) in Theorem (2C). If we have case (a), then Theorem (2A) has analogues for elements $z$ of odd prime order instead of involutions. However, it has not been possible to prove this without further hypotheses.

**III. Groups with a cyclic Sylow $p$-subgroup.** Sporadic groups were introduced in §1 as the simple groups which are neither of prime order, nor alternating groups, nor of Lie type. Because of this rather negative type of description, there is really nothing much of a general nature we can say about sporadic groups. On the other hand, if we are to solve the problem of classifying the simple groups, it will be sporadic groups on which we have to concentrate.

In order to make any progress, it will be necessary to add special assumptions, preferably assumptions which are satisfied by the twenty odd sporadic groups known today.

A look at the list in Appendix II will divulge a remarkable fact. The order of each of the known sporadic groups $G$ contains prime factors $p$ with the exact exponent 1. Of course, we have no idea whether or not this is also true for the unknown sporadic groups. Incidentally, it is of course true for the simpler groups of prime order and—what is not at all trivial—for the alternating groups.

It seems reasonable then to study groups $G$ which have a Sylow $p$-subgroup $P$ of order $p$ for some prime number $p$. It is not necessary to require simplicity of $G$ at this stage.
If we do this, again block theory can be applied. In the character matrix $X_G$ in (1.1), we first take the irreducible characters $\chi$ whose degree is not divisible by $p$ and we first take the conjugacy classes $K \in \text{Cl}(G)$ consisting of elements of order prime to $p$. Then $X_G$ breaks up in the form

$$X_G = \begin{pmatrix} U_G & V_G \\ W_G & 0 \end{pmatrix}$$

(3.1)

where 0 denotes a zero-matrix. Moreover, if we set $N = \mathcal{N}_G(P)$ and if we take the irreducible characters and conjugacy classes of $N$ in a suitable order, then in

$$X_N = \begin{pmatrix} U_N & V_N \\ W_N & 0 \end{pmatrix}$$

the matrix $V_N$ is almost the same as $V_G$; we only have to multiply certain of the rows of $V_N$ with $-1$ in order to obtain $V_G$, cf. [51].

It is much easier to study $N$ than $G$. In fact, $N$ does not possess irreducible characters whose degree is divisible by $p$. Hence we have

$$X_N = (U_N, V_N).$$

(3.2)

**Theorem (3A).** Let $G$ be a group which has a cyclic Sylow $p$-subgroup $P$ of prime order $p$. Set $N = \mathcal{N}_G(P)$. If the irreducible characters and conjugacy classes of $G$ and $N$ are taken in a suitable order, the character matrices of these groups take the form

$$X_G = \begin{pmatrix} U_G & V_G \\ W_G & 0 \end{pmatrix}, \quad X_N = (U_N, V_N)$$

where $V_G$ is obtained from $V_N$ by multiplying some of the rows with $-1$.

**Corollary (3B).** If $G$ and $N$ are as in (3A), the class number $k(G)$ of $G$ is at least as large as $k(N)$.

No direct proof of (3B) is known. We derive some further corollaries. Note that it follows from Sylow's theorem that $g = |G|$ has the form

$$g = prm(1 + n*p)$$

(3.3)

where $|\mathcal{P}_G(P)| = pm$, where $r = |\mathcal{N}_G(P)/\mathcal{P}_G(P)|$ divides $p - 1$, and where $m > 1$ and $n^* > 0$ are integers. Since

$$|G: \mathcal{N}_G(P)| = 1 + n^*p,$$

(3.4)

$1 + n^*p$ is the number of distinct Sylow $p$-subgroups of $G$.

In [6], we dealt with the case that $m = 1$ and that $G$ is perfect. We have:

**Corollary (3C).** Assume that $G$ is a perfect group with a Sylow $p$-subgroup $P$ of prime order $p$. If $n^*$ in (3.4) is less than $\frac{1}{2}(p - 3)$, then $G \simeq \text{PSL}(2, p)$ with $p > 3$ or $G \simeq \text{PSL}(2, p - 1)$, where $p > 3$ is a Fermat prime. On the other hand, if $n^* > \frac{1}{2}(p - 3)$, then $n^*$ has the form

$$n^* = (puw + u^2 + u + w)/(w + 1)$$

where $u$ and $w$ are positive integers with $(u + 1)|w(p - 1)$. 
In [20], the method was used to prove the following result which had been conjectured by E. Artin.

**Corollary (3D).** The only simple groups $G$ whose order $g = |G|$ is divisible by a prime $p > g^{1/3}$ are the groups isomorphic to one of the two groups occurring in the first part of (3C).

The Theorem (3A) was derived from properties of a $p$-block with a defect group of order $p$. In an important paper, E. C. Dade [28] showed that analogous properties hold for $p$-blocks with a cyclic defect group. Using Dade's theorem, Marcel Herzog [44] succeeded in determining all perfect groups $G$ with a cyclic $Sylow/p$-subgroup $P$ such that $|P|$ exceed $|G|^{1/3}$.

Recently, in [15], I have used Dade's theorem to study groups with a cyclic $Sylow/p$-subgroup $P$. The number $q^*$ in [15] is taken as $p$. The result is as follows.

**Theorem (3E).** Assume that $G$ is a perfect group with a cyclic $Sylow/p$-subgroup $P$. Set $|P| = q$, $|\mathcal{S}_G(P)| = qm$, $|\mathcal{R}_G(P)| = qmr$, $|G: \mathcal{R}_G(P)| = n = 1 + np$.

(i) The numbers $m$, $r$, and $n^*$ are integers; $r|p - 1$; $g = qrmn$.

(ii) There is associated with $G$ a finite set $\mathcal{L}$ of lattice points in a Cartesian $x - y$-plane. The set $\mathcal{L}$ consists of the lattice points $(x, y)$ which lie on a nondegenerate hyperbola and for which $0 < y < n^*$. The hyperbola $\mathcal{H}$ passes through the points $(-1, 0)$, $(n^*, 0)$, $(0, n^*)$ and the line $y = -1/p$ is an asymptote. Furthermore, the involutory birational transformation $\gamma$

$$
(x, y) \rightarrow (y/(x + 1), (xy + x^2 + x)/(x + 1))
$$

maps $\mathcal{H}$ onto itself.

(iii) The set $\mathcal{L}$ is empty, if and only if $G/O_p(G) \simeq PSL(2, p)$ with $p > 3$ or if $p$ is a Fermat prime larger than 3 and $G/O_p(G) \simeq PSL(2, p - 1)$.

(iv) Except in the cases in (iii), there exist points $Z_1, Z_2$ in $\mathcal{L}$ such that $Z_2 \neq Z_1$, $Z_2 \neq \gamma(Z_1)$. If two such points $Z_1, Z_2$ are given, then $\mathcal{H}$ and $\mathcal{L}$ are uniquely determined and so are $p$ and $n$. We can give an upper bound for $|G/O_p(G)|$.

On applying (3E), we choose arbitrarily two lattice points $Z_1, Z_2$ with $Z_2 \neq Z_1$, $Z_2 \neq \gamma(Z_1)$. We can then determine $\mathcal{H}$, $n$ and $p$. However, in general, $p$ will not be a prime number nor will $n$ be an integer with $n \equiv 1 \pmod{p}$. In these cases, $Z_1$ and $Z_2$ will not belong to a group $G$. In the opposite case, we can find $\mathcal{L}$, $n$ and $p$. We also have information concerning the $\chi$ in the principal $p$-block. It is still possible that no group $G$ exists, but there are at most finitely many possibilities for $G/O_p(G)$.

So far, this method has not led to the discovery of a new sporadic group, but maybe it will some day.

It seems that all simple groups have cyclic $Sylow/p$-subgroups for some prime $p$ dividing $|G|$.

**IV. Characters of groups with a given Sylow $p$-subgroup.** It is now natural to ask: Can the results of §III be generalized to the case where the group $G$ has a noncyclic $Sylow/p$-subgroup $P$? So far, all attempts to do so have failed.
The purpose of what we call "block theory" is to find a substitute.

We mention here only the papers on block theory which are needed in these notes. In addition to my papers [8], [9], [10], there are the important contributions of J. A. Green [39], [40], and [41] and of Walter Feit [J]. A great deal of work appears in the literature, some in different context and under different names. As discussed in [9 II], it is natural to assume that not only the Sylow $p$-subgroup $P$ of $G$ but also the fusion $\mathcal{F}(G)$ of $G$ in $P$ is given.

So far, essentially the only cases treated have been cases where the prime $p$ is 2. The reason for this can be seen from §II where we discussed the importance of involutions and their centralizers.

Up to now, only certain classes of 2-groups have been treated. These include the groups $P$ of 2-rank at most 2, cf. [21], [32], [1], and [2]; the case that $P$ is the Sylow 2-subgroup of $U_3(4)$ does not appear in the literature but since $|P|$ has the small value 64, it can be treated without difficulty.

As an example of a group $P$ of 2-rank 3, we mention the Sylow 2-subgroup of the group $G_2(3)$. The latter group plays a dominant role in Thompson's $N$-group paper [65]; for this reason it is of particular interest. Assume then that $G$ is a finite group with the Sylow 2-subgroup $P$ and that the fusion $\mathcal{F} = \mathcal{F}(G)$ is given. As is well known, it depends only on $\mathcal{F}$ whether or not $G$ has a normal subgroup of index 2; we shall assume that this is not the case. It can then be shown [18] that there are exactly two possibilities for $\mathcal{F}$; in the case of the first one, $G$ has two conjugacy classes of involutions and in the second case, there is only one such class. Moreover, in the first case, $G/O_2(G)$ is either isomorphic to the Mathieu group $M_{12}$ or to a group $W$ which is determined uniquely up to isomorphism by the conditions that $W$ is nonsoluble and nonsimple and has order 1344.

If $G$ has only one conjugacy class of involutions, $G/O_2(G)$ is isomorphic to $G_2(3)$, cf. [3511]. Actually, [35] gives a characterization of the finite simple groups $G_2(q)$, the projective symplectic group $\text{PSp}(4, q)$, and the Steinberg simple groups $D_4(q)$ where $q$ is an odd prime power.

V. Groups of characteristic 2-type. It has been observed by Daniel Gorenstein [37] that the following conditions appear to be satisfied by the simple groups $G$ of Lie type over fields of characteristic 2 with a few exceptions:

(a) The group $G$ is simple. (b) Its 2-rank is more than 2 (i.e., $G$ contains elementary abelian subgroups of order 8. (c) A Sylow 2-subgroup $S$ of $G$ does not normalize a subgroup of $G$ of odd order $k > 1$. (d) All 2-local subgroups of $G$ are 2-constrained. (e) For this reason, Gorenstein calls groups $G$ satisfying the conditions (e) groups of characteristic 2-type. He observes that a very large portion of J. G. Thompson's $N$-group papers [65] deals with such groups. In addition to the Lie groups over fields of characteristic 2, the group $G_2(3)$ and the following sporadic groups are characteristic 2-type groups: The Mathieu groups $M_{22}$, $M_{23}$, $M_{24}$; the Suzuki group of order 448,345,497,600, and the large Conway group. It seems reasonable to try to study sporadic groups which are of characteristic 2-type.
We mention the following result of Gorenstein \cite[Theorem 1]{Gorenstein1968}.

**Theorem (5A).** If $G$ is a simple group of characteristic 2-type, then $O_2(H) = \langle 1 \rangle$ for every 2-local subgroup $H$ of $G$.

We shall find it convenient to speak of characteristic 2-type groups $G$ if $G$ is simple or nonsimple and if the conditions $(*)$ (b), (c), and (d) are satisfied. The proof of Theorem (5A) yields here a slightly weaker result.

**Theorem (5A*).** If $G$ is a characteristic 2-type group and if $H = \cap_{G}(P)$ is a 2-local subgroup with $P$ a 2-group of order more than 2, then $O_2(H) = \langle 1 \rangle$.

Now an idea of David Wales and proved in final form by Ronald Solomon \cite{Solomon1980} can be applied. We state the result in a different language. In \cite{Wales1990}, groups $G$ of 2-deficiency class two were defined as groups $G$ for which there does not exist a nonprincipal 2-block of defect larger than 1. We then have the theorem.

**Theorem (5B).** If $G$ is a characteristic 2-type group, then $G$ is of 2-deficiency class 2.

On combining Theorem (5B) with \cite[(7A)]{Wales1990}, we find

**Corollary (5C).** Let $G$ be a characteristic 2-type group. If the Sylow 2-subgroup $P$ of $G$ has abelian 2-rank larger than two, there exists a bound $f(|P|)$ depending only on $|P|$ such that $|G| < f(|P|)$.

It follows that there exist only finitely many nonisomorphic characteristic 2-type groups $G$ with a Sylow 2-subgroup $P$ of given order, provided that $P$ has 2-rank at least 2. Again no proof seems to be known which does not use block theory.

It follows from \cite{Wales1990} that a finite group $G$ of even order is of 2-deficiency class two, if and only if $\mathfrak{C}_G(z)/\langle x \rangle = W$ is of 2-deficiency class 1 for every involution $z$ of $G$. Of course, $W$ has smaller order than $G$. If we assume that we know all groups $W$ of 2-deficiency class 1 and smaller order than $|G|$, we can construct all possible groups $\mathfrak{C}_G(z)$ as extensions of a group of order 2 by a known group $W$. In order to find $G$, we have to solve the problem of finding the groups in which the centralizer of an involution is isomorphic to a given group. It was already mentioned in §2 that problems of this kind have been treated by quite a number of authors.

A further reduction of a similar nature is possible. In order to find all groups $W$ of 2-deficiency class 1, we can proceed as follows. We construct all groups $V$ of 2-deficiency class 1 of smaller order than $|W|$, then construct the extensions $U$ of a cyclic group $\langle s \rangle$ of order 2 by the group $V$, and finally have to find the groups $G$ in which the centralizer of an involution is isomorphic to $U$.

VI. Examples and Remarks.\textsuperscript{3} It may be of interest to some readers if we mention some examples. We wish to show that the results discussed above can be used to answer very concrete questions.

\textsuperscript{3}In §§VI and VIII, a large number of facts are discussed very briefly. The reader may do well to read only parts of special interest to him.
(1) For certain orders, for instance for the orders 5616, 6048, and 7920, the existence of simple groups of that order was known. However, it was not known whether or not there were nonisomorphic groups of that order. Here, Theorem (3A) with suitable choice of \( p \) can be applied. This provides sufficient information to permit construction of the character matrix \( X_G \), (1.1). Finally, this yields enough information that we can prove that simple groups of the orders in question have to be isomorphic to the known groups.

(2) If the given order \( g \) contains primes with the exponent 1, similar methods can be used frequently to show that no simple group of order \( g \) exists.

(3) Burnside [24, Note N, p. 504] reports on his work leading to a determination of all simple groups of orders up to 1,000. He writes "The labour involved in such a direct examination increases very rapidly with the order, and puts a practical limit on carrying it on to considerable values of the order."

The methods discussed in (1) and (2) changed the picture. H. F. Tuan [66] was able to determine the simple groups of orders up to 10,000, Sister Elizabeth Louise Michaels [54] extended this to the upper bound 20,000 and finally, Marshall Hall, Jr. [42], [43] started to work on the construction of simple groups of orders up to 1,000,000. There were twenty-one orders for which he did not obtain results. The most interesting of the orders treated is the order 604,800, since this led Hall to the construction of the Janko-Hall group [42], see also Janko's paper [48].

(4) There are a number of aids which can be used to eliminate cases in a program of the type discussed in (3). (a) If \(|G|\) is divisible by primes \( p \) with the exact exponent 1, the results of [22] can be helpful. (b) It follows from the Corollaries (3C) and (3D) in §III that only primes \( p < |G|^{1/3} \) can divide \(|G|\) except when \( G \) is isomorphic to one of the groups \( \text{PSL}(2, p) \) or \( \text{PSL}(2, p - 1) \) in the corollaries. (c) The following results can be shown: If \(|G|\) contains \( p \) with the exact exponent \( a \), then \(|G| > p^{2a}\), if the Sylow 2-subgroup \( P \) is abelian. The same is still true, if \( P \) is nonabelian, but if \( G \) does not contain elements of order \( 2p \). For \( a > 3 \), we have \(|G| > p^{a+3}\).

The following two results are more difficult to prove. The prime 2 divides \(|G|\) at least with the exponent 6 except in cases which can be listed explicitly [34]. If \( a > 2 \), then \(|G| > p^5\) [36].

(e) It follows from Thompson's \( N \)-group paper [65] that if \(|G|\) contains only three distinct prime factors, two of the prime factors are 2 and 3 and the remaining prime factor is 5, 7, 13, or 17. In the last two cases, \( G \) is isomorphic to \( \text{PSL}(3, 3) \) or, respectively, to \( \text{PSL}(2, 17) \). If \(|G|\) has the form \(|G| = 2^a \cdot 3^b \cdot 5 \) (and if \(|G| \neq 5\)), I have shown that \( G \approx A_5 \) or \( G \approx A_{69} \), or \( G \approx \text{PSp}(3, 4) \) of order 25920 [12]. If \( g = 2^a \cdot 3^b \cdot 7 \), then \( G \approx \text{PSL}(2, 7) \) or \( G \approx \text{PSL}(2, 8) \), [68]. The order 84,672 can be removed from Hall's list [R. Brauer, J. S. Leon]; also as can be shown without much difficulty the order 43,200. Hence all simple groups of order less than 86,400 are actually known.

(4) Among the simple groups \( G \), not of prime order and of order, say, below 1,000,000, a very large percentage is of type \( \text{PSL}(2, q) \). It is therefore of interest to have a criterion that allows us to decide whether or not \( G \) is isomorphic to a group of this type. Such a criterion has been given by Hans
Zassenhaus [70]; this criterion is already used in the proof of Corollary (3C) in §III and other work of theoretical and not numerical nature. Zassenhaus' investigations led him to the introduction of the concept of near fields and the class of groups now called Zassenhaus groups.

(5) A systematic study of Zassenhaus groups (as well as of Frobenius groups) was made by Noboru Ito [46]. The last part of Ito's book also deals with the Suzuki groups Sz(q) which the reader will encounter below in this section.

(6) Some of the first characterizations of sporadic groups G by their order was given by R. G. Stanton [61]. Stanton treated the Mathieu groups M_{12} and M_{24}. Application of Theorem (3A) and of [61] allows Stanton to construct the character matrix (1.1). This again yields enough information to determine G up to isomorphism. Similar methods were used by David Parrott and S. K. Wong to characterize M_{22} and the Higman Sims group, [56], [57].

(7) In 1960, Michio Suzuki constructed an infinite sequence Sz(2^{2n+1}) of order

\[2^{4n+2}(2^{2n+1} + 2^n + 1)(2^{2n+1} - 2^n + 1)(2^{2n+1} - 1)\quad (n \geq 1)\]

[62]. These are now usually called the Suzuki groups, see above in (5). At the time of their discovery, it was believed that they were sporadic groups which later was shown to be false.

(8) Block theoretic methods allowed me to show that Sz(8) was the only simple group of its order. Later Michael Collins [26] generalized this result by proving that if a simple group G has a Sylow 2-subgroup isomorphic to that of Sz(q), then G is itself isomorphic to Sz(q). His proof uses some of the most sophisticated tools developed by Bender, Goldschmidt, Gorenstein, and Walter. Collins [27] also proved a similar result for the unitary groups U_3(q) with even q > 4.

(9) As we mentioned in (7), it was believed in 1960 that the Suzuki groups Sz(q) were sporadic groups and, in particular, that there were infinitely many sporadic groups. This belief was already shattered in 1961 when Rimhak Ree and, independently, Robert Steinberg noted that the groups Sz(q) were twisted groups of Lie type B_2 that had been overlooked! As a consequence, we had to change our opinion after only one year. It is again conceivable that there are only finitely many (nonisomorphic) sporadic groups. I have already mentioned that it is still anybody's guess now fifteen years later.

(10) Rimhak Ree's work mentioned in (9) was the starting point for his discovery that two more families of simple groups of Lie type have been overlooked. One of them, of type G_2, [59] is of special interest to us. The groups in it resemble in some ways the Suzuki groups with the prime 2 replaced by the prime 3. Ree also made a statement which was of special interest to me personally. He mentioned that the Sylow 2-groups of all the groups in his family were of order 8. It was then clear that Sylow 2-groups of the new simple Ree groups had to be all elementary abelian of order 8. Hence no characterization of the groups by their Sylow 2-subgroup S and the fusion in S was possible.
(11) At that time, H. N. Ward started to work on his Ph.D. Thesis at Harvard under my direction. I suggested to him the question of §11 for the Ree groups: Given a simple group $G$ and an involution $z$ in $G$ such that $G_G(z)$ is isomorphic to the analogous group with $G$ replaced by one of the simple Ree groups. What can you say about $G$? Subsequently, Ward [72] succeeded in obtaining the character table of $G$. However, his attempts to prove the isomorphism of $G$ with the Ree group in question failed. John Thompson who had been a member of the Harvard Mathematics Department in 1962 became interested in the question and made considerable progress [64]. However, it is still unsolved. Possibly, there exist infinitely many sporadic groups of Ree type and, possibly, none at all.

Our discussion of examples in 1–6 has ended in 7–11 with a report on some of the strangest chapters of mathematical history in modern times.

VII. A digression. We said at the beginning that most group theorists felt that it would only be a matter of time until the simple groups would be classified. We shall now take a closer look at this statement.

Clearly, a requirement for a classification of the simple groups is that we can arrange a set of representatives for the isomorphism classes of simple groups in a sequence

$$G_1, G_2, G_3, \ldots$$

indexed by the integers, and that we know the multiplication table of $G_n$ for each $n$. We should also know to which of the four types of simple groups in §1 the group $G_n$ belongs. We may assume that the groups $G_n$ in (7.1) are arranged such that $|G_n| < |G_n'|$ for $n < n'$.

There is no difficulty about the solvable simple groups; they are the simple groups of prime order. A necessary condition that $G_n$ be isomorphic to the alternating group $A_n$ is that $|G_n| = n!$ However, this condition is not sufficient. For instance, there exists a simple group $G_n$ of order $\frac{1}{2} 8!$ which is not isomorphic to $A_8$.

Let $M$ be a given positive integer. Given enough money, space, and time, there would be no theoretical difficulty about building a computer which could construct the part $\{G_1, G_2, \ldots \}$ of (7.1) which consists of the groups $G_n$ with $|G_n| < M$.

It is possible that, for a suitable choice of $M$, we are finished at this point. This would of course require that there exist only finitely many nonisomorphic sporadic groups, all of order at most equal to $M$. In addition, we would have to have a proof that there do not exist sporadic groups of order larger than $M$.

If there exist sporadic groups of order larger than $M$, possibly the situation may be remedied by replacing $M$ by a larger value.

So far, it has not been proved that there are only finitely many nonisomorphic sporadic groups. Let us consider the case that there exist infinitely many nonisomorphic sporadic groups. We speak here of a system of classification $\mathcal{S}$ for the sporadic groups, if the set of sporadic groups in (7.1) is written as a disjoint union
of finitely many or infinitely many subsets \( C_j \). In order that this classification be of any value, we would require that the \( G_n \) in the same \( C_j \) share some important group theoretical properties.

Depending on the exact circumstances, this might be a satisfactory answer to the problem of classifying the sporadic groups. However, we are far from knowing that such an answer exists.

**VIII. Additional topics.** We discuss briefly a number of topics where block theory can be used.

1. We define a system of classification \( \mathcal{S} \) (§VII) as follows. The class \( C_j \) consists of the sporadic groups \( G_n \) whose order is divisible by exactly \( j \) distinct prime numbers.

**CONJECTURE (8A).** If the system \( \mathcal{S} \) is used, the class \( C_3 \) is empty.

We can write the whole set (7.1) as a union of disjoint sets \( C_j^* \) where \( C_j^* \) is the set of groups \( G_n \) whose order is divisible by exactly \( j \) distinct primes, \( j = 1, 2, \ldots \). Then \( C_5^* \) consists of the solvable simple groups. A well-known theorem of Burnside shows that \( C_5^* \) is empty.

**CONJECTURE (8A*).** The set \( C_5^* \) consists of

\[
A_5, A_6, U_4(2), \text{ PSL}(2, 7), \text{ PSL}(2, 8), U_3(3), \text{ PSL}(3, 3), \text{ PSL}(2, 17).
\]  

(8.1)

Clearly, (8A*) implies (8A).

No proof of (8A*) is known. Using block theory, at least some special results covered by the conjecture (8A*) can be proved. For instance, if \( G \) is simple of an order \( |G| = 5 \cdot 3^a \cdot 2^b \) with \( a > 0, b > 0 \), then \( G \) is isomorphic to one of the first three groups in (8.1), cf. [12]. If \( G \) is simple and \( |G| = 7 \cdot 3^a \cdot 2^b \) with \( a > 0, b > 0 \), then \( G \) is isomorphic to one of the next three groups in (8.1), [71].

If we use more recent results whose proof depends on much deeper methods, we can say more. It follows from Thompson's \( N \)-group paper [65] that the three primes dividing \( |G| \) belong to one of the set

\[
\{2, 3, 5\}, \{2, 3, 7\}, \{2, 3, 13\}, \{2, 3, 17\}.
\]

In the last two cases, it was proved recently by Kenneth Klinger [49] and by Geoffrey Mason [53] that the groups in question are isomorphic to \( \text{PSL}(3, 3) \) and \( \text{PSL}(2, 17) \) respectively. It is also known that if \( G \) belongs to \( C_5^* \) and if some Sylow subgroup of \( G \) is cyclic, then \( G \) is isomorphic to a group in (8.1).

The class \( C_5 \) is no longer empty (see Appendix II). One may conjecture that all classes \( C_j^* \) are finite. This would of course be the case if there are only finitely many nonisomorphic sporadic groups, but it might still be true in the opposite case.

2. **Application to linear groups.** We consider here finite linear groups of a given dimension \( n \), i.e., finite subgroups of \( \text{GL}(n, \mathbb{C}) \). We say that such a group \( G \) is quasi-primitive, if \( G \) is irreducible and if, for every normal subgroup \( H \) of \( G \), any two irreducible constituents of \( H \) are similar. The following result is essentially due to H. F. Blichfeldt [4].

\[
C_1 \cup C_2 \cup \cdots
\]  

(7.2)
THEOREM (8B). If $G$ is a finite, quasi-primitive linear group of degree $n$, then for every prime number $p < n + 1$, we have
\[ |G_p| \leq |z(G)| p^{n-1}(n!)_p. \tag{8.2} \]
Moreover, (cf. [6II] and [31])
\[ |G: \mathcal{L}(G)| < n! (2n + 1)6^{(n-1)\pi(n+1)}. \tag{8.3} \]
Here, for $\alpha \in \mathbb{Z}$ and $\alpha \neq 0$, $(\alpha)_p$ is the highest power of $p$ dividing $\alpha$ and $\pi(\cdots)$ is the prime number function.

The Theorem (8B) is a refinement of a classical theorem of C. Jordan. In particular, it follows that there exist only a finite number of possibilities for the projective group $\overline{G} = G/\mathcal{L}(G)$ (apart from equivalence).

For $n < 4$, the groups $\overline{G}$ were determined explicitly by Felix Klein, C. Jordan, Valentiner, and H. F. Blichfeldt, cf. [4], but no further progress was made after that for about fifty years. By the use of block theory it became possible to treat the cases $n = 5$ [11], $n = 6$ [52], $n = 7$ [70], and most recently, $n = 8$ [45] and [32]. Results of this kind are important for the theory of algebraic equations of degree $n - 1$.

The results of [13] are a first step in the direction of finding the order of magnitude of the best possible upper bounds in Jordan's theorem.

Finally, in [17] an analogue of Jordan's theorem for fields of characteristic different from 0 is proved.

3. There are cases in which block theory can be used to obtain new proofs of important older theorems. In [63], John Thompson obtained a more direct approach to the celebrated "Theorem B" of Graham Higman and Philip Hall which plays an important role in the "odd order paper" [32] of Feit and Thompson.

A similar case is a proof of J. L. Alperin [1, §4] of a theorem of George Glauberman.

IX. An epilogue: Work not yet done. Apart from the many questions in the preceding pages, there are many open problems. Since there are now so many mathematicians working in the theory of finite groups, perhaps some of them may try to solve them.

Most of the recent work on simple groups uses purely combinatorial arguments. A number of new concepts have been introduced which are certainly highly significant. It will be of interest to see, if any of them play a role in problems of the representation theory of finite groups.

There are also questions of a more technical nature. The character theory of groups $G$ with a given Sylow 2-subgroup $S$ has been developed for the cases where $S$ has abelian 2-rank at most two (cf. §IV). There is no reason why the case of larger 2-rank of $S$ could not be treated. If this can be done, it may become possible to prove the Schreier conjecture for simple groups $G$ whose Sylow 2-subgroup is isomorphic to one of the 2-groups $S$ for which results are available.
Even if the classification problem for simple groups can be solved in the most satisfactory form, we still do not know all about finite groups that we want to know, e.g., about the structure of the modular representations, about the invariants of finite linear groups, and so on.

I, for one, hope that finite group theory will keep mathematicians busy for a long time to come.

Appendix I

REMARKS ON THE THEORY OF BLOCKS

If $G$ is a finite group of order $g$ and if $K$ is a field, we can embed $G$ in an associative algebra $K[G]$ over the field $K$ such that if $\sigma \in G$ corresponds to $k(\sigma) \in K[G]$, the elements $\{k(\sigma)\}$ form a $K$-basis of $K[G]$ and that the mapping $\sigma \to k(\sigma)$ is a (nonzero) group isomorphism. The algebra $K[G]$ is the group algebra of $G$ over $K$. In working with $K[G]$, we assume tacitly that the mapping $k$ is given.

The investigation of $K[G]$ in the case of an algebraically closed field $K$ of characteristic 0 is equivalent with Frobenius' theory of group representations; it does not matter, if we choose $K$ simply as the complex field $\mathbb{C}$. In particular, Frobenius defined the irreducible characters of $G$ and obtained their basic properties. It should be emphasized that the characters describe 'purely group-theoretical properties' of $G$. If a certain theorem of group theory is proved by means of characters, it may be of technical interest to find a proof which is 'free of characters', but it is not of theoretical interest.

The case of a group algebra $K[G]$ over a field of prime characteristic $p \neq 0$ leads to the study of the $p$-modular representations of $G$. We refer here to the books [B], [E], [G], and [J]. It is no restriction for our purposes to assume that $K$ be algebraically closed.

We said in §IV that what we call "block theory" is to serve as a substitute for the results of [51] which were exploited in §III.

The basic references for block theory as used here are my papers [8], [9], [10], J. A. Green's paper [39], [40], [41], and Walter Feit's lecture notes [J] which contain a great deal of new material.

In addition, we may mention [14] and, for a different point of view [23]. We restrict ourselves to publications which deal with results applied in these notes.

The very fact that block theory is a substitute for an unknown theory means that there are many open problems. Some interesting contributions to such questions were given recently in [50] and [55].

Appendix II

SPORADIC GROUPS

In Part I, we give the orders of the sporadic groups listed in [J]. Part II deals with the recent discoveries. If two names are given for one of the sporadic groups, the first is that of the group theorist who suggested the existence of the group and the second that of the person who checked the existence, usually on a computer.
### Part I

<table>
<thead>
<tr>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_{11}$</td>
</tr>
<tr>
<td>$M_{12}$</td>
</tr>
<tr>
<td>$M_{22}$</td>
</tr>
<tr>
<td>$M_{23}$</td>
</tr>
<tr>
<td>$M_{24}$</td>
</tr>
</tbody>
</table>

The five Mathieu groups

<table>
<thead>
<tr>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>$J$</td>
</tr>
</tbody>
</table>

The Janko group

<table>
<thead>
<tr>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>$J_1$</td>
</tr>
</tbody>
</table>

The Janko-Hall group

<table>
<thead>
<tr>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>$J_2$</td>
</tr>
</tbody>
</table>

The Janko-Higman and McKay group

<table>
<thead>
<tr>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Held-Higman and McKay group</td>
</tr>
<tr>
<td>The Higman-Sims group</td>
</tr>
<tr>
<td>The McLaughlin group</td>
</tr>
<tr>
<td>The Suzuki sporadic group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>The three Conway groups</td>
</tr>
<tr>
<td>The three Fischer groups</td>
</tr>
<tr>
<td>The Lyons-Sims group</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>The O'Nan-Sims group</td>
</tr>
<tr>
<td>The Rudvalis-Conway and Wales group</td>
</tr>
<tr>
<td>The “Baby Monster”</td>
</tr>
<tr>
<td>The Thompson group</td>
</tr>
<tr>
<td>The Harada-F. S. Norton and P. E. Smith group</td>
</tr>
<tr>
<td>The “Monster”</td>
</tr>
<tr>
<td>The Janko “group” $J_4$</td>
</tr>
</tbody>
</table>

**Note.** The actual existence of the “Monster” and of $J_4$ has not yet been established.

### REFERENCES

#### I. Books


RICHARD BRAUER

II. Survey articles


III. Conferences


IV. Other publications


6. ______, On permutation groups of prime degree and related groups, Ann. of Math. 44 (1943), 57–79.


27. The characterization of the unitary groups $U_n(2^k)$ by their Sylow 2-subgroups, Bull. London Math. Soc. 4 (1972), 49-53.


32. On finite linear groups in dimension at most $10$, in [S] (1976), 397-407.

33. Walter Feit and John G. Thompson, Solvability of groups of odd order, Pacific J. Math. 13 (1963), 775-1029.

34. Paul Fong, Sylow 2-subgroups of small order (unpublished).


41. ______, A transfer theorem for modular representations, J. Algebra 1 (1964), 73-84.


43. ______, Simple groups of order less than one million, J. Algebra 20 (1972), 98-102.


68. ________, *Simple groups of order \(7 \cdot 3^a \cdot 2^b\)*, J. Algebra 16 (1970), 575–595.