Introduction

This book presents an almost self-contained introduction to the theory of *abstract* finite (non-abelian) simple groups, which together with the cyclic groups of prime order are the building blocks of all finite groups. The theory developed here has concrete applications. In particular, it yields the theoretical and algorithmic background for uniform existence and uniform uniqueness proofs of the (known) sporadic simple groups. This is demonstrated by several examples studied in detail in the second half of the book. However, the theoretical results and algorithms presented in the first seven chapters hold in general. They are not restricted to sporadic groups at all.

The theory of abstract finite simple groups presented here is inspired by the Brauer–Fowler Theorem. It asserts that there are only finitely many simple groups G which possess an involution $z \neq 1$ such that its centralizer $C_G(z)$ is isomorphic to a given group H of even order. This is an important observation, because there are several series of infinitely many simple groups where all the members in such a series have isomorphic Sylow 2-subgroups. In particular, there are infinitely many simple groups G having a Klein four group as a Sylow 2-subgroup, see Theorem 1.6.2. Hence a simple group G is not uniquely determined by the structure of its Sylow 2-subgroups. It is therefore a necessary and natural hypothesis of the Brauer–Fowler Theorem to assume that the structure of the centralizer $H = C_G(z)$ of some involution z is known.

In fact, when R. Brauer spoke about the Brauer–Fowler Theorem at the International Congress in Amsterdam in 1954, he assumed that G was a group of even order. At that time the celebrated Theorem of Feit and Thompson [38] on the solvability of the finite groups of odd order was not known. It implies that each finite non-abelian simple group has even order. Therefore it has elements of order 2. Such an element is also called an involution. The Feit–Thompson Theorem cannot be proved here. It is one of four important cited results a proof of which cannot be found in a standard textbook. The best known proof of the Feit–Thompson Theorem is given in the two recent books by Bender and Glauberman [10] and Peterfalvi [129]. Whenever a proof of a quoted result cannot be given, proper references to the literature are provided.

The reader is assumed to know the content of a first-year graduate course in algebra. For the study of explicit examples some practical experience with the computer algebra systems GAP [40] and MAGMA [12] and [22] will be helpful. Many fundamental algorithms in computational group and representation theory are described in the recent handbook of computational group theory [76]. Therefore it is not necessary to give here a summary of all the elementary procedures and commands of these software packages which have to be applied to perform concrete calculations in a finite group G of which a faithful permutation representation is given.

The book contains 12 chapters each of which has an introduction summarizing its contents. The theory of abstract finite simple groups is built on the intimate relations between general group theory, ordinary character theory, modular representation theory and algorithmic algebra.

Chapter 1 provides the basic definitions and results about presentations of finite groups in terms of generators and relations. In several subsequent chapters it will be a demanding task to find a finite presentation of a simple group G for which only such a presentation of the centralizer $C_G(z)$ of a suitable involution z of G is known. For this purpose several classical results on p-groups, especially 2-groups, fusion and transfer are proved in this chapter. In particular, a self-contained proof of Ph. Hall's Theorem is given which characterizes all 2-groups having only cyclic characteristic subgroups.

In Chapter 2, all the definitions and results of ordinary representation theory of finite groups are presented which will be used later on. The main purpose of this chapter is to provide general results which help to classify all the conjugacy classes of a finite group G in terms of fairly short words in the elements x_i of a given finite set $X = \{x_1, x_2, \dots, x_n\}$ of generators of G, construct all its irreducible ordinary characters χ and determine their values $\chi(g)$ for all $g \in G$. Such a character table of G is called a *concrete character table*.

One of the main results proved in Chapter 2 is R. Brauer's characterization of characters of finite groups. It finds many applications later on. It is not only used for the determination of splitting fields and concrete character tables of finite groups, but also for the solution of difficult group theoretical questions.

Brauer began his lecture at the International Congress in 1954 as follows: “The theory of groups of finite order has been rather in a state of stagnation in recent years. If I present here some investigations on groups of finite order, it is with the hope of raising new interest in the field.” He had good reasons for that optimistic statement, because at that time he had already published or announced most of his major theorems on p-blocks of finite groups G, where p is a fixed prime divisor of the order $|G|$ of G. They are proved in Chapter 3. The deepest result is his second main theorem on p-blocks. It yields an explicit character formula $\chi(g)$ for all irreducible characters χ of G belonging to a p-block B of G with defect group D and all elements g of G whose p-part $g_p \neq 1$ is conjugate to some non-trivial element of D in G. Its proof given here employs J. A. Green's theory of indecomposable modules of group algebras. It is also presented in this chapter. Brauer's second main theorem and Green's correspondence theorem are then applied in the proof of Brauer's famous character formulas for irreducible characters belonging to p-blocks B of G with cyclic defect groups D of prime order $|D| = p$.

Cambridge University Press
978-0-521-86625-5 - Theory of Finite Simple Groups
Gerhard O. Michler
Excerpt
More information

The most important invariant of a finite group G is its order $|G|$. In Chapter 4 the group order formulas of M. Suzuki, J. G. Thompson, G. Frobenius and R. Brauer are proved by means of representation theoretic results dealt with in Chapters 2 and 3. For groups G having only one conjugacy class of involutions these formulas do not suffice. Therefore the author proves a new one in this chapter. It has been used to determine the orders of all (known) sporadic simple groups having a unique conjugacy class of involutions. The reader will find examples of such applications in Chapters 9 and 12.

Chapter 4 also contains a new proof for the famous non-simplicity criterion of Brauer and Suzuki. Together with Brauer's theorems on 2-blocks it is the main tool for the proof of Glauberman's Z^*-Theorem. These results then pave the way for an elementary proof of the author's structure theorem of abstract simple groups: If S is a Sylow 2-subgroup of such a group G, then exactly one of the following statements holds:

(a) S is dihedral.

(b) S is semi-dihedral.

(c) G has a strongly embedded subgroup.

(d) S has a non-cyclic elementary abelian characteristic subgroup A, and $E = N_G(A)$ has finitely many conjugacy classes z_i^E of involutions which do not fuse in G such that G is generated by E and the centralizers $C_G(z_i)$.

The simple groups G satisfying condition (a), (b) or (c) have been classified long ago by Gorenstein and Walter; Alperin, Brauer and Gorenstein; or Bender and Suzuki, respectively. These important theorems are stated in Chapter 1 without proof, but with proper references to the existing literature. They have not been used in the proof of the above-mentioned structure theorem, but are quoted in the last three chapters, which deal with some important examples.

A main task of the representation theory of finite groups is to provide theoretical results and practical methods for the calculation of a concrete character table of a finite group G of which a finite presentation in terms of generators and relations is known. In Chapter 5 several deterministic algorithms are described that help to find representatives of all conjugacy classes and all character values of all irreducible characters of a finite permutation group. The basic tool for that purpose is the recent character formula of M. Weller and the author. It is proved in Chapter 5.

In Chapter 6 these methods are extended to calculate concrete character tables of finitely generated matrix groups $G \leq \mathrm{GL}_n(F)$ over finite fields F. This is done by transforming such a group G into a permutation group. Then the algorithms of Chapter 5 can be applied.

In general finite simple groups are large objects. Therefore explicit examples often cannot be studied without the use of computer algebra systems like

MAGMA [12] and GAP [40]. In modern mathematics these systems play a similar role to that of pocket calculators many years ago. Therefore the deterministic algorithms presented in Chapters 5 and 6 are set up in such a way that the applications of the algebra software packages will produce the same results whenever they start from the same faithful permutation representation of a finitely presented group G. It is uniquely determined by a given set of generators of its stabilizer. In all the examples dealt with in this book the generators of such a stabilizer are documented as short words in the given generators of G.

The remainder of the book is devoted to the study of the simple groups G satisfying condition (d) of the structure theorem mentioned above.

An involution z of a finite group G is called *2-central* if z belongs to the center $Z(S)$ of some Sylow 2-subgroup S of G. Let H be a given finite group with a center $Z(H)$ of even order. Any finite simple group G having a 2-central involution z with centralizer $C_G(z) \cong H$ is said to be of *H-type*. Since all known proofs of the Brauer–Fowler Theorem are not constructive, it is a natural question to ask whether there is a practical algorithm which constructs all finite simple groups of H-type from a given finite presentation of the group H. Such an algorithm has recently been published by the author. It is described in Algorithm 7.4.8 of Chapter 7.

Compared to the unknown simple target groups G the given centralizer H is reasonably small. Therefore one constructs from a given presentation of H a faithful transitive permutation representation of H. Applying standard commands of the computer algebra system MAGMA one can determine a Sylow 2-subgroup S and a maximal non-cyclic elementary abelian characteristic subgroup A of S. Then using Kratzer's algorithms described in Chapter 5 one can find representatives of all conjugacy classes of H as short words in the generators of H. MAGMA also provides generators of the subgroups $C_G(A) = C_H(A)$ and $D = N_H(A)$. With this information one has to study theoretically the possible fusion of the H-conjugacy classes meeting A in the unknown target groups G. Here Thompson's Transfer Lemma and Glauberman's Z^*-Theorem, proved in Chapters 1 and 4, respectively, are helpful to decide whether $|N_G(A) : N_H(A)| \neq 1$. If so, then Algorithm 7.4.8 can be applied. It determines the precise group structure of $E = N_G(A)$ and often a faithful irreducible p-modular representation κ of each target group G. Hence G is isomorphic to a subgroup $\kappa(G)$ of $\mathrm{GL}_n(F)$, where F is a finite field of characteristic $p > 0$ not dividing $|D|$. Furthermore, Algorithm 7.4.8 provides methods for calculating the concrete character tables of the simple target groups.

In general, a finite simple group G of H-type is not uniquely determined by H. If G is a finite simple group of H-type, then any finite simple group X of H-type which is not isomorphic to G is called a proper *H-satellite* of G. The finite simple groups with proper simple satellites are dealt with in Chapter 8. M. Suzuki's survey article [139] lists the following examples:

G	H	Simple satellites of G	authors
M_{11}	$2.S_4$	$PSL_3(3) = L_3(3)$	R. Brauer
M_{24}	$2^{1+6} : L_3(2)$	$L_5(2), He$	Held
J_2	$2^{1+4} : A_5$	J_3	Janko
A_6	D_8	$L_2(7) \cong L_3(2)$	M. Suzuki
A_8	$2^3 : S_4$	A_9	Held
A_{12}	$2^5 : S_6$	$A_{13}, Sp_6(2)$	Yamaki
A_{4k}	$2^{2k-1} : S_{2k}$	$A_{4k+1}, k = 4, 5, \dots$	Kondo

The existing literature does not contain a proof that this list shows all the known simple groups having a proper simple satellite.

In the first three sections of Chapter 8 the (sporadic) simple Mathieu groups M_{11}, M_{12}, M_{22}, M_{23}, M_{24} are dealt with. From J. A. Todd's abstract definitions [143] of these groups, presentations of the centralizers $H_i = C_{M_i}(z_i)$ of 2-central involutions z_i of the simple groups M_i, $i \in \{11, 12, 22, 23, 24\}$ are derived. The satellites $L_5(2)$ and Held's simple sporadic group He are constructed from H_{24} by means of Algorithm 7.4.8. Similar proofs are given for Janko's sporadic groups J_2 and J_3. Finally, Held's and Yamaki's Theorems are proved which classify the simple satellites of the alternating groups A_{4k} for $k = 2, 3$. Kondo's Theorem [93] classifying the simple satellites of A_{4k} for all $k > 3$ is stated without proof because of a lack of space.

A finite simple group G is *uniquely determined* by the centralizer H of a 2-central involution $z \in G$, if G does not have any non-isomorphic simple H-satellites. The author's uniqueness criterion is proved in the last section of Chapter 7. It is practical because it builds on the fact that one simple group $\mathfrak{G}$ of H-type has already been constructed. It also requires to show theoretically that all finite simple groups G of H-type have (a) the same order $|G| = |\mathfrak{G}|$, and (b) a faithful irreducible representation of minimal degree n over some finite field of odd characteristic q.

Hypothesis (a) can be satisfied by verifying the sufficient conditions of the group order formulas presented in Chapter 4. One way to check hypothesis (b) is to show that all simple groups G of H-type have the same character table and a q-block B of defect 1 which has a q-modular irreducible representation of degree n. For an example of such a solution see Chapter 9. Another way to verify hypothesis (b) is to find a complete classification of all conjugacy classes of elements x of prime order of any finite simple group G of H-type and to determine the structure of their normalizers $N_G(x) = N_G(\langle x \rangle)$, where $\langle x \rangle$ denotes the cyclic subgroup of G generated by x. If the conditions of Brauer's characterization of characters proved in Chapter 2 can be satisfied for a suitable n-dimensional complex valued class function χ, then each of these groups G has an irreducible ordinary character of degree $\chi(1) = n$. Finally, one has to show that χ remains irreducible after reduction modulo the prime q. In Chapter 12 we apply these methods in a uniqueness proof for Thompson's sporadic simple group.

In Chapter 7 we also describe deterministic methods that help to find a system of representatives of the elements y of prime order of all the unknown simple target groups G of H-type and the structure of their normalizers $N_G(y)$. Such a normalizer often contains some composition factors Y which are simple groups. They have to be recognized. If the Sylow 2-subgroups of Y are dihedral, semi-dihedral or if Y contains a strongly embedded subgroup then Y is a known simple group characterized by the theorems of Gorenstein–Walter, Alperin–Brauer–Gorenstein or Bender–Suzuki mentioned before. In all other cases one has to find a presentation of the centralizer $C_Y(y)$ of some 2-central involution y of Y. Then applying Algorithm 7.4.8 one may be able to construct Y from $C_Y(y)$. After the completion of this existence proof one has either to know or to show that Y is uniquely determined by the centralizer $C_Y(y)$ of y.

In the last four chapters of this book we demonstrate that the group order formulas, character formulas, the structure theorem, the algorithms and the uniqueness criterion proved and developed in the first seven chapters are practical. This is done by presenting uniform existence and uniqueness proofs for Janko's smallest sporadic simple group J_1, the Higman–Sims group HS, the Harada group Ha and the Thompson group Th. Each of those four chapters has an introduction where the reader will also find some information about the discovery of these groups and the relevant literature. Whereas in the first three cases, J_1, HS and Ha, the details of the existence and uniqueness proofs are documented on paper, this is not possible for Th. The reader will find the documentation of its four generating matrices, its smallest faithful permutation representation (of degree 143 127 000) and several other technical data in the attached DVD at the back of this book. There one will also find M. Weller's and H. Gollan's standalone programs for calculating with large permutation matrices.

The results of the last chapter are due to M. Weller, A. Previtali and the author. Their recent joint paper [148] solved the long standing open problem on the uniqueness of the simple group Th originally discovered by J. G. Thompson [141].

In the literature the reader will find several characterizations of finite simple groups by centralizers H of involutions. In most cases the authors describe the structure of H by means of its composition factors and some additional technical conditions. However, there are several examples where such a description of H is not sufficient for a uniqueness proof. Janko [82] showed that there are two non-isomorphic extensions H of the elementary abelian group of order 16 by the symmetric group S_4 which can be realized as the 2-central involution centralizers of the alternating group A_{10} and the Mathieu group M_{22}, respectively. In order to avoid such ambiguities, in all examples dealt with in this book the given centralizer $H = C_G(z)$ of the particular class of simple groups G of H-type is well defined by an explicit system of generators and relations. Whenever it can be proved that all simple groups G of H-type are isomorphic, then this system of generators and defining relations of H yields an abstract definition of the simple group G itself.

CAMBRIDGE

Cambridge University Press
978-0-521-86625-5 - Theory of Finite Simple Groups
Gerhard O. Michler
Excerpt
More information

1

Prerequisites from group theory

The reader is assumed to be familiar with the basic concepts and results on finite groups like Sylow's Theorems and the Theorem of Jordan-Hölder. The standard textbooks on group theory by B. Huppert [77] and M. Suzuki [135] treat these subjects in their first chapter and first two chapters, respectively.

In this chapter we give an introduction to that part of finite group theory which is needed for the study of the structure of abstract finite simple groups and their ordinary and modular representations. Most of these results are easy to prove. Therefore we do not hesitate to present proofs whenever possible. This will help the reader later on to understand the intimate relations between group theory and representation theory.

In Section 1.1 we restate some basic definitions, notations and results about finitely presented groups. They will be used throughout the book.

Since finite simple groups are generated by involutions we begin their theory by classifying all non-cyclic 2-groups S which have only one involution. The classical theorem proved in Section 1.2 states that such a 2-group S is a generalized quaternion group. This result is needed for the proof of Ph. Hall's Theorem given in Section 1.3. Hall's Theorem classifies all 2-groups S which do not have any non-cyclic abelian characteristic subgroups. It will be applied in Chapter 4 where the author's structure theorem of finite simple groups is proved. The statement and proof of Hall's Theorem require the introduction of the dihedral, semi-dihedral and extra-special 2-groups and the study of their properties. For that purpose we have to state some results about general p-groups.

Suppose that the given group H is isomorphic to the centralizer $C_G(z)$ of a 2-central involution z of some unknown simple group G. In order to find representatives for the conjugacy classes of elements of even order in G one has to study the fusion of the conjugacy classes of the involutions of H in all possible target groups G. For that purpose we prove in Section 1.4 the classical results on fusion, transfer and existence of complements. In particular, D. G. Higman's Focal Subgroup Theorem, the Schur–Zassenhaus Theorem, Gaschütz Theorem and Burnside's Transfer Theorem are dealt with in detail.

It is a hard group theoretical problem to determine the structure of the centralizers $C_G(y)$ of the elements y of prime order of an unknown target group G. By hypothesis only the centralizer $H = C_G(z)$ of the 2-central involution z of G is known. Thus we have only information about the centralizers $C_H(y)$ of the elements y of prime order in H. In Section 1.5 we study actions of solvable groups A on finite groups Q of coprime orders $|A|$ and $|Q|$. As an application we obtain a classical result which will help to determine the largest normal subgroup $O(C_G(y))$ of odd order in the centralizer $C_G(y)$. This study will be continued in Chapter 4 where the Brauer–Wielandt Theorem will be proved.

Unfortunately, the classification theorems on finite simple groups with a dihedral or semi-dihedral Sylow 2-subgroup cannot be proved in the frame of this book. In view of their importance for the statement of the structure theorem of finite simple groups they are stated in Section 1.6. They also find important applications in the study of the examples dealt with in the last three chapters of this book.

Later on we also need the Bender–Suzuki Theorem classifying the simple groups with a strongly embedded subgroup. This work is explained in the last section of this chapter.

Whenever a complete proof of a result cannot be given, references to the literature are provided.

1.1 Presentations of groups

In this section we collect some basic definitions and results about presentations of abstract groups G. They will be used throughout the text of the book without further reference.

Definition 1.1.1 Let $X = \{g_1, g_2, \dots, g_m\}$ be a set of m elements g_i of the group G. Then G is *generated by* X if every element $g \in G$ is expressible as a finite product of their positive and negative powers $g_i^{a_i}$, where a_i is an integer.

When a finite product $u_1u_2\dots u_n$ of elements $u_i \in X$ or $u_i^{-1} \in X^{-1} = \{g_1^{-1}, g_2^{-1}, \dots, g_m^{-1}\}$ is equal to the identity element 1 of G, then the expression $u_1u_2\dots u_n = 1$ is called a *relation* of the generators $g_i \in X$ of G.

In order to simplify the notation, one sets $r = u_1u_2\dots u_n$, and one calls $r = 1$ a relation.

A set $\mathcal{R}$ of relations $r_1, r_2, \dots, r_k$ satisfied by the generators $g_i \in X$ of G is called a *set of defining relations* of G if every relation r of the generators $g_i \in X$ is an algebraic consequence of the relations $r_1, r_2, \dots, r_k \in \mathcal{R}$. The pair $\langle X; \mathcal{R}\rangle$ is called a presentation of the group G.

Since X is a finite set, the group G is called *finitely generated*. If it also has a finite set $\mathcal{R}$ of defining relations then G is called a *finitely presented group*.

Definition 1.1.2 Let X be a finite set with n elements. A group F is called *free on* X, if the following two conditions are satisfied:

(a) There is a map $\alpha : X \to F$ from X into F.

(b) For any map $\beta : X \to G$ from X into an arbitrary group G, there exists a unique group homomorphism $\gamma : F \to G$ from F into G such that the following diagram commutes

$$\begin{tikzcd}
X \arrow[rr, "\alpha"] \arrow[dr, "\beta"'] & & F \arrow[dl, "\exists!\gamma"] \\
& G &
\end{tikzcd}$$

The group F is called a *free group of rank n*.

Definition 1.1.3 Let F be a free group generated by the finite set $X = \{x_1, x_2, \dots, x_n\}$. A presentation $g = y_1 y_2 \dots y_m$ of an element $g \in F$ as a product of some generators $y_j \in X$ is called a *standard factorization* if no two adjacent factors y_j and y_{j+1} of g are inverses of each other.

Remark 1.1.4 Each element of a finitely generated free group F has a uniquely determined standard factorization, and the number m of its factors y_j in the given set X of generators of F is called the *length* $l(g)$ of g.

Theorem 1.1.5 *For any set X with n elements there is a free group of rank n. It is uniquely determined by n up to isomorphism.*

Proof. See [135], its p. 166.

Theorem 1.1.6 *Let X be a finite set of n generators of the group G. Let $\mathcal{R}$ be a set of relations $r_i = 1$ in the generators of X. Let F be the free group on X with the canonical embedding $\alpha : X \to F$. Let $i : X \to G$ be the inclusion of X in G. Then the following assertions hold:*

(a) *There exists a unique epimorphism $\gamma : F \to G$ such that the following diagram commutes:*

$$\begin{tikzcd}
X \arrow[rr, "\alpha"] \arrow[dr, "i"'] & & F \arrow[dl, "\exists!\gamma"] \\
& G &
\end{tikzcd}$$

(b) *If $K = \mathrm{Ker}(\gamma)$, then $\mathcal{R}$ is a defining set of relations for G if and only if K is the intersection of all normal subgroups N of F containing the set $\alpha\mathcal{R} = \{\alpha r_k \mid r_k \in \mathcal{R}\}$.*

Proof. See [135], its p. 171.

Definition 1.1.7 Let U be a subgroup of the group G. A set T of representatives $y \in G$ of the right cosets Uy of U in G is called a (right)*transversal*.