Introduction

This is the second and last volume of the author's introduction to the representation theoretic and algorithmic theory of *abstract* finite simple groups. In particular, it yields the theoretical and algorithmic background for uniform existence and uniform uniqueness proofs of the (known) sporadic simple groups. A finite simple group G is called *sporadic* if it is not isomorphic to an alternating group A_n or a finite simple group of Lie type described in R. W. Carter's book [13]. The theoretical results and algorithms presented in the first volume [92] and here hold in general. They are not restricted to sporadic groups at all as will be shown again in this volume.

Many results on abstract finite simple groups are inspired by the celebrated 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. But it does not give any hint of how to find such a group H without knowing at least one of the simple groups G. In particular, most of the known sporadic simple groups G were not discovered by a construction from a given centralizer H. In his survey article [37], p. 71, D. Gorenstein wrote in 1979: "Much of the excitement generated by the developments in simple group theory over the last 20 years can be directly attributed to the discovery of over 20 sporadic new simple groups... The existence of these strange objects...revealed the richness of the subject and lent an air of mystery to the nature of simple groups." After a brief survey about the "presently known" 26 sporadic simple groups he remarks: "There you have the 26 beautiful enigmatic sporadic groups with Janko's fourth group and the Fischer monster still waiting to be born. Arising out of so many unrelated contexts, is it yet possible that there is a single, coherent explanation for their existence? If so, it will require some new

2

Introduction

vision, seemingly beyond the capabilities of the present generation, to discover it."

It is one purpose of this second volume to answer Gorenstein's question using the representation theoretic and algorithmic methods developed in the first volume [92]. This solution is achieved by means of the author's Algorithm 1.3.8 and its iterated version 1.3.15 described in Chapter 1. They construct centralizers H of 2-central involutions z of certain finite simple groups G from indecomposable subgroups T of the general linear groups $GL_n(2)$. By Definition 1.3.5 such a subgroup T is called indecomposable if the natural vector space $V = F^n$ is an indecomposable FT-module over the prime field F = GF(2) of characteristic 2. Irreducible subgroups T of $GL_n(2)$ are defined similarly. In general H is not uniquely determined by T. Several steps of Algorithm 7.4.8 of [92] have been incorporated into Algorithm 1.3.8. Thus it is possible to build the simple target groups G from a previously constructed centralizer H provided all its conditions can be satisfied in the course of the construction. This algorithm constructs (in theory) all simple groups G whose Sylow 2-subgroups S have a non-cyclic elementary abelian normal subgroup Aof order 2^n such that $N_G(A)/C_G(A) \cong T \leq \operatorname{GL}_n(2)$ and the centralizer $C_G(A)$ is either A or an iterated FT-module extension. In view of Theorem 4.8.5 of [92] and Remark 1.3.14, these requirements are not serious restrictions. It is shown in this book that these conditions are satisfied by all known sporadic groups. By Kondo's work [77] they hold for all alternating groups A_{4k+r} with $k \geq 2$ and $0 \leq r \leq 3$. They are also true for several simple groups of Lie type whose Sylow 2-subgroups are neither metabelian, dihedral nor semi-dihedral.

Algorithm 1.3.8 provides a new link between modular representation theory and the study of finite simple groups. Since the Sylow 2subgroups S of the relevant indecomposable groups T of $GL_n(2)$ are not cyclic, their group algebras FT have infinitely many non-isomorphic finite-dimensional indecomposable FT-modules by a classical theorem of D. G. Higman; see Theorem 1.2.3. This means that there are infinitely many dimensions m such that $GL_m(2)$ has an indecomposable subgroup T_m which is an epimorphic image of T. In theory Algorithm 1.3.8 can be applied to any of these groups T_m again. Therefore the first section of Chapter 1 contains a summary of two survey articles by R. Brauer [10] and D. Gorenstein [37] addressing the general classification problem of the finite simple groups. They were published in 1979, two years before D. Gorenstein's announcement of the classification theorem; see Theorem 1.1.2 and its Corollary 1.1.3. Gorenstein's approach to the classification problem assumes implicitly that an inductive argument can

Introduction

be produced which shows that there will be exactly 26 sporadic simple groups. On the other hand, R. Brauer addresses all aspects of the classification problem. In particular, he remarks: "It is not even impossible that no classification exists."

The present mathematical literature does not contain an accessible proof of the announced classification theorem; see Theorem 1.1.2. Furthermore, D. G. Higman's Theorem 1.2.3, Algorithm 1.3.8 and all its successful applications in nature provide strong support for R. Brauer's remark. In particular, we show in [92] and in this book that 23 of the known sporadic simple groups can be constructed by means of Algorithms 1.3.8 and 1.3.15 in a uniform way. The smallest sporadic group is not considered here because the Sylow 2-subgroups of Mathieu group M_{11} are semi-dihedral; see Theorem 1.6.7 of [92]. In theory, given enough computational power and efficient implementations of the relevant basic algorithms of MAGMA, an application of Algorithm 1.3.15 to some well determined indecomposable subgroups of $GL_9(2)$ and $GL_{10}(2)$ will also construct the baby monster and the monster, respectively; see Chapter 16.

This volume contains 16 chapters, each of which has an introduction summarizing its contents and mentioning the relevant literature. The given proofs build again on the intimate relations between general group theory, ordinary character theory, modular representation theory and algorithmic algebra described in [92].

The last three sections of Chapter 1 contain several new algorithms and theoretical results that improve the applicability of Algorithms 1.3.8 and 1.3.15. Remarks 1.3.11 and 1.3.12 present a survey about the sporadic simple groups dealt with in [92] that can be constructed from an indecomposable subgroup T of some $GL_n(2)$. They are the four Mathieu groups M_{12}, M_{22}, M_{23} and M_{24} , Janko's group J_1 , Held's group He, Harada's group Ha and Thompson's group Th. All these simple groups G have a Sylow 2-subgroup S containing a maximal elementary abelian normal subgroup A which is self centralizing in G. By Remark 1.3.14, the two Janko groups J_2 and J_3 and the Higman–Sims group HS dealt with in Chapters 8 and 10 of [92] can be constructed from an indecomposable subgroup T of $GL_2(2)$ by means of Algorithm 1.3.15 using iterated FT-module extensions. In this book we show that the iterated version of Algorithm 1.3.8 can be applied to construct the Tits group, $F_2(4)'$, and the sporadic simple groups Ru of Rudvalis, Ly of Lyons, Suz of M. Suzuki and ON of O'Nan.

Since the Mathieu group M_{11} has a semi-dihedral subgroup it can be neglected by Theorem 1.6.7 of [92] due to J. Alperin, R. Brauer and

4

Introduction

D. Gorenstein; see [2]. All other known sporadic simple groups are dealt with in [92] and in this book.

In the course of their constructions, several simple groups of Lie type, such as $Sp_6(2)$, $U_4(2)$, $U_4(3)$, $U_6(2)$ and $O_8(2)$ are constructed by means of Algorithm 1.3.8 from the given data of certain constructed subgroups of the particular sporadic groups. Each time, these classical groups could be realized in some of their indecomposable or irreducible representations over their fields of definition; see Carter's book [13].

In Chapter 2, Algorithm 1.3.8 is applied to the irreducible subgroup $T = \operatorname{GL}_3(2)$ of $\operatorname{GL}_3(2)$. Thus one obtains Dickson's simple group $G = \operatorname{G}_2(3)$. We also present in Chapter 2, L. Wang's and the author's proof for Z. Janko's characterization [68] of this simple group by its centralizer $H = C_G(z)$ of a 2-central involution z. Let q be an odd prime power such that $q \equiv 3$ or 5 mod (8). By P. Fong's article [31], there are infinitely many simple Dickson groups $\operatorname{G}_2(q)$, each of which, in theory, can be constructed by means of Algorithm 1.3.8 from the irreducible subgroup $T = \operatorname{GL}_3(2)$ of $\operatorname{GL}_3(2)$; see Corollary 2.1.3. So it cannot be proved that Algorithm 1.3.8 constructs finitely many simple groups from a given indecomposable subgroup T of some $\operatorname{GL}_n(2)$.

Chapter 3 deals with Conway's sporadic simple group Co_3 . The presented existence and uniqueness proofs for Co_3 are due to the author. J. Conway discovered this simple group in 1969. He proved its existence in his famous paper on the automorphism group of the Leech lattice [16]. The first uniqueness proof for Co_3 was given by D. Fendel in [28]. It depends on a deep theorem of W. Feit, classifying certain integral sublattices of the Leech lattice; see [27]. We construct in Proposition 3.1.2 a finitely presented group H with center of order 2 by an application of Algorithm 1.3.8 to the irreducible subgroup \mathcal{C} of $\mathrm{GL}_{23}(23)$ such that $H \cong C_{\mathfrak{G}}(\mathfrak{z})$ for a 2-central involution \mathfrak{z} of \mathfrak{G} . This matrix group is an important ingredient of the given self-contained uniqueness proof of Co_3 ; see Theorem 3.3.13. In particular, we do not quote Feit's theorem.

Chapters 4–9 describe H. Kim's and the author's recent applications of Algorithm 1.3.8 to the 10-dimensional and 11-dimensional 2-modular irreducible representations of the Mathieu groups M_{22} , M_{23} and M_{24} over GF(2), respectively. The resulting simple groups are isomorphic to the sporadic Conway groups Co_2 , Co_1 , the sporadic Fischer groups Fi_{22} , Fi_{23} , Fi'_{24} and the large Janko group J_4 discovered in [16], [29] and [69], respectively.

Whereas the three Conway groups were originally constructed in [16] as subgroups or factor groups of the group $Aut(\Lambda)$ of isometries of the

Introduction

24-dimensional Leech lattice Λ , Fischer realized his groups as automorphism groups of special graphs defined by means of certain involutions of his simple groups; see [29]. Janko's original article [69] on J₄ employs purely algebraic methods. They have been generalized by the author to obtain uniform existence proofs for all sporadic simple groups. In fact, the combinatorial methods used in Conway's survey article on the Leech lattice groups [17] and the geometric methods described in the books by Aschbacher [3] and Ivanov [64], dealing with the Fischer groups and the large Janko group J₄, respectively, are distinct and unrelated.

Chapters 4 and 5 present H. Kim's and the author's simultaneous existence proofs for the simple sporadic groups Co_2 of Conway and Fi_{22} of Fischer published in [72]. The sporadic simple group Co_2 is constructed as a simple subgroup \mathfrak{G}_3 of $GL_{23}(13)$ by an application of Algorithm 1.3.8 to a well determined irreducible subgroup $T \cong Aut(M_{22})$ of $GL_{10}(2)$. In Chapter 5 the simple group Fi_{22} is constructed as a simple subgroup \mathfrak{G}_2 of $GL_{78}(13)$ by applying Algorithm 1.3.8 to another well determined irreducible subgroup $T \cong M_{22}$ of $GL_{10}(2)$. Section 5.3 contains a sketch of a uniqueness proof for Fi_{22} . In Section 5.4 we give some examples of irreducible subgroups T of $GL_{10}(2)$ for which no simple group G exists having a Sylow 2-subgroup S containing a non-cyclic maximal elementary abelian normal subgroup A such that $C_G(A) = A$ and $N_G(A)/A \cong T$.

The constructions of the large sporadic groups Fi_{23} , Co_1 , J_4 and Fi_{24} are technically more demanding because (in 2007) our applications of MAGMA were not able to calculate the cohomological data required for performing Steps 2 and 5 of Algorithm 1.3.8. In order to obtain the presentations of the centralizers H of the 2-central involutions z of the simple target groups G we were forced to construct some local subgroups of H in advance.

Chapter 6 describes Kim's application [73] of Algorithm 1.3.8 to the non-split extension E of the simple Mathieu group M_{23} by a well determined irreducible module V_2 of dimension 11 over GF(2). Proposition 6.2.1 gives a presentation of the centralizer $D = C_E(z)$ of a 2-central involution z of E by means of Step 4 of Algorithm 1.3.8. It also describes the construction of a presentation of another group H_2 having a central subgroup $Z_2 = \langle z \rangle$ such that H_2/Z_2 is isomorphic to the centralizer H_1 of a 2-central involution z of Fi₂₂ constructed in Chapter 5. Using the character tables of D and H_2 and Algorithm 7.4.8 of [92], Kim constructed a matrix subgroup \mathfrak{H}_1 in $\mathfrak{SL}_{352}(17)$ with center \mathfrak{Z} of order 2 and showed in [73] that $\mathfrak{H}/\mathfrak{Z} \cong \mathrm{Fi}_{22}$. The details are given in Proposition 6.2.2. Proposition 6.2.3 constructs a fairly nice presentation and a faithful

© in this web service Cambridge University Press

6

Introduction

permutation representation of \mathfrak{H} of degree 28160. Since all conditions of Step 5 of Algorithm 1.3.8 are verified in Corollary 6.2.4, its Steps 6– 11 are applied in the proof of Theorem 6.3.1, realizing Fischer's simple group Fi₂₃ as a simple subgroup \mathfrak{G} of GL₇₈₂(17). This existence theorem is due to Kim [73]. The constructions by means of Algorithm 1.3.8 of the large Conway's group Co₁, Janko's group J₄ and Fischer's group Fi₂₄ from the two 11-dimensional irreducible 2-modular representations of the Mathieu group M₂₄ are summarized in the following diagram:



Introduction

The smallest non-trivial irreducible 2-modular representations of M_{24} denoted by V_1 and V_2 are of dimension 11 over GF(2). Chapter 7 describes H. Kim's and the author's application of Algorithm 1.3.8 to the split extension E_1 of M_{24} by V_1 . Using similar methods as the ones described in Chapter 6 we constructed a finitely presented group H having a center $\langle z \rangle$ of order 2 in Proposition 7.2.2 satisfying all conditions of step 5 of Algorithm 1.3.8. It is then used to realize Co_1 as a matrix subgroup \mathfrak{G} of $GL_{276}(13)$; see Theorem 7.3.2. In particular, \mathfrak{G} has a 2central involution \mathfrak{z} such that $C_{\mathfrak{G}}(\mathfrak{z}) \cong H$. In Section 7.3 we also prove Soicher's Theorem 7.3.3 of [120], giving a nice presentation of Conway's original group Co_1 . Using it and the constructed faithful permutation representation of H of degree 61440 it is shown in Corollary 7.3.4 that H is also isomorphic to a centralizer of a 2-central involution of Co_1 . Section 7.4 discusses the uniqueness problem of \mathfrak{G} and Co_1 .

Applying Algorithm 1.3.8 to the split extension E_2 of M_{24} by V_2 , one obtains Janko's sporadic group J_4 as a simple subgroup \mathfrak{G} of $GL_{1333}(43)$; see Theorem 8.3.2. Because of lack of space, only the construction of \mathfrak{G} from a constructed presentation of the centralizer H of a 2-central involution z of the simple target group G is described in detail in Chapter 8. This construction and several results of Janko's original article [69] are applied in Section 8.3 to give a uniqueness proof for J_4 ; see Theorem 8.3.4. In Section 8.4 we present a survey about earlier constructions of J_4 as subgroups of $GL_{112}(2)$ and $GL_{1333}(11)$ due to Benson, Conway, Norton, Parker and Thackray [8] (see also [102]) and W. Lempken [84], respectively. We also mention Weller's construction of a faithful permutation representation of Lempken's group G of degree 173067389 in [135]. It has been used by Weller and the author in [98] to construct a 112dimensional representation J of G in $GL_{112}(2)$ and to show that J and the original group constructed by Benson, Conway, Norton, Parker and Thackray are conjugate in $GL_{112}(2)$. All generating matrices of \mathfrak{G} , G and J and the corresponding permutations are stored on the accompanying DVD.

Fischer's simple group F'_{24} is constructed in Chapter 9 as a simple subgroup \mathfrak{G} of $GL_{8671}(13)$ following H. Kim's and the author's recent article [74]; see Proposition 9.3.2. Let E_3 be the uniquely determined non-split extension of M_{24} by V_2 . For technical reasons described in the introduction of Chapter 9 it is constructed by means of an application of Algorithm 1.3.8 to a non-2-central involution v of E_3 with centralizer $U = C_{E_3}(v)$ of order $2^{19} \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$. In Section 9.4 we construct an isomorphism between the matrix group $\mathfrak{G} = \langle \mathfrak{q}, \mathfrak{y}, \mathfrak{t}, \mathfrak{w} \rangle$ of Proposition 9.3.2 and the commutator subgroup of the finitely presented group G of

8

Introduction

Hall and Soicher; see [110], p. 111. Hence \mathfrak{G} is isomorphic to Fischer's simple group Fi'_{24} . Thus it follows that \mathfrak{G} has a faithful permutation representation of degree 306936 with stabilizer $G_1 \cong \mathsf{Fi}_{23}$ constructed in Chapter 6. It is used to calculate the character table of \mathfrak{G} by means of MAGMA. In Section 9.5 we determine a presentation of the centralizer H of a 2-central involution z of \mathfrak{G} . It is used in Section 9.6 to prove D. Parrott's Theorem [107] asserting that all simple groups G of Fi'_{24} -type have the same order $G = 2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$.

By Remark 1.3.11 the Mathieu groups M_{22} , M_{23} and M_{24} can be constructed from irreducible subgroups of $GL_4(2)$ and $GL_6(2)$. Therefore the two large Conway groups Co_2 and Co_1 , all three Fischer groups and the large Janko group J_4 can be constructed from these small linear groups by repeated applications of Algorithm 1.3.8.

In Chapter 10 we apply Algorithm 1.3.8 to an *indecomposable* subgroup of $\operatorname{GL}_5(2)$ and obtain a self-contained existence proof of Tits' simple group $G = F_2(4)'$ of Lie type; see Theorem 10.3.1. It is used in the uniqueness proof of Theorem 10.6.2 due to L. Wang and the author; see [97]. This example also shows how difficult it can be to find the indecomposable subgroups T of $\operatorname{GL}_n(2)$ which lead to a simple group. The constructed simple subgroup \mathfrak{G} of $\operatorname{GL}_{26}(73)$ is shown to be isomorphic to the original Tits group by means of Parrott's presentation [105] of a centralizer of a 2-central involution.

The existence and uniqueness of J. McLaughlin's simple group McL [89] is proved in Chapter 11 by deriving a presentation of this group from I. Schur's presentation of the covering group $2A_8$ of the alternating group A_8 , which is assumed to be the given centralizer of a 2-central involution z of the simple target group G; see Theorem 11.3.1 due to M. Kratzer, W. Lempken, K. Waki and the author [80]. These results show that McL could also have been constructed by application of Algorithm 1.3.8 to the irreducible subgroup A_7 of GL₄(2).

The simple groups G studied in the remaining chapters of the book can be constructed by applications of Algorithm 1.3.15 to indecomposable subgroups of some $\operatorname{GL}_n(2)$. In Chapter 12 we apply it to an irreducible subgroup $T \cong \operatorname{GL}_3(2)$ of $\operatorname{GL}_8(2)$ and construct an iterated extension Eof T by its irreducible FT-modules W and V of dimensions 8 and 3 over F = GF(2), respectively. In Sections 12.2 and 12.3 we show that the application of all the steps of Algorithm 1.3.15 gives an existence proof of the sporadic simple group Ru discovered by A. Rudvalis [115]; see Theorem 12.2.1. It is used in Section 12.4, where we prove the uniqueness of Ru in Theorem 12.4.1 due to D. Parrott [106].

Introduction

Chapter 13 provides a self-contained existence proof for the simple sporadic group Ly originally discovered R. Lyons [88]. It is constructed as a simple subgroup \mathfrak{G} of $\operatorname{GL}_{2480}(31)$ from Schur's presentation of the given centralizer $H \cong 2A_{11}$ of an involution z of the simple target group G, which is assumed to be the covering group of the alternating group A_{11} ; see Theorem 13.5.2. In Section 13.6, M. Weller's and the author's uniqueness proof for the Lyons group is given; see Theorem 13.5.4.

Chapter 14 contains an existence proof for the sporadic simple Suz of M. Suzuki [124]. The sporadic Suzuki group can be constructed by means of an application of Algorithm 1.3.15 to an irreducible subgroup $L \cong 3A_6$ of GL₆(2). Because of lack of space we present only our construction of Ru inside GL₁₄₃(13) from a presentation of the given centralizer of a 2-central involution. We also give a uniqueness proof. It is self-contained, except for a quotation of Phan's uniqueness theorem of U₄(3) of [109], which can also be proved completely by means of the methods and results of [92] and this book.

The last sporadic simple group dealt with in this book is O'Nan's simple group ON [104]. Its Sylow 2-subgroup S was originally constructed by J. Alperin [1] in terms of generators and relations. O'Nan derived the structure of the centralizer $H = C_G(z)$ of a 2-central involution z from Alperin's presentation. He proved important results on the structure of the maximal subgroups and determined the character table of his group. The first published existence and uniqueness proof for ON is due to L. Soicher [121]. It depends heavily on O'Nan's work. The existence and uniqueness proof given in Chapter 14 is due to A. Previtali and the author; see [94]. It starts from a given presentation of the group H. It derives from that a uniquely determined presentation of a simple group $\mathfrak{G} \cong ON$ and a faithful permutation representation of degree 2624832 with stabilizer \mathfrak{J} isomorphic to Janko's sporadic group J₁ dealt with in [92].

Most of the sporadic simple groups G treated in this book have been constructed as matrix subgroups of $\operatorname{GL}_n(p)$, where n is the degree of an ordinary irreducible character χ of G which is of p-defect zero. The reason for that choice is Brauer's characterization of characters proved in [92]. It allows us to construct irreducible ordinary characters from the normalizers of cyclic subgroups of prime order. This is an important ingredient of all our uniqueness proofs. It does not have any analog for p-modular representations. By Theorem 3.12.4 of [92], due to R. Brauer, the reduction of an ordinary character of p-defect zero yields a uniquely

10

Introduction

determined modular representation of G in $\operatorname{GL}_n(p^k)$, where the finite field $GF(p^k)$ is a splitting field for G.

The final chapter contains a number of open problems related to R. Brauer's remarks on the aforementioned classification project. Section 16.2 summarizes a selection of uniqueness problems of some finite simple groups that we either left open in the previous chapters or have not been dealt with in the mathematical literature. In Section 16.3 we describe Thompson's suggestion [127] for finding a possibly new 27th sporadic simple group. Its Sylow 2-subgroup would have order 2²⁵. Therefore an application of Algorithm 1.3.15 to the iterated extension K of $T = GL_5(2)$ described in R. Griess' Theorem 16.3.2 would be technically very demanding. But it would prove or disprove Thompson's suggestion ignored in [38] and the recent literature. In Section 16.4 we illustrate Brauer's question for a general classification scheme of the finite simple groups by means of a special classification problem. It asks for an abstract classification of all finite simple groups G which can be constructed by an application of Algorithm 1.3.8 to all the indecomposable subgroups of the infinite sequence of general linear groups $GL_n(2)$. For a fixed integer n we also describe an exhaustive search method for finding the corresponding simple groups. In view of D. G. Higman's Theorem 1.2.3, one cannot bound the dimension n.

The practicality of Algorithm 1.3.8 has been greatly improved by recent implementations of Holt's Algorithm [53] into MAGMA for constructing presentations of the FG-module extensions E of a finitely presented transitive permutation group G. Furthermore, the isomorphism test described in Chapter 6 of [92] has been improved by Cannon and Holt [12]. Recent releases of MAGMA also contain an implementation of a powerful algorithm due to Cannon, Cox and Holt [11], constructing the conjugacy classes of subgroups of a finite permutation group. Many of the group constructions described in this book would not have been possible without these tools. Furthermore, MAGMA [9] is very well documented. Therefore the author quotes its commands that have been used in the specific calculations of a proof or in the constructions of the simple groups dealt with in this book. Of course, that will help only those readers who have a computer at hand. On the other hand, young students, like the author's collaborator H. Kim, can get started in this area of research without great difficulty provided they have a good knowledge of undergraduate mathematics.

The Appendix contains a detailed table of contents of the accompanying DVD. It consists of two parts. On DVD.1 we stored all the large